

Security+™ Fast Pass

James Michael Stewart

SYBEX®

Security+

Fast Pass



Security+™ Fast Pass



James Michael Stewart

San Francisco • London



Associate Publisher: Neil Edde
Acquisitions Editor: Jeff Kellum
Developmental Editor: Jeff Kellum
Production Editor: Rachel Gunn
Technical Editor: Patrick Bass
Copyeditor: Tiffany Taylor
Compositor: Kate Kaminski, Happenstance Type-O-Rama
CD Coordinator: Dan Mummert
CD Technician: Kevin Ly
Proofreaders: Nancy Riddiough, Laurie O'Connell
Indexer: Lynnzee Elze
Book Designer: Judy Fung, Bill Gibson
Cover Designer: Richard Miller, Calyx Design
Cover Illustrator/Photographer: Richard Miller, Calyx Design

Copyright © 2004 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic, or other record, without the prior agreement and written permission of the publisher.

Library of Congress Card Number: 2004109304

ISBN: 0-7821-4359-8

SYBEX and the SYBEX logo are either registered trademarks or trademarks of SYBEX Inc. in the United States and/or other countries.

Screen reproductions produced with FullShot 99. FullShot 99 © 1991-1999 Inbit Incorporated. All rights reserved. FullShot is a trademark of Inbit Incorporated.

The CD interface was created using Macromedia Director, COPYRIGHT 1994, 1997-1999 Macromedia Inc. For more information on Macromedia and Macromedia Director, visit <http://www.macromedia.com>.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturer(s). The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Software License Agreement: Terms and Conditions

The media and/or any online materials accompanying this book that are available now or in the future contain programs and/or text files (the "Software") to be used in connection with the book. SYBEX hereby grants to you a license to use the Software, subject to the terms that follow. Your purchase, acceptance, or use of the Software will constitute your acceptance of such terms. The Software compilation is the property of SYBEX unless otherwise indicated and is protected by copyright to SYBEX or other copyright owner(s) as indicated in the media files (the "Owner(s)"). You are hereby granted a single-user license to use the Software for your personal, noncommercial use only. You may not reproduce, sell, distribute, publish, circulate, or commercially exploit the Software, or any portion thereof, without the written consent of SYBEX and the specific copyright owner(s) of any component software included on this media.

In the event that the Software or components include specific license requirements or end-user agreements, statements of condition, disclaimers, limitations or warranties ("End-User License"), those End-User Licenses supersede the terms and conditions herein as to that particular Software component. Your purchase, acceptance, or use of the Software will constitute your acceptance of such End-User Licenses.

By purchase, use or acceptance of the Software you further agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

Software Support

Components of the supplemental Software and any offers associated with them may be supported by the specific Owner(s) of that material, but they are not supported by SYBEX. Information regarding any available support may be obtained from the Owner(s) using the information provided in the appropriate read.me files or listed elsewhere on the media.

Should the manufacturer(s) or other Owner(s) cease to offer support or decline to honor any offer, SYBEX bears no responsibility. This notice concerning support for the Software is provided for your information only. SYBEX is not the agent or principal of the Owner(s), and SYBEX is in no way responsible for providing any support for the Software, nor is it liable or responsible for any support provided, or not provided, by the Owner(s).

Warranty

SYBEX warrants the enclosed media to be free of physical defects for a period of ninety (90) days after purchase. The Software is not available from SYBEX in any other form or media than that enclosed herein or posted to

www.sybex.com. If you discover a defect in the media during this warranty period, you may obtain a replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to:

SYBEX Inc.
Product Support Department
1151 Marina Village Parkway
Alameda, CA 94501
Web: <http://www.sybex.com>

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for \$10, payable to SYBEX.

Disclaimer

SYBEX makes no warranty or representation, either expressed or implied, with respect to the Software or its contents, quality, performance, merchantability, or fitness for a particular purpose. In no event will SYBEX, its distributors, or dealers be liable to you or any other party for direct, indirect, special, incidental, consequential, or other damages arising out of the use of or inability to use the Software or its contents even if advised of the possibility of such damage. In the event that the Software includes an online update feature, SYBEX further disclaims any obligation to provide this feature for any specific duration other than the initial posting.

The exclusion of implied warranties is not permitted by some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights; there may be other rights that you may have that vary from state to state. The pricing of the book with the Software by SYBEX reflects the allocation of risk and limitations on liability contained in this agreement of Terms and Conditions.

Shareware Distribution

This Software may contain various programs that are distributed as shareware. Copyright laws apply to both shareware and ordinary commercial software, and the copyright Owner(s) retains all rights. If you try a shareware program and continue using it, you are expected to register it. Individual programs differ on details of trial periods, registration, and payment. Please observe the requirements stated in appropriate files.

Copy Protection

The Software in whole or in part may or may not be copy-protected or encrypted. However, in all cases, reselling or redistributing these files without authorization is expressly forbidden except as specifically provided for by the Owner(s) therein.

To Catharine Renee Dodds, I can't believe how amazing it is.

Acknowledgments

Thanks to all those at Sybex that continue to allow me to do what I enjoy most—impart knowledge to others. Thanks to Jeff Kellum and Rachel Gunn for professional juggling services adequately rendered. And thanks to others behind the scenes, including my tech editor, Patrick Bass, and my copyeditor, Tiffany Taylor, who helped turn my thoughts into comprehensible sentences. To my parents, Dave and Sue, thanks for your love and consistent support. To my sister Sharon and nephew Wesley, it's great seeing you so often. To Mark, now that munchkin number three is in the oven, how long until you have your own sports team? To HERbert and Quin, behave or the catnip will stay in the container. And finally, as always, to Elvis—why does everyone think I'm such a fan? I mean really, just because I have a picture of you in every room... Geesh!

Contents at a Glance

<i>Introduction</i>	<i>xiii</i>
Chapter 1 General Security Concepts	1
Chapter 2 Communication Security	37
Chapter 3 Infrastructure Security	71
Chapter 4 Basics of Cryptography	117
Chapter 5 Operational/Organizational Security	147
<i>Index</i>	<i>181</i>

Contents

Introduction

xiii

Chapter 1	General Security Concepts	1
1.1	Identifying Access Control Models	3
	Critical Information	3
	Role-Based Access Control (RBAC)	6
	Exam Essentials	6
1.2	Identifying Authentication Methods	7
	Critical Information	7
	Exam Essentials	15
1.3	Identifying Non-Essential Services	15
	Critical Information	16
	Exam Essentials	17
1.4	Identifying Attack Methods	18
	Critical Information	18
	Exam Essentials	28
1.5	Identifying Malicious Code	29
	Critical Information	29
	Exam Essentials	30
1.6	Understanding Social Engineering	31
	Critical Information	31
	Exam Essentials	32
1.7	Understanding Auditing	32
	Critical Information	33
	Exam Essentials	33
	Review Questions	34
	Answers to Review Questions	36
Chapter 2	Communication Security	37
2.1	Remote Access Technologies	39
	Critical Information	40
	Exam Essentials	47
2.2	E-mail Security	48
	Critical Information	48
	Exam Essentials	53
2.3	Internet Security	54
	Critical Information	54
	Exam Essentials	59

	2.4 Directory Security	60
	Critical Information	60
	Exam Essentials	61
	2.5 File Transfer Protocols	61
	Critical Information	62
	Exam Essentials	63
	2.6 Wireless	64
	Critical Information	64
	Exam Essentials	66
	Review Questions	68
	Answers to Review Questions	70
Chapter 3	Infrastructure Security	71
	3.1 Security Devices	74
	Critical Information	74
	Exam Essentials	82
	3.2 Media Security	82
	Critical Information	82
	Exam Essentials	88
	3.3 Security Topologies	89
	Critical Information	89
	Exam Essentials	94
	3.4 Intrusion Detection	95
	Critical Information	95
	Active Detection and Passive Detection	97
	Exam Essentials	102
	3.5 Environment Hardening	103
	Critical Information	103
	Exam Essentials	111
	Review Questions	113
	Answers to Review Questions	115
Chapter 4	Basics of Cryptography	117
	4.1 Cryptographic Algorithms	119
	Critical Information	119
	Exam Essentials	124
	4.2 Cryptography Security Concepts	125
	Critical Information	125
	Exam Essentials	128
	4.3 Public Key Infrastructure	129
	Critical Information	129
	Exam Essentials	134
	4.4 Cryptographic Standards and Protocols	135

	4.5 Key Management and Certificate Life Cycles	136
	Critical Information	136
	Exam Essentials	141
	Review Questions	144
	Answers to Review Questions	146
Chapter 5	Operational/Organizational Security	147
	5.1 Physical Security	150
	Critical Information	150
	Exam Essentials	155
	5.2 Disaster Recovery	156
	Critical Information	156
	Exam Essentials	158
	5.3 Business Continuity	159
	Critical Information	159
	Exam Essentials	162
	5.4 Security Policy Issues	163
	Critical Information	163
	Exam Essentials	166
	5.5 Privilege Management	167
	Critical Information	167
	Exam Essentials	169
	5.6 Forensics	170
	Critical Information	170
	Exam Essentials	171
	5.7 Risk Identification	171
	Critical Information	171
	Exam Essentials	173
	5.8 Security Training	173
	Critical Information	173
	Exam Essentials	174
	5.9 Security Documentation	175
	Critical Information	175
	Exam Essentials	177
	Review Questions	178
	Answers to Review Questions	180
<i>Index</i>		181

Introduction

The Security+ certification program was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of computer service technicians in basics of computer security. The Security+ certification is granted to those who have attained the level of knowledge and security skills that show a basic competency with security needs of both personal and corporate computing environments.

CompTIA's exam objectives are periodically updated to keep their exams applicable to the most recent developments. However, this isn't a regular occurrence since the foundational elements remain constant even as the higher-end technology advances. The Security+ objectives themselves haven't been altered since the exam came out in 2002.

What Is Security+ Certification?

The Security+ certification was created to offer an introductory step into the complex world of IT security. You only need to pass a single exam to become Security+ certified. However, obtaining this certification doesn't mean you can provide realistic security services to a company. In fact, this is just the first step toward true security knowledge and experience. By obtaining Security+ certification, you should be able to acquire more security experience in order to pursue more complex and in-depth security knowledge and certification.

For the latest pricing on the exam and updates to the registration procedures, call Prometric at (866) 776-6387 or (800) 776-4276. You can also go to either www.2test.com or www.prometric.com for additional information or to register online. If you have further questions about the scope of the exams or related CompTIA programs, refer to the CompTIA website at www.comptia.org.

Is This Book for You?

Security+ Fast Pass is designed to be a succinct, portable exam review guide that can be used either in conjunction with a more complete study program (Sybex's *Security+ Study Guide, 2nd Edition* (Sybex, 2004), CBT courseware, classroom/lab environment) or as an exam review for those who don't feel the need for more extensive test preparation. It isn't our goal to give away the answers, but rather to identify those topics on which you can expect to be tested and to provide sufficient coverage of these topics.

Perhaps you've been working with information technologies for years. The thought of paying lots of money for a specialized IT exam-preparation course probably doesn't sound appealing. What can they teach you that you don't already know, right? Be careful, though—many experienced network administrators have walked confidently into the test center only to walk sheepishly out of it after failing an IT exam. After you've finished reading this book, you should have a clear idea of how your understanding of the technologies involved matches up with the expectations of the Security+ test makers.

Or perhaps you're relatively new to the world of IT, drawn to it by the promise of challenging work and higher salaries. You've just waded through an 800-page study guide or taken a class at a local training center. Lots of information to keep track of, isn't it? Well, by organizing the *Fast Pass* book according to CompTIA's exam objectives, and by breaking up the information into concise, manageable pieces, we've created what we think is the handiest exam review guide available. Throw it in your briefcase and carry it to work with you. As you read the book, you'll be able to quickly identify those areas you know best and those that require a more in-depth review.



The goal of the *Fast Pass* series is to help certification candidates brush up on the subjects on which they can expect to be tested in the exams. For complete in-depth coverage of the technologies and topics involved in the Security+ exam, we recommend the *Security+ Study Guide, Second Edition*, by Sybex.

How Is This Book Organized?

This book is organized according to the official objectives list prepared by CompTIA for the Security+ exam. The chapters correspond to the five major domains of objective and topic groupings. The exam is weighted across these five domains as follows:

- Domain 1.0—General Security Concepts (30%)
- Domain 2.0—Communication Security (20%)
- Domain 3.0—Infrastructure Security (20%)
- Domain 4.0—Basics of Cryptography (15%)
- Domain 5.0—Operational/Organizational Security (15%)

Within each chapter, the top-level exam objective from each domain are addressed in turn. Each objective's section is further divided into Critical Information, Exam Essentials, and Review Questions:

Critical Information The Critical Information section presents the greatest level of detail about information relevant to the objective. This is the place to start if you're unfamiliar with or uncertain about the technical issues related to the objective.

Exam Essentials Here you're given a short list of topics that you should explore fully before taking the test. Included in the Exam Essentials areas are notations of the key information you should have taken from the Critical Information section of this chapter or the corresponding content from the *Security+ Study Guide, Second Edition*.

Review Questions This section ends every chapter and provides 10 questions to help you gauge your mastery of the chapter.

The Security+ Exam Objectives

The following are the areas (referred to as *domains* by CompTIA) in which you must be proficient in order to pass the Security+ exam:

Domain 1: General Security Concepts This content area deals with basics of access control, methods of authentication, removing non-essential components, recognizing vulnerabilities and risks, dealing with malicious code, and auditing.

Domain 2: Communication Security This content area deals with the various types of remote access technologies, e-mail security, Internet security, directory security, file transfer security, and wireless security.

Domain 3: Infrastructure Security This content area deals with network devices, storage media, security topologies, intrusion detection systems, and hardening servers.

Domain 4: Basics of Cryptography This content area deals with hashing, symmetric cryptography, asymmetric cryptography, PKI, key management, and certificates.

Domain 5: Operational/Organizational Security This content area deals with physical security, disaster recovery, business continuity, security policy, privilege management, forensics, risk management, user training, and security documentation.

How to Contact the Publisher

Sybex welcomes feedback on all of its titles. Visit the Sybex website at www.sybex.com for book updates and additional certification information. You'll also find forms you can use to submit comments or suggestions regarding this or any other Sybex title.

The Security+ Exam Objectives

Throughout this book, we've used abridged versions of the Security+ objectives. For easy reference and clarification, the following is a complete listing of Security+ objectives.



Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit the Security+ Certification page of CompTIA's website (<http://www.comptia.org/certification/security/default.aspx>) for the most current listing of exam objectives.

General Security Concepts

1.1 Recognize and be able to differentiate and explain the following access control models

- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)

1.2 Recognize and be able to differentiate and explain the following methods of authentication

- Kerberos
- CHAP (Challenge Handshake Authentication Protocol)
- Certificates
- Username/Password
- Tokens
- Multi-factor
- Mutual
- Biometrics

1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols

1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk

- DOS/DDOS (Denial of Service/Distributed Denial of Service)
- Back Door
- Spoofing
- Man in the Middle
- Replay
- TCP/IP Hijacking
- Weak Keys
- Mathematical
- Social Engineering
- Birthday
- Password Guessing
 - Brute Force
 - Dictionary
- Software Exploitation

1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk

- Viruses
- Trojan Horses
- Logic Bombs
- Worms

1.6 Understand the concept of and know how reduce the risks of social engineering

1.7 Understand the concept and significance of auditing, logging and system scanning

Communication Security

2.1 Recognize and understand the administration of the following types of remote access technologies

- 802.1x
- VPN (Virtual Private Network)
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)
- L2TP/PPTP (Layer Two Tunneling Protocol/Point to Point Tunneling Protocol)
- SSH (Secure Shell)
- IPSEC (Internet Protocol Security)
- Vulnerabilities

2.2 Recognize and understand the administration of the following email security concepts

- S/MIME (Secure Multipurpose Internet Mail Extensions)
- PGP (Pretty Good Privacy) like technologies
- Vulnerabilities
 - SPAM
 - Hoaxes

2.3 Recognize and understand the administration of the following Internet security concepts

- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- HTTP/S (Hypertext Transfer Protocol/Hypertext Transfer Protocol over Secure Sockets Layer)
- Instant Messaging
 - Vulnerabilities
 - Packet Sniffing
 - Privacy
- Vulnerabilities
 - Java Script
 - ActiveX
 - Buffer Overflows
 - Cookies
 - Signed Applets
 - CGI (Common Gateway Interface)
 - SMTP (Simple Mail Transfer Protocol) Relay

2.4 Recognize and understand the administration of the following directory security concepts

- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- LDAP (Lightweight Directory Access Protocol)

2.5 Recognize and understand the administration of the following file transfer protocols and concepts

- S/FTP (File Transfer Protocol)
- Blind FTP (File Transfer Protocol)/Anonymous
- File Sharing
- Vulnerabilities
 - Packet Sniffing
 - Naming Conventions

2.6 Recognize and understand the administration of the following wireless technologies and concepts

- WTLS (Wireless Transport Layer Security)
- 802.11 and 802.11x
- WEP/WAP (Wired Equivalent Privacy/Wireless Application Protocol)
- Vulnerabilities
 - Site Surveys

Infrastructure Security

3.1 Understand security concerns and concepts of the following types of devices

- Firewalls
- Routers
- Switches
- Wireless
- Modems
- RAS (Remote Access Server)
- Telecom/PBX (Private Branch Exchange)
- VPN (Virtual Private Network)
- IDS (Intrusion Detection System)
- Network Monitoring/Diagnostics
- Workstations
- Servers
- Mobile Devices

3.2 Understand the security concerns for the following types of media

- Coaxial Cable
- UTP/STP (Unshielded Twisted Pair/Shielded Twisted Pair)
- Fiber Optic Cable
- Removable Media
 - Tape

- CD-R (Recordable Compact Disks)
- Hard Drives
- Diskettes
- Flashcards
- Smartcards

3.3 Understand the concepts behind the following kinds of Security Topologies

- Security Zones
 - DMZ (Demilitarized Zone)
 - Intranet
 - Extranet
- VLANs (Virtual Local Area Network)
- NAT (Network Address Translation)
- Tunneling

3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system

- Network Based
 - Active Detection
 - Passive Detection
- Host Based
 - Active Detection
 - Passive Detection
- Honey Pots
- Incident Response

3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system

- OS/NOS (Operating System/Network Operating System) Hardening
 - File System
 - Updates (Hotfixes, Service Packs, Patches)
- Network Hardening
 - Updates (Firmware)
 - Configuration
 - Enabling and Disabling Services and Protocols
 - Access Control Lists

- Application Hardening
 - Updates (Hotfixes, Service Packs, Patches)
 - Web Servers
 - E-mail Servers
 - FTP (File Transfer Protocol) Servers
 - DNS (Domain Name Service) Servers
 - NNTP (Network News Transfer Protocol) Servers
 - File/Print Servers
 - DHCP (Dynamic Host Configuration Protocol) Servers
 - Data Repositories
 - Directory Services
 - Databases

Basics of Cryptography

4.1 Be able to identify and explain the following different kinds of cryptographic algorithms

- Hashing
- Symmetric
- Asymmetric

4.2 Understand how cryptography addresses the following security concepts

- Confidentiality
- Integrity
 - Digital Signatures
- Authentication
- Non-Repudiation
 - Digital Signatures
- Access Control

4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure)

- Certificates
 - Certificate Policies
 - Certificate Practice Statements
- Revocation
- Trust Models

4.4 Identify and be able to differentiate different cryptographic standards and protocols

4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles

- Centralized vs. Decentralized
- Storage
 - Hardware vs. Software
 - Private Key Protection
- Escrow
- Expiration
- Revocation
 - Status Checking
- Suspension
 - Status Checking
- Recovery
 - M of N Control (Of M appropriate individuals, N must be present to authorize recovery)
- Renewal
- Destruction
- Key Usage
 - Multiple Key Pairs (Single, Dual)

Operational/Organizational Security

5.1 Understand the application of the following concepts of physical security

- Access Control
 - Physical Barriers
 - Biometrics
- Social Engineering
- Environment
 - Wireless Cells
 - Location
 - Shielding
 - Fire Suppression

5.2 Understand the security implications of the following topics of disaster recovery

- Backups
 - Off Site Storage
- Secure Recovery
 - Alternate Sites
- Disaster Recovery Plan

5.3 Understand the security implications of the following topics of business continuity

- Utilities
- High Availability/Fault Tolerance
- Backups

5.4 Understand the concepts and uses of the following types of policies and procedures

- Security Policy
 - Acceptable Use
 - Due Care
 - Privacy
 - Separation of Duties
 - Need to Know
 - Password Management
 - SLAs (Service Level Agreements)
 - Disposal/Destruction
 - HR (Human Resources) Policy
 - Termination (Adding and revoking passwords and privileges, etc.)
 - Hiring (Adding and revoking passwords and privileges, etc.)
 - Code of Ethics
- Incident Response Policy

5.5 Explain the following concepts of privilege management

- User/Group/Role Management
- Single Sign-on
- Centralized vs. Decentralized
- Auditing (Privilege, Usage, Escalation)
- MAC/DAC/RBAC (Mandatory Access Control/Discretionary Access Control/Role Based Access Control)

5.6 Understand the concepts of the following topics of forensics

- Chain of Custody
- Preservation of Evidence
- Collection of Evidence

5.7 Understand and be able to explain the following concepts of risk identification

- Asset Identification
- Risk Assessment
- Threat Identification
- Vulnerabilities

5.8 Understand the security relevance of the education and training of end users, executives and human resources

- Communication
- User Awareness
- Education
- On-line Resources

5.9 Understand and explain the following documentation concepts

- Standards and Guidelines
- Systems Architecture
- Change Documentation
- Logs and Inventories
- Classification
 - Notification
- Retention/Storage
- Destruction

Chapter

1

General Security Concepts

COMPTIA SECURITY+ EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.1 Recognize and be able to differentiate and explain the following access control models**
 - MAC (Mandatory Access Control)
 - DAC (Discretionary Access Control)
 - RBAC (Role Based Access Control)
- ✓ **1.2 Recognize and be able to differentiate and explain the following methods of authentication**
 - Kerberos
 - CHAP (Challenge Handshake Authentication Protocol)
 - Certificates
 - Username/Password
 - Tokens
 - Multi-factor
 - Mutual
 - Biometrics
- ✓ **1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols**
- ✓ **1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk**
 - DOS/DDOS (Denial of Service/Distributed Denial of Service)
 - Back Door
 - Spoofing



- Man in the Middle
 - Replay
 - TCP/IP Hijacking
 - Weak Keys
 - Mathematical
 - Social Engineering
 - Birthday
 - Password Guessing
 - Brute Force
 - Dictionary
 - Software Exploitation
- ✓ **1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk**
- Viruses
 - Trojan Horses
 - Logic Bombs
 - Worms
- ✓ **1.6 Understand the concept of and know how reduce the risks of social engineering**
- ✓ **1.7 Understand the concept and significance of auditing, logging and system scanning**



The Security+ exam will test your basic IT security skills—those skills needed to effectively secure stand-alone and networked systems in a corporate environment. To pass the test and be effective in implementing security, you need to understand the basic concepts and terminology in this chapter. This chapter covers all of the seven major sections of the first domain of the Security+ objectives. These sections focus on the following topics: access control models, authentication methods, non-essential services, common attacks, malicious code, social engineering, and system auditing.

1.1 Identifying Access Control Models

The full name of this section from the Security+ objectives list is “Recognize and be able to differentiate and explain the following access control models.” The mechanism by which users are granted or denied the ability to interact with and use resources is known as *access control*. Access control is often referred to using the term *authorization*. Authorization defines the type of access to resources users are granted—in other words, what users are authorized to do. Authorization is often considered the next logical step immediately after authentication. *Authentication* is the proving of your identity to a system or the act of logging on. With proper authorization or access control, a system will properly control access to resources in order to prevent unauthorized access.



For more information on this topic, refer to Chapter 1 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

There are three common access control methods:

- *Mandatory Access Control (MAC)*
- *Discretionary Access Control (DAC)*
- *Role-Based Access Control (RBAC)*

These three models are widely used in today’s IT environments. Familiarity with these three models is essential to the Security+ exam.



These three access control models aren't mutually exclusive. Two or more of them can be deployed simultaneously in a single environment.

Mandatory Access Control (MAC)

MAC is a form of access control commonly employed by government and military environments. MAC specifies that access is granted based on a set of rules rather than at the discretion of a user. The rules that govern MAC are hierarchical in nature and are often called *sensitivity labels*, *security domains*, or *classifications*. MAC environments define a few specific security domains or sensitivity levels and then use the associated labels from those domains to impose access control on objects and subjects.

A government or military implementation of MAC typically includes five levels:

- Unclassified
- Sensitive but unclassified
- Confidential
- Secret
- Top secret

This list is in order from least sensitive to most sensitive. Objects or resources are assigned sensitivity labels corresponding to one of these security domains. Each specific security domain or level defines the security mechanisms and restrictions that must be imposed in order to provide protection for objects within that domain.

MAC can also be deployed in private sector or corporate business environments. Such cases typically involve four levels of security domains:

- Public
- Sensitive
- Private
- Confidential

This list is also in order from least sensitive to most sensitive.

The primary purpose of a MAC environment is to prevent *disclosure*: the violation of the security principle of *confidentiality*. When an unauthorized user gains access to a secured resource, this is a security violation. Objects are assigned a specific sensitivity label based on the damage that would be caused if disclosure occurred. For example, if a top secret resource was disclosed, it could cause grave damage to national security.

A MAC environment works by assigning subjects a *clearance level* and objects a *sensitivity label*; in other words, everything is assigned a classification marker. *Subjects* or users are assigned clearance levels. The name of the clearance level is the same as the name of the sensitivity label assigned to *objects* or resources. A person (or other subject, such as a program or a computer system) must have the same or greater assigned clearance level as the resources they wish to

access. In this manner, access is granted or restricted based on the rules of classification (that is, sensitivity labels and clearance levels).

MAC is named as it is because the access control it imposes on an environment is mandatory. Its assigned classifications and the resulting granting and restriction of access can't be altered by users. Instead, the rules that define the environment and judge the assignment of sensitivity labels and clearance levels control authorization.

MAC isn't a very granularly controlled security environment. An improvement to MAC includes the use of *need to know*: a security restriction where some objects (resources or data) are restricted unless the subject has a need to know them. The objects that require specific need to know are assigned a sensitivity label, but they're compartmentalized from the rest of the objects with the same sensitivity label (within the same security domain). The need to know is a rule in and of itself, which states that access is only granted to subjects who have been assigned work tasks that require access to the cordoned-off object. Even if a subject has the proper level of clearance, without need to know, they are denied access. Need to know is the MAC equivalent of the principle of least privilege from DAC (see the following section).



The Trusted Computer System Evaluation Criteria (TCSEC), or Orange Book specifications, which defined government computer security classifications before December 2000 (when they were replaced by the Common Criteria), reference only MAC and DAC methods of access control.

Discretionary Access Control (DAC)

DAC is the form of access control or authorization that is used in most commercial and home environments. DAC is user directed or, more specifically, controlled by the owner and creators of the objects (resources) in the environment. DAC is identity based: Access is granted or restricted by an object's owner based on user identity and on the discretion of the object owner. Thus, the owner or creator of an object can decide whom to grant and deny access to their object.

DAC uses access control lists (ACLs). An ACL is a security logical device attached to every object and resource in the environment; it defines which users are granted or denied the various types of access available based on the object type. Individual user accounts or user groups can be added to an object's ACL and granted or denied access.

If your user account isn't granted access through an object's ACL, then you're denied access by default. If your user account is specifically granted access through an object's ACL, then you're granted the specific level or type of access defined. If your user account is specifically denied access through an object's ACL, then you're denied the specific level or type of access defined. In most cases, a Denied setting in an ACL overrides all other settings. Table 1.1 shows an access matrix for a user who is a member of three groups, and the resulting access to a folder on a network server. As you can see, the presence of the Denied setting overrides any other access granted from another group. Thus, if your membership in one user group grants you write access over an object, but another group specifically denies you write access to the same object, then you're denied write access to the object.

TABLE 1.1 Cumulative Access Based on Group Memberships

Sales Group	User Group	Research Group	Resulting Access
Change	Read	None specified	Change
Read	Read	Change	Change
None specified	Read	Denied	Denied
Full Control	Denied	None specified	Denied

The security concept of the *principle of least privilege* is connected to DAC. The principle of least privilege states that users should be granted only the minimum level of access that is necessary for them to perform their work tasks, and no more.

Role-Based Access Control (RBAC)

RBAC is another form of rules-based access control. It may be grouped with the nondiscretionary access control methods along with MAC. The rules used for RBAC are basically job descriptions: Users are assigned a specific role in an environment, and access to objects is granted based on the necessary work tasks of that role. For example, the role of backup operator may be granted the ability to back up every file on a system to a tape drive. The user given the backup operator role would then be able to perform that function.

RBAC is most suitable for environments with a high rate of employee turnover. It allows the job descriptions or roles to remain static even when the user performing that role changes often.



The acronym RBAC has a second definition. Rule-Based Access Control (RBAC) is typically used in relation to network devices that filter traffic based on filtering rules. Be sure you understand the context of the Security+ exam question before assuming *Role* or *Rule* when you see RBAC.

Exam Essentials

Mandatory Access Control (MAC) MAC is based on classification rules. Objects are assigned sensitivity labels. Subjects are assigned clearance labels. Users obtain access by having the proper clearance for the specific resource. Classifications are hierarchical.

Common MAC hierarchies Government or military MAC uses the following levels: unclassified, sensitive but unclassified, confidential, secret, and top secret. Private sector or corporate business environment MAC uses these: public, sensitive, private, and confidential.

Discretionary Access Control (DAC) DAC is based on user identity. Users are granted access through ACLs on objects, based on the discretion of the object's owner or creator.

Role-Based Access Control (RBAC) RBAC is based on job description. Users are granted access based on their assigned work tasks. RBAC is most suitable for environments with a high rate of employee turnover.

1.2 Identifying Authentication Methods

The full name of this section from the Security+ objectives list is “Recognize and be able to differentiate and explain the following methods of authentication.” *Authentication* is the mechanism by which a person proves their identity to a system. Often the authentication process involves a simple username and password. But other more complex authentication factors or credential-protection mechanisms are involved in order to provide strong protection for the logon and account-verification process.



For more information on this topic, refer to Chapter 1 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Authentication is little more than the process of proving that a subject is the valid user of an account. The authentication process requires that the subject provide an identity and then proof of that identity. Identity proofing typically takes the form of one or more of the following three authentication factors:

- *Something you know* (such as a password)
- *Something you have* (such as a smartcard)
- *Something you are* (such as a fingerprint)

This section discusses the specific authentication factors of passwords, tokens, and biometrics. In addition, it addresses the concepts of multi-factor and mutual authentication.

The topic of authentication also includes the protection mechanisms used to secure the authentication credentials (identity claim and identity proofs) while they're in transit from the client to the authentication server. Three such mechanisms are addressed here: Kerberos, CHAP, and certificates.

Kerberos

Early authentication transmission mechanisms sent logon credentials from the client to the authentication server in clear text. Unfortunately, this solution is vulnerable to eavesdropping and interception, thus making the security of the system suspect (if not decimating it). What was needed was a solution that didn't transmit the logon credentials in a form that could be easily captured, extracted, and reused.

One such method for providing protection for logon credentials is *Kerberos*: a trusted third-party authentication protocol that was originally developed at MIT under Project Athena. The current version of Kerberos in widespread use is version 5. Kerberos is used to authenticate network principles (subjects) to other entities on the network (objects, resources, and servers). Kerberos is platform independent; however, some operating systems require special configuration adjustments to support true interoperability (for example, Windows Server 2003 or Windows 2000 Server with Unix).

Kerberos is a centralized authentication solution. The core element of a Kerberos solution is the Key Distribution Center (KDC), which is responsible for verifying the identity of principles and granting and controlling access within a network environment through the use of secure cryptographic keys and tickets.

Kerberos is a trusted third-party authentication solution because the KDC acts as a third party in the communications between a client and a server. Thus, if the client trusts the KDC and the server trusts the KDC, then the client and server can trust each other.

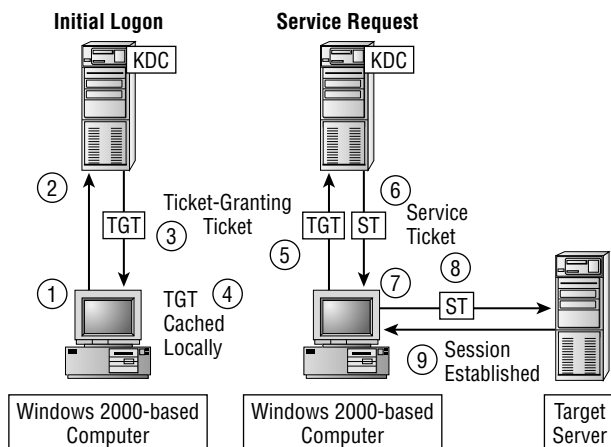
Kerberos is also a single sign-on solution. *Single sign-on* means that once a user (or other subject) is authenticated into the realm, they need not reauthenticate to access resources on any realm entity. (A *realm* is the network protected under a single Kerberos implementation.)

The basic process of Kerberos authentication is as follows:

1. The subject provides logon credentials.
2. The Kerberos client system encrypts the password with Data Encryption Standard (DES) and transmits the protected credentials to the KDC.
3. The KDC verifies the credentials and then creates a Ticket Granting Ticket (TGT—a hashed form of the subject's password with the addition of a timestamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.
4. The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.
5. The subject requests access to resources on a network server. This causes the client to request a Service Ticket (ST) from the KDC.
6. The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a timestamp that indicates its valid lifetime.
7. The client receives the ST.
8. The client sends the ST to the network server that hosts the desired resource.
9. The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

Figure 1.1 shows the Kerberos authentication process.

The Kerberos authentication method helps to ensure that logon credentials aren't compromised while in transit from the client to the server. The inclusion of a timestamp in the tickets ensures that expired tickets can't be reused. This prevents replay and spoofing attacks against Kerberos.

FIGURE 1.1 The Kerberos authentication process

Kerberos supports mutual authentication (client and server identities are proven to each other). It's scalable and thus able to manage authentication for large networks. Being centralized, Kerberos helps reduce the overall time involved in accessing resources within a network.



Kerberos is used to provide security and protection for authentication credentials alone. It isn't used in any way to provide encryption or security for other types of data transfer.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is an authentication protocol used primarily over dial-up connections (usually Point-to-Point Protocol [PPP]) as a means to provide a secure transport mechanism for logon credentials. It was developed as a secure alternative and replacement to Password Authentication Protocol (PAP), which transmitted authentication credentials in clear text.

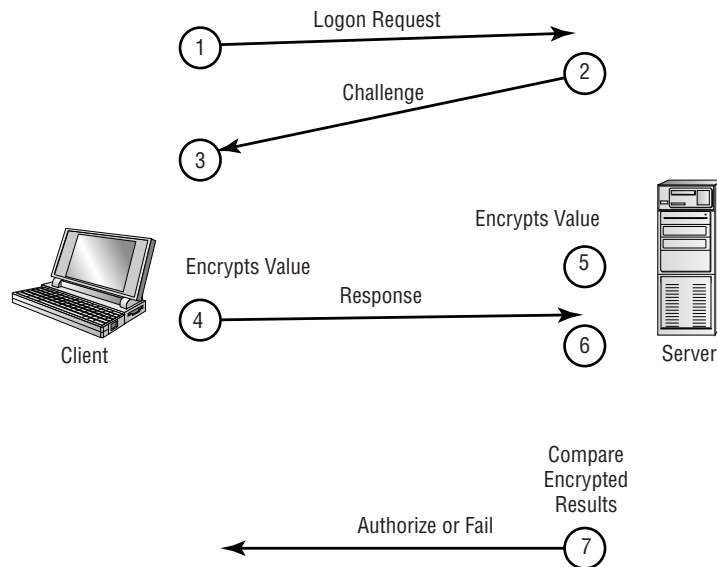
CHAP uses an initial authentication protection process to support logon and an ongoing verification process to ensure the subject/client is still who they claim to be. The process is as follows.

1. The initial authentication process performs a one-way hash function (specifically, MD5) on the subject's password and then passes the username and hash value to the authentication server.
2. The authentication server compares the username to its accounts database and the hash value to that stored for the identified user in its database.
3. If there is a match, the server transmits a challenge to the client.

4. The client produces the correct response and transmits it back to the server.
5. The server computes the response.
6. The server compares the response to that received by the client.
7. If everything matches, the subject is authenticated and allowed to communicate over the link.

Figure 1.2 shows the CHAP authentication process.

FIGURE 1.2 CHAP authentication



Once the client is authenticated, CHAP periodically sends a challenge to the client at random intervals. The client must compute the correct response to the issued challenge; otherwise the connection is automatically severed. This post-authentication verification process ensures that the authenticated session hasn't been hijacked.

Certificates

Certificates are another means of authentication. They typically involve a trusted third-party *certificate authority* (CA): a private or public entity that issues certificates to entities serving as either clients (subjects) or servers (objects). It's the responsibility of the CA to verify the identity of each entity before issuing a certificate. Once a certificate is issued, the entity can use the certificate as proof of their identity.

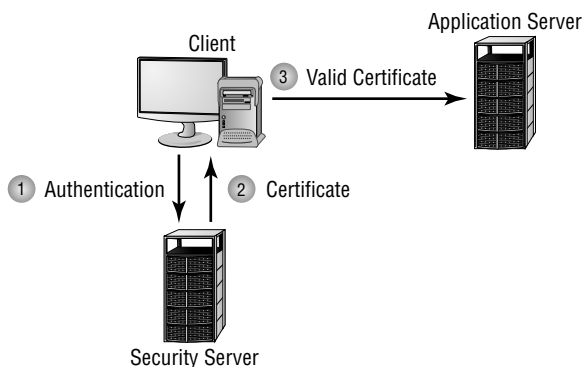
When you're using certificates in a private network, you are your own trusted third party (that is, you are your own CA). Such a private certificate solution is known as a Public Key

Infrastructure (PKI). A PKI is the definition (like a blueprint or schematic) of the mechanisms involved in implementing certificates. For the most part, you must deploy one or more servers with Certificate Services in order to create your own hierarchy of CAs.

Certificates can be used logically or electronically only (such as by the operating system or web browser directly) or via physical access control devices (such as a smartcard). In a logical deployment, certificates are installed into a client operating system or a specific application. Whenever identity proofing is required, the operating system transmits its certificate to the requesting party. In a physical deployment, the certificate is stored on a smartcard or some form of removable media. When the system needs user authentication, it requests the physical access control device.

When a user requests a certificate, they must usually provide proof of their identity along with their public key. This means they must use the same PKI solution as the CA issuing the certificate. The CA then uses the public key from the subject as the basis to generate the certificate returned to the user (see Figure 1.3). In this fashion, the certificate is tied to the subject's public key-private key pair and provides a mechanism for identity proofing.

FIGURE 1.3 A certificate being issued once identification has been verified



Certificates are commonly used over the Internet as a means of logical or electronic identity proofing. As long as both parties in a communication or transaction trust a specific third-party CA, such as VeriSign, then the two entities can trust that each is who they claim to be. It's very important to understand that a certificate only provides proof of identity, and that proof is based on trusting a third party (the CA that performed testing on the subject's identity). It in no way ensures that the subject or object so identified has benevolent motives or will function, perform, or operate in any specific manner.

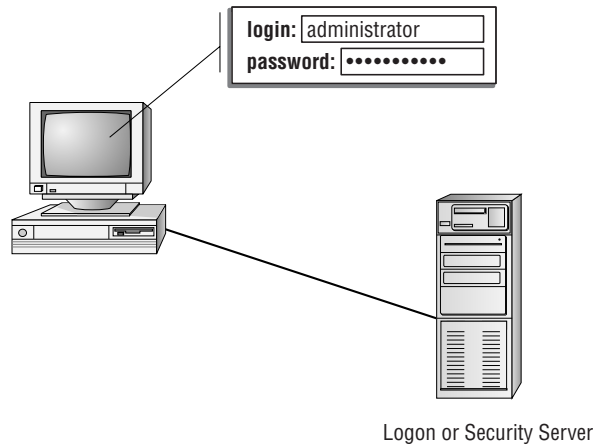


Certificates are discussed in more depth in Chapter 4, "Basics of Cryptography."

Username/Password

The combination of a username and a *password* is the most common form of authentication (see Figure 1.4). If the provided password matches the password stored in a system's accounts database for the specified user, then that user is authenticated to the system. However, just because using a username and password is the most common form of authentication, that doesn't mean it's the most secure. On the contrary, it's generally considered to be the least secure form of authentication.

FIGURE 1.4 A basic logon process employing a username and password



Numerous means to improve the basic username/password combination have been developed. First is the storage of passwords in an accounts database in an encrypted form. Typically that form is the hash value from a one-way hash function (see Chapter 4). Second is the use of an authentication protocol (or mechanism) that prevents the transmission of passwords in an easily readable form over a network or especially the Internet. Third, strong (complex) passwords are often enforced at a programmatic level. This is used to ensure that only passwords that are difficult for a password-cracking tool to discover are allowed by the system.

The strength of a password is generally measured in the amount of time and effort—that is, work—involved in breaking the password through various forms of cryptographic attacks. These attacks are collectively known as *password cracking* or *password guessing* (discussed in more depth in Chapter 4). A weak password invariably uses only alphanumeric characters; often employs dictionary or other common words; and may include user profile–related information such as birthdates, social security numbers, and pet names.

Strong passwords consist of numerous characters (8 or more); include at least three types of characters (uppercase, lowercase, numerals, and keyboard symbols); are changed on a regular basis (every 30 days); don't include any dictionary or common words or acronyms; and don't include any part of the subject's real name, user name, or e-mail address.

Passwords should be strong enough to resist discovery through attack but easy enough for the person to remember. This can sometimes be a difficult line to walk.

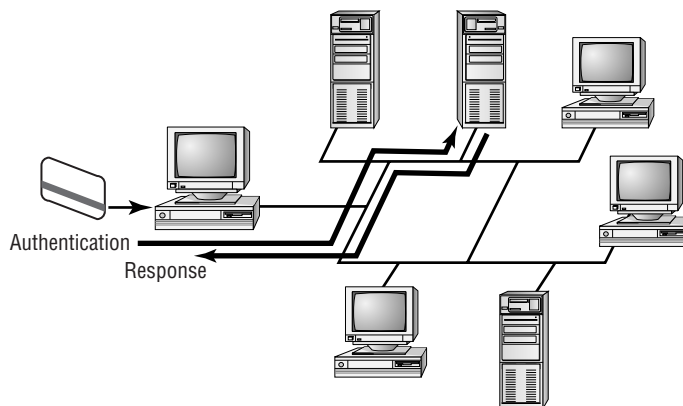
Tokens

A *token* is a form of authentication factor that is something you have. It's usually a hardware device, but it can be implemented in software. A token is used to generate temporary single-use passwords for the purpose of creating stronger authentication. In this way, a user account isn't tied to a single static password. Instead, the user must be in physical possession of the password-generating device. The user enters the currently valid password from the token as their password during the logon process.

There are several forms of tokens. Some generate passwords based on time, whereas others generate passwords based on challenges from the authentication server. In either case, the user can use (or attempt to use) the generated password just once before they must either wait for the next time window or request another challenge. Passwords that can only be used once are known as *one-time passwords*. This is the most secure form of password, since regardless of whether its use results in a successful logon, that one-use password is never valid again for reuse. One-time passwords can only be employed when a token device is used, due to the complexity and ever-changing nature of the passwords.

A token may be a device like a small calculator with or without a keypad. It may also be a high-end smartcard (see Figure 1.5). When properly deployed, a token-based authentication system is more secure than a password-only system.

FIGURE 1.5 The smartcard authentication process



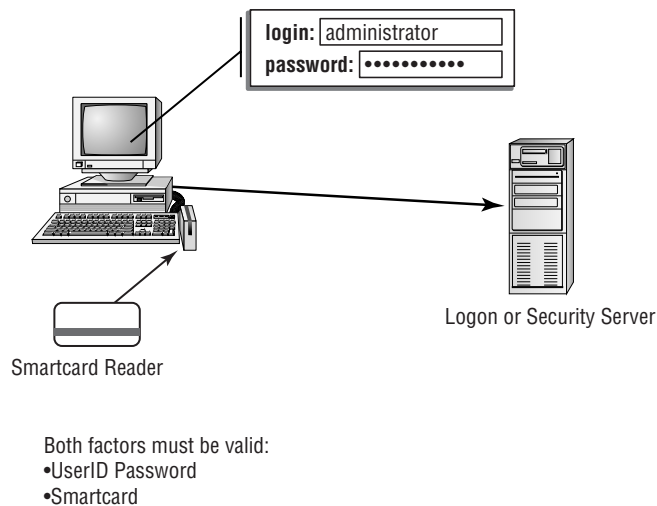
Multi-Factor Authentication

Multi-factor authentication is the requirement that a user must provide two or more authentication factors in order to prove their identity. There are three generally recognized categories of authentication factors:

- Something you know (such as a password)
- Something you have (such as a token)
- Something you are (such as a biometric)

When two different authentication factors are used, this is known as *two-factor authentication* (see Figure 1.6). If two of the same authentication factors are used, this is known as *strong authentication*. Whenever different factors are used (whether two or three), this is always a more secure solution than any number of the same authentication factors. This is due to the fact that with two or more different factors, two or more different types of attacks must take place in order to steal or capture the authentication factor itself. With strong authentication, even if 10 passwords are required, only a single type of password-stealing attack needs to be waged to break through the authentication security.

FIGURE 1.6 Two-factor authentication



Mutual Authentication

Mutual authentication is two-way authentication. The subject (user) authenticates to the object (server), and the object (server) authenticates back to the subject (user). In this way, both ends of the communication have proof of the identity of the other partner.

Biometrics

Biometrics is the term used to describe the collection of physical attributes of the human body that can be used as authentication factors. Biometrics fall into the authentication factor category of “something you are”: You, as a human, have the element of identification as part of your physical body. Biometrics include fingerprints, palm scans (use of the entire palm as if it were a fingerprint), hand geometry (geometric dimensions of the silhouette of a hand), retinal scans (pattern of blood vessels at the back of the eye), iris scans (colored area of the eye around the pupil), facial recognition, voice recognition, signature dynamics, and keyboard dynamics.

Although biometrics are a stronger form of authentication than passwords alone, biometrics in and of themselves aren't the best solution. Even with biometrics, implementing multi-factor authentication is the most secure solution.

Exam Essentials

Kerberos Kerberos is a trusted third-party authentication protocol. It uses encryption keys as tickets with timestamps to prove identity and grant access to resources. Kerberos is a single sign-on solution employing a Key Distribution Center (KDC) to manage its centralized authentication mechanism.

Challenge Handshake Authentication Protocol (CHAP) CHAP is an authentication protocol used primarily over dial-up connections (usually PPP) as a means to provide a secure transport mechanism for logon credentials. CHAP uses a one-way hash to protect passwords and periodically reauthenticates clients.

Certificates Certificates are an electronic means of proving subject and object identity. They are issued by certificate authorities (CAs).

Passwords Passwords are the most common form of authentication, but they're also the weakest. Passwords can be improved through the use of strong password policies enforced by software.

Tokens Tokens are a "something you have" type of authentication factor. They support one-time passwords, which are the most secure form of passwords.

Multi-factor authentication Multi-factor authentication is the requirement that a user must provide two or more authentication factors in order to prove their identity.

Mutual authentication Mutual authentication is two-way authentication. The subject (user) authenticates to the object (server), and the object (server) authenticates back to the subject (user).

Biometrics Biometrics is the collection of physical attributes of the human body that can be used as authentication factors ("something you are"). Biometrics include fingerprints, palm scans (use of the entire palm as if it were a fingerprint), hand geometry (geometric dimensions of the silhouette of a hand), retinal scans (pattern of blood vessels at the back of the eye), iris scans (colored area of the eye around the pupil), facial recognition, voice recognition, signature dynamics, and keyboard dynamics.

1.3 Identifying Non-Essential Services

The full name of this section from the Security+ objectives list is "Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols." It's important to realize that a key element in securing a system is to reduce its attack surface. The *attack surface* is the area that is exposed to untrusted networks or entities and that is vulnerable to attack. If a system is hosting numerous services and protocols, then its attack surface is larger than that of a system running only essential services and protocols.



For more information on this topic, refer to Chapter 1 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

It's tempting to install every service, component, application, and protocol available to you on every computer system you deploy. However, this temptation is in direct violation of a security best practice stating that you should have each system host only those services and protocols that are absolutely essential to its mission-critical operations.

The real issue is that software isn't trusted. Software is what services, applications, components, and protocols are; unfortunately, software is written by people and therefore in all likelihood isn't perfect. But even if software was without bugs, errors, oversights, mistakes, and so on, it would still represent a security risk. Software that is working as expected can often still be exploited by a malicious entity. Therefore, every instance of software deployed onto a computer system represents a collection of additional vulnerability points that may be exposed to external, untrusted, and possibly malicious entities.

From this perspective, you should understand that all non-essential software elements should be removed from a system before it's deployed on a network, especially if that network has Internet connectivity. But how do you know what is essential and what isn't? Here is a basic methodology:

1. Plan the purpose of the system.
2. Identify the services, applications, and protocols needed to support that purpose. Make sure these are installed on the system.
3. Identify the services, applications, and protocols that are already present on the system. Remove all that aren't needed.

Often, you won't know if a specific service that appears on a system by default is needed. Thus, a trial-and-error test is required. If software elements aren't clearly essential, disable them one by one and test the capabilities of the system. If the system performs as you expect, the software probably isn't needed. If the system doesn't perform as expected, then the software will need to be re-enabled. This process is known as application and system hardening.



Application and system hardening is discussed in greater detail in Chapter 3, "Infrastructure Security."

You may discover that some services and protocols offer features and capabilities that aren't necessary to the essential functions of your system. If so, find means to disable or restrict those characteristics. This may include restricting ports or reconfiguring services through a management console.

The essential services on a system are usually easy to identify; they generally have recognizable names that correspond to the function of the server. However, you must determine which services are essential on your specific system. Services that are essential on a web server may not be essential on a file server or an e-mail server. Some examples of possible essential services include the following:

- File sharing
- E-mail
- Web
- File Transfer Protocol (FTP)
- Telnet
- Remote access
- Network news (Network News Transfer Protocol [NNTP])
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Non-essential services are more difficult to identify. Just because a service doesn't have the same name as an essential function of your server doesn't mean that it isn't used by the underlying operating system or as a support service. It's extremely important to test and verify whether any service is being depended on by an essential service. However, several services are common candidates for non-essential services that you may want to locate and disable first (assuming you follow the testing method described earlier). These may include:

- NetBIOS
- Unix RPC
- Network File System (NFS)
- X services
- R services
- Telnet
- FTP
- Trivial File Transfer Protocol (TFTP)
- NetMeeting
- Instant messaging
- Remote control software
- Simple Network Management Protocol (SNMP)

Exam Essentials

Security risks of non-essential software Non-essential software increases the attack surface of your systems. Removing every element of software that isn't required will improve the security of a system.

1.4 Identifying Attack Methods

The full name of this section from the Security+ objectives list is “Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk.” The rate at which systems connected to networks are attacked is increasing at an alarming rate. Systems that aren’t even connected to the Internet, but just to a private network, may come under attack. There are myriad ways to attack a computer system. Your familiarity with a small collection of these attacks and how to respond to them is an essential skill for the Security+ exam.



For more information on this topic, refer to Chapters 2 and 7 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Any computer system connected to any type of network is subject to various methods of attack. The following section discusses common attack methods.

Denial of Service/Distributed Denial of Service (DOS/DDOS) Attacks

Denial of Service (DoS) is a form of attack that has the primary goal of preventing the victimized system from performing legitimate activity or responding to legitimate traffic. There are two basic types of DoS attack. The first form exploits a weakness, error, or standard feature of software to cause a system to hang, freeze, consume all system resources, and so on. The end result is that the victimized computer is unable to process any legitimate tasks. The second form floods the victim’s communication pipeline with garbage network traffic. The end result is that the victimized computer is unable to send or receive legitimate network communications. In either case, the victim has been denied the ability to perform normal operations (services).

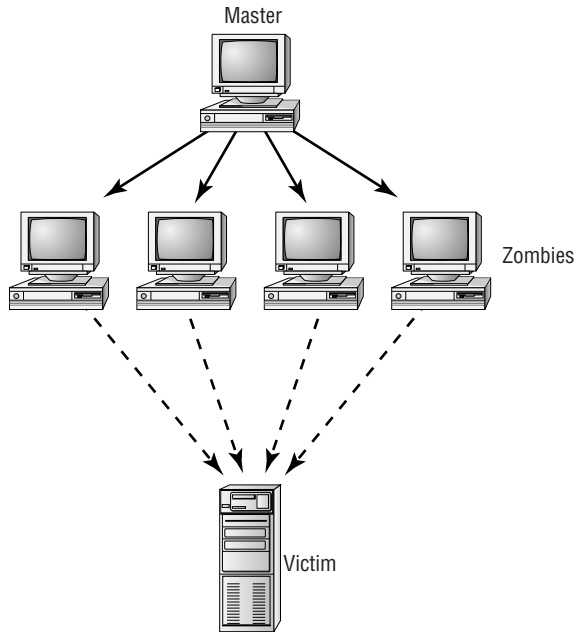
DoS isn’t a single attack but rather an entire class of attacks. Some attacks exploit flaws in operating system software, whereas others focus on installed applications, services, or protocols. Some attacks exploit specific protocols, including Internet Protocol (IP), *Transmission Control Protocol (TCP)*, *Internet Control Message Protocol (ICMP)*, and *User Datagram Protocol (UDP)*.

DoS attacks typically occur between one attacker and one victim. However, they don’t have to be waged in that simple a manner. Most DoS attacks employ some form of intermediary system (usually an unwilling and unknowing participant) in order to hide the attacker from the victim. For example, if an attacker sends attack packets directly to a victim, then it’s possible for the victim to discover who the attacker is. This is made more difficult, although not impossible, through the use of spoofing (discussed later in this chapter).

Many DoS attacks are waged by first compromising or infiltrating one or more intermediary systems that serve as launch points, or attack platforms. The attacker installs remote-control tools, often called *bots*, *zombies*, or *agents*, onto these systems. Then, at an appointed time or in response to a launch command from the attacker, the DoS attack is conducted against the victim. In this manner, the victim may be able to discover the one or many zombied systems that are

causing the DoS attack but probably won't be able to track down the actual attacker. This form of attack involving zombied systems is known as Distributed Denial of Service (DDoS), as shown in Figure 1.7.

FIGURE 1.7 Distributed Denial of Service attack

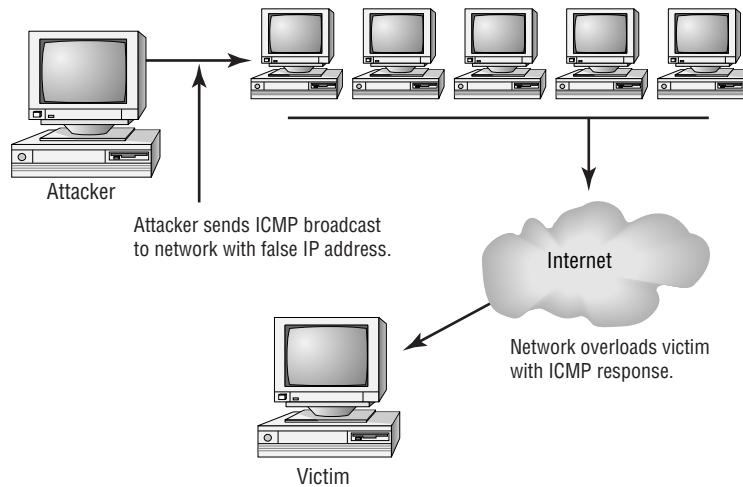


There is a third level of DoS known as Distributed Reflective Denial of Service (DRDoS). This form of attack employs an *amplification* or *bounce* network that is an unwilling and unknowing participant but that has unfortunately left on its ability to receive broadcast messages and create message responses, echoes, or bounces. In effect, the attacker sends spoofed message packets to the amplification network's broadcast address. This causes each single inbound received packet to be distributed to all the hosts inside that network (which could be in the 10,000 or 100,000 range). Each host then responds to each packet, but since the source of the original packet was falsified, the response goes to the victim instead of the true sender (the attacker). So, what originated from the attacker as a single packet is transformed into numerous packets exiting the amplification network and ultimately flooding the victim's communication link.

There are numerous specific DoS, DDoS, and DRDoS attack tools and methods. Here are a few that you should be able to recognize:

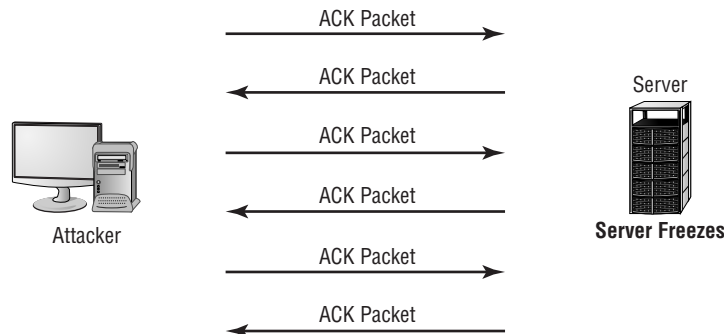
Smurf This form of DRDoS uses Internet Control Message Protocol (ICMP) echo reply packets (ping packets). See Figure 1.8 for an example.

Fraggle This form of DRDoS uses User Datagram Protocol (UDP) packets directed to port 7 (echo port) or 19 (chargen [character generator] port).

FIGURE 1.8 A smurf attack underway against a network

SYN flood This type of attack is an exploitation of a TCP three-way handshake. Every TCP session starts with the client sending a SYN (synchronize) packet to a server, the server responding with a SYN/ACK (synchronize/acknowledgment) packet, and the client sending a final ACK packet. The attack consists of the attacker serving as a client and sending numerous SYN packets but never any final ACK packets. This causes the server to consume all system resources opening incomplete communication sessions. Figure 1.9 shows an example of a TCP SYN flood attack.

Teardrop Numerous partial IP packets are sent to a victim with overlapping sequencing and offset values. The victim attempts to assemble complete IP packets from the received partials, but the fragments overwrite each other and may produce a packet of an invalid size. This causes the victim to freeze or crash.

FIGURE 1.9 TCP SYN flood attack

Land attack Numerous SYN packets are sent to the victim with source and destination addresses spoofed as the victim's address. The victim is confused because it's unable to respond to a packet it sent to itself that it has no record of sending. This often results in a freeze or crash.

Ping flood The attacker sends numerous ping echo requests to a victim. The victim responds with the echo. If enough inbound and outbound packets are transmitted, no legitimate traffic will be able to use the communication link.

Ping of death The attacker sends oversized ping packets to the victim; the victim doesn't know how to handle invalid packets, and it freezes or crashes.

Bonk The attacker sends a corrupt UDP packet to DNS port 53. This type of attack may cause Windows systems to crash.

Boink The same as Bonk, but the corrupt UDP packets are sent to numerous ports. The result may cause a Windows system to crash.

Fortunately, most of the basic DoS attacks that exploit error-handling procedures (such as ping of death, land attack, teardrop, bonk, boink, and so on) are now automatically handled by improved versions of the protocols installed in the operating system. However, most of the DDoS and DRDoS attacks aren't as easy to safeguard against. SYN flood, teardrop, land attack, ping flood, ping of death, bonk, and boink are typically labeled DoS attacks, but they can be waged as a DDoS if the attacker compromises several intermediary systems and uses those as launching points to attack the victim.

Some countermeasures and safeguards against these attacks include the following:

- Adding firewalls, routers, and intrusion detection systems (IDSs) that detect DoS traffic and automatically block the port or filter out packets based on the source or destination address
- Disabling echo replies on external systems
- Disabling broadcast features on border systems
- Blocking spoofed packets from entering or leaving your network
- Keeping all systems patched with the most current security updates from vendors

Back Door Attacks

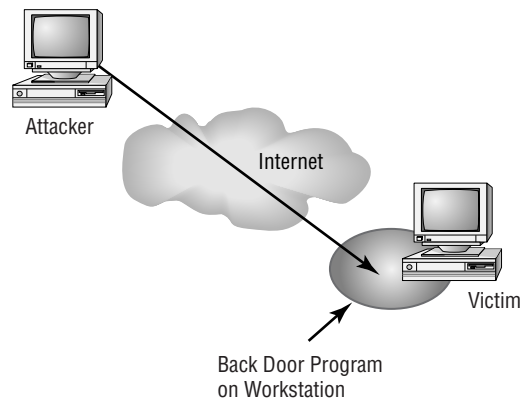
The term *back door* can refer to two types of problems or attacks on a system. The first and oldest meaning of back door was a developer-installed access method that bypassed all security restrictions. The back door was a special hard-coded user account, password, or command sequence that allowed anyone with knowledge of the access hook (sometimes called a *maintenance hook*) to enter the environment and make any changes. This sounds great from a developer's perspective, especially during the coding and debugging process. Unfortunately, such programming shortcuts are often overlooked when the product nears completion; thus, they end up in the final product. Fortunately, once a back door is discovered in a released product, the vendor usually releases a patch to remove the back door code from the installed product. The possible presence of back doors is another good reason to stay current with vendor-released updates and patches.

The second meaning of *back door* is a hacker-installed remote access client. These small, maliciously purposed tools can be easily deposited on a computer through a Trojan horse, a

virus, or a website mobile code download, or even as part of an intrusion activity. Once active on a system, they open up access ports and wait for an inbound connection. Thus, a back door serves as an access portal for a hacker so they can bypass any security restrictions and gain (or regain) access to a system. Some common back door tools include Back Orifice, NetBus, and Sub7 (all of which function on Windows). These and other common back door tools are detected and removed by virus scanners and spy-ware scanning tools.

Figure 1.10 shows a back door attack in progress.

FIGURE 1.10 A back door attack in progress



Preemptive measures against back doors include the following:

- Restricting mobile code from being automatically downloaded to your systems
- Using software policies to prevent unauthorized software from being installed
- Requiring software and driver signing

Spoofing Attacks

Spoofing is the act of falsifying data. Usually the falsification involves changing the source address of network packets. As a result of the changed source address, victims are unable to locate the true attackers or initiators of a communication. Also, by spoofing the source address, the attacker redirects responses, replies, and echoes to packets to some other system (such as in the case of smurf, fraggle, and land DoS attacks).

Spoofing is also a common activity for unsolicited e-mail, commonly known as spam. Spoofed e-mail means that you're unable to reply to the e-mail or determine where it originally came from.

There are innumerable forms of spoofing attacks. Spoofing can be used to redirect packets, bypass traffic filters, steal data, perform social engineering attacks, and even falsify websites.

Countermeasures against spoofing attacks include the following:

- Using e-mail spam and spoofing filters

- Dropping all inbound packets received by border systems that have a source destination from inside your private network (this indicates spoofing)
- Dropping all outbound packets received by border systems that have a source destination from outside your private network (this also indicates spoofing)

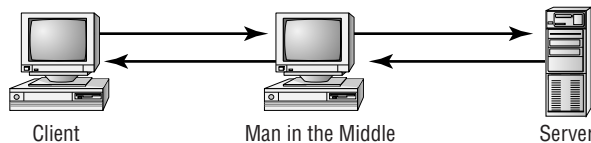
Man-in-the-Middle Attacks

A *man-in-the-middle attack* is a form of communications eavesdropping attack. Attackers position themselves in the communication stream between a client and server (or any two communicating entities). The client and server believe that they are communicating directly with each other; they may even have secured or encrypted communication links. However, the attacker can access and even modify the communications.

Waging a man-in-the-middle attack is complex. It involves altering network traffic and possibly poisoning name-resolution systems (such as DNS or WINS) in order to fool the client into perceiving the attacker as the server and to fool the server into perceiving the attacker as the client. Once that charade is successful, the client will submit their logon credentials to the fake server (the masked attacker), which in turn sends the credentials to the actual server while masquerading as the actual client. As a result, the client establishes a communication link (maybe even an encrypted link) with the attacker, and the attacker establishes a communication link with the server. As data is transmitted in either direction between the true client and server systems, the attacker can read and access all the data and can choose to modify the traffic to further the subterfuge.

Figure 1.11 shows a man-in-the-middle attack.

FIGURE 1.11 A man-in-the-middle attack occurring between a client and a web server



Such attacks are usually most successful when routing and name resolution systems are first compromised in order to position the attacker before the client-to-server communication is initiated. However, man-in-the-middle attacks can be conducted against existing client-server communication links (usually assuming they aren't encrypted). This second form of attack is much more difficult due to existing routing, name resolution, TCP sequencing, and the speed of the communication. However, several tools exist that perform the necessary operations against both sides of the communication connection in order to implement a man-in-the-middle injection. Some of these tools include Juggernaut, T-Sight, and Hunt.

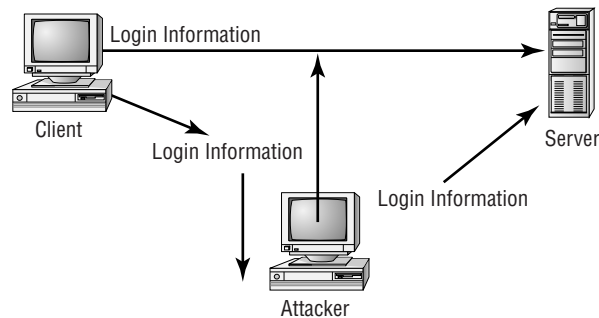
Countermeasures to man-in-the-middle attacks include strong encryption protocols, such as IPSec, and the use of strong authentication, such as Kerberos, certificates, multi-factor authentication, and mutual authentication.

Replay Attacks

A *replay attack* is just what it sounds like: An attacker captures network traffic and then replays the captured traffic in an attempt to gain unauthorized access to a system. Most commonly, the attacker focuses on network traffic that is the exchange between a client and server performing authentication. If an attacker can capture the authentication traffic—especially the packets containing the logon credentials, even if they are more than just username and password (such as certificates, token responses, or biometric values)—then a replay attack may grant the attacker the ability to log on to a system by retransmitting the captured packets.

Figure 1.12 shows a replay attack.

FIGURE 1.12 A replay attack occurring



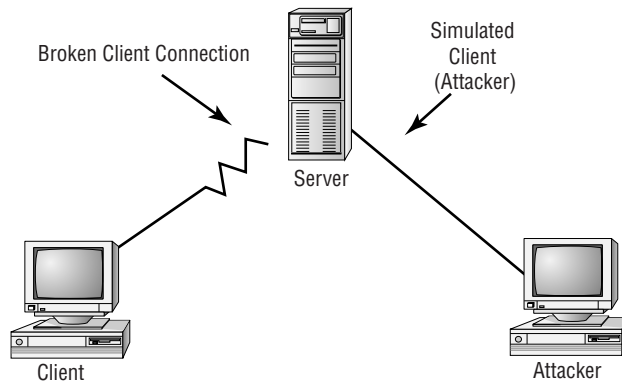
If a replay attack succeeds, then the attacker gains the same level of access as the user that originally submitted the authentication information. Fortunately, most modern operating systems, networks, protocols, services, and applications use various replay protection mechanisms to directly prevent such attacks. Two of the most common countermeasures are packet sequencing and timestamps. Packet sequencing ensures that any packet received that isn't in the proper order (or within a reasonable margin) is dropped and ignored. Packet timestamps ensures that any packet received outside of a specific time window is dropped and ignored.

TCP/IP Hijacking Attacks

TCP/IP hijacking is a form of attack where the attacker takes over an existing communication session. The attacker can take over the role of the client or the server, depending on the purpose of the attack. Session hijacking is a simpler one-sided form of man-in-the-middle attack. Many of the same tools and techniques are used in both forms of attack. However, with a session hijacking, the other partner in the communication is disconnected—they're aware that they are no longer communicating and that their session was interrupted. However, they may not immediately realize that they were the collateral damage in a session hijacking attack.

Figure 1.13 shows a TCP/IP hijacking attack.

Countermeasures to TCP/IP hijacking attacks include using encrypted protocols and performing reauthentication during a session.

FIGURE 1.13 TCP/IP hijacking attack

Weak Keys

Weak keys isn't an attack but rather a vulnerability in how a cryptography system is used that makes various types of attacks possible. The term *weak keys* implies that the cryptographic key selected to encrypt a file or a communication session is either too short or too easily guessed. Weak keys are generally anything less than 64 bits in length. As a result of weak keys, attackers have an easier time cracking encrypted communications because they have to try fewer possible permutations during a full brute-force attack than they would for strong keys (those at least 128 bits long). In general, you should avoid using weak keys by only using cryptography solutions that use longer, stronger keys.



For more information on keys and cryptography, see Chapter 4.

Mathematical Attacks

Mathematical attacks are a specific type of attacks against cryptography. They're directed against the algorithm in an attempt to exploit the arithmetic it employs. The goal of a mathematical attack is to either decrypt an encrypted message or to discover the key used for encryption.



For more information on cryptography and related attacks, see Chapter 4.

Social Engineering

Social engineering is mentioned twice in the first domain of the Security+ exam objectives list. We discuss it later in this chapter, in the section "1.6 Understanding Social Engineering."

Birthday Attacks

A *birthday attack* is used against a specific form of cryptography called hashing. The birthday attack gets its name from a bar bet that exploits the mathematical probability of shared birthdays: It takes only 46 people in a room for there to be a greater than 50 percent probability that any two of those people share the same birthday. (The bar bet is that you'll drink for free if two people in the bar share a birthday; otherwise you'll buy the house a round of drinks.)

Hashing is a one-way function that creates a fixed-length output (known as the hash, hashing value, fingerprint, message digest, and so on) from an input of any length. A hash serves as an ID code to detect when the original data source has been altered, since no two data sources produce the same hash.

The birthday attack exploits a mathematical property that states that if the same mathematical function is performed on two values and the result for each is the same, then the original values are the same. This concept is often represented with the following syntax:

$f(M)=f(M')$ therefore $M=M'$

Birthday attacks can be waged against any use of hashing. However, they're most commonly employed during password-guessing attacks (discussed in the following section). In a password-guessing attack, a program compares possible passwords with passwords stored in an accounts database. But passwords stored in an accounts database are secured because only their hash values are stored there. Thus, the password-cracking program first performs the same hashing function used by the secured system on each possible password before scanning the accounts database for a match. If a match is found, then the password-guessing tool has discovered a password based on the $f(M)=f(M')$ property. This is more specifically known as *reverse hash matching*.



For more information on cryptography and related attacks, see Chapter 4.

Password-Guessing Attacks

Password guessing is an attack aimed at discovering the passwords employed by user accounts. Password guessing is often called password *cracking*. There are several forms of password-guessing attack tools: Some attempt to guess passwords by attacking a logon prompt, others try to extract passwords directly from an accounts database, and others attempt to capture authentication traffic and extract passwords out of the network packet. In most cases, the latter two options employ birthday attack (reverse hash matching) methods to discover the password used by a user account.

There are innumerable password-guessing tools on the Internet. However, they can be distilled into two primary categories based on the method used to select possible passwords for a direct logon prompt or birthday attack procedure: brute force and dictionary.

No matter what tool is used to discover passwords, the most important countermeasure against password crackers is to use complex passwords and change them on a regular basis. See the discussion in the section “Username/Password” for details on strong passwords.

Brute Force

A *brute-force* attack is designed to try every possible valid combination of characters to construct possible passwords in the attempt to discover the specific passwords used by user accounts. Brute-force attacks rarely begin at 0000001 or 000000a but rather take a statistical probability approach to the selection of possible passwords. Most noncomplex passwords under 8 characters long can be discovered in less than 30 minutes.

Longer and more complex passwords make brute-force attacks less successful. However, given enough time, a brute-force attack will always succeed. Thus, regularly changing a password will thwart the use of any discovered old passwords.

Dictionary

A *dictionary attack* performs password guessing by using a preexisting list of possible passwords. Password lists can include millions of possible passwords. Often password lists or dictionaries are constructed around topics. Thus, if an attacker knows basic information about you as a person, they can attempt to exploit human nature's propensity to select passwords using words common or familiar to you. For example, if an attacker knows that you work in the medical industry, you have cats, and you enjoy sailing, they can select password dictionaries that include words, acronyms, and phrases common to those issues.

Dictionary attacks are surprisingly effective against users who have not been trained in the methods and skills of creating complex passwords.

Software Exploitation Attacks

Software exploitation attacks are directed toward known flaws, bugs, errors, oversights, or normal functions of the operating system, protocols, services, or installed applications. One of the most common forms of software exploitation is a buffer overflow attack.



Buffer overflow attacks are discussed in detail in Chapter 2, "Communication Security."

A buffer overflow attack occurs when an attacker submits data to a process that is larger than the input variable is able to contain. Unless the program is properly coded to handle excess input, the extra data is dropped into the system's execution stack and may execute as a fully privileged operation. Buffer overflow attacks can result in system crashes, corrupted data, user privilege escalation, or just about anything a hacker can think of. The only countermeasures to buffer overflow attacks are to patch the software when issues are discovered and to properly code software to perform input validation checks before accepting input for processing.

Once a weakness is discovered in software, a hacker often writes an exploit or attack tool. These tools are easily accessible on the Internet. They then allow anyone to grab the tool and point it at a victim to perform the attack, even when the attacker has no knowledge of how to perform the attack.

Exam Essentials

Denial of Service attacks Denial of Service (DoS) is a form of attack that has the primary goal of preventing the victimized system from performing legitimate activity or responding to legitimate traffic. There are two basic types of DoS attack. The first form exploits a weakness, error, or standard feature of software on the victim system to cause the system to hang, freeze, consume all system resources, and so on. The second form floods the victim's communication pipeline with garbage network traffic.

Examples of DoS attacks Examples of DoS include smurf, fraggle, SYN flood, teardrop, land, ping flood, ping of death, bonk, and boink.

Back door attacks The term *back door* can refer to two types of problems or attacks on a system: a developer-installed access method that bypasses any and all security restrictions, or a hacker-installed remote access client.

Spoofing attacks Spoofing is the act of falsifying data. Usually the falsification involves changing the source address of network packets. Because the source address is changed, victims are unable to locate the true attackers or initiators of a communication. Also, by spoofing the source address, attackers redirect responses, replies, and echoes to packets to some other system.

Man-in-the-middle attacks A man-in-the-middle attack is a form of communications eavesdropping attack. Attackers position themselves in the communication stream between a client and server (or any two communicating entities). The client and server believe that they are communicating directly with each other.

Replay attacks In a replay attack, an attacker captures network traffic and then replays the captured traffic in an attempt to gain unauthorized access to a system.

TCP/IP hijacking attacks TCP/IP hijacking is a form of attack where the attacker takes over an existing communication session.

Weak keys Weak keys isn't an attack but rather a weakness in how a cryptography system is used that makes various types of attacks possible. Weak keys implies that the cryptographic key selected to encrypt a file or a communication session is either too short or too easily guessed. Weak keys are generally anything less than 64 bits in length.

Mathematical attacks Mathematical attacks are direct against the algorithm in an attempt to exploit the arithmetic it employs.

Birthday attacks The birthday attack exploits a mathematical property that states that if the same mathematical function is performed on two values and the result is the same, then the original values are the same. This concept is often represented with the syntax $f(M)=f(M')$ therefore $M=M'$.

Password guessing Password guessing is an attack aimed at discovering the password employed by user accounts. It's often called password cracking. There are two primary categories of

password-guessing tools, based on the method used to select possible passwords for a direct logon prompt or birthday attack procedure: brute force and dictionary.

Software exploitation Software exploitation attacks are directed toward known flaws, bugs, errors, oversights, or normal functions of the operating system, protocols, services, or installed applications. One of the most common forms of software exploitation is a buffer overflow attack.

1.5 Identifying Malicious Code

The full name of this section from the Security+ objectives list is “Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk.” Knowing how to recognize and respond to malicious code is an essential skill in today’s networking environments.



For more information on this topic, refer to Chapter 2 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Malicious code is any element of software that performs an unwanted or undesired function from the perspective of the legitimate user or owner of a computer system. This section explores four specific types of malicious code.

Viruses

Viruses get their name from their biological counterparts. They are programs that are designed to spread from one system to another through self-replication and to perform any of a wide range of malicious activities. The malicious activities performed by viruses include data deletion, corruption, alteration, and theft. Some viruses replicate and spread so rapidly that they consume system and network resources, thus performing a type of DoS attack.

Most viruses need a host to latch onto. The host can be a file or a sector of a hard drive. Viruses that attach themselves to the boot sector of a hard drive and thus are loaded in memory when the drive is activated are known as *boot sector viruses*. *Polymorphic viruses* have the ability to alter their own code in order to avoid detection by antivirus scanners. *Macro viruses* live within documents or e-mails and exploit the scripting capabilities of productivity software.

The best countermeasure to viruses is an antivirus scanner, which is updated regularly and which monitors all local storage devices, memory, and communication pathways for viral activities. Other countermeasures include avoiding downloading software from the Internet, not opening e-mail attachments, and avoiding the use of removable media from other environments.

Trojan Horses

A *Trojan horse* is a form of malicious software that is disguised as something useful or legitimate. The most common forms of Trojan horses are games and screen savers, but any software can be made into a Trojan horse. The goal of a Trojan horse is to trick a user into installing it on their computer. This allows the malicious code portion of the Trojan horse to gain access to the otherwise secured environment. Some of the most common Trojan horses are tools that install DoS zombies onto systems.

Countermeasures for Trojan horses are the same as for viruses.

Logic Bombs

A *logic bomb* is a form of malicious code that remains dormant until a triggering event occurs. The triggering event can be a specific time and date, the launching of a specific program, or the accessing of a specific URL (such as your online banking logon page). Logic bombs can perform any malicious function the programmer wishes, from causing system crashes to deleting data to altering configurations to stealing authentication credentials.

Countermeasures for logic bombs are the same as for viruses.

Worms

Due to the expanding capabilities (although malicious) of viruses, *worms* are no longer an easily identifiable distinct category of malicious code. Worms are designed to exploit a single hole in a system (operating system, protocol, service, or application) and then use that flaw to spread themselves to other systems with the same flaw. Worms may be used to deposit viruses, Trojan horses, or logic bombs, or they may perform direct virus-like maelstrom activities on their own.

Countermeasures for worms are the same as for viruses with the addition of keeping systems patched.

Exam Essentials

Viruses Viruses are programs that are designed to spread from one system to another through self-replication and to perform any of a wide range of malicious activities.

Trojan horses A Trojan horse is a form of malicious software that is disguised as something useful or legitimate.

Logic bombs A logic bomb is a form of malicious code that remains dormant until a triggering event occurs. The triggering event can be a specific time and date, the launching of a specific program, or the accessing of a specific URL (such as your online banking logon page).

Worms Worms are designed to exploit a single flaw in a system (operating system, protocol, service or application) and then use that hole to replicate itself to other systems with the same flaw.

Malicious code countermeasures The best countermeasure to viruses and other malicious code is an antivirus scanner, which is updated regularly and which monitors all local storage devices, memory, and communication pathways for viral activities. Other countermeasures include avoiding downloading software from the Internet, not opening e-mail attachments, and avoiding the use of removable media from other environments.

1.6 Understanding Social Engineering

The full name of this section from the Security+ objectives list is “Understand the concept of and know how reduce the risks of social engineering.” No matter how much technical protection has been deployed in an environment, there will always be a known weakness: people. *Social engineering* is a class of attacks directed toward people. Unless you can remove all personnel from your environment, you’ll have to deal with social-engineering attacks.



For more information on this topic, refer to Chapter 2 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Social engineering is a unique type of attack that attempts to exploit human behavior. Social-engineering attacks can take many forms, from skillfully worded websites to clever e-mail messages to personnel impersonations over the phone to face-to-face acting. In just about every case, a social-engineering attack tries to convince the victim to perform some activity or reveal a piece of information that they shouldn’t.

Any form of advertisement could be considered a form of social-engineering attack—ads appeal to you in an attempt to get you to purchase or use a product or service. Although an advertisement’s motivation is profit, most social-engineering attacks’ motives are more malevolent. Here are some example scenarios of common social-engineering attacks:

- You receive an e-mail warning you about a dangerous new virus spreading across the Internet. The message tells you to look for a specific file on your hard drive and delete it, since it indicates the presence of the virus. Often, however, the identified file is really an essential file needed by your system.
- A website claims to offer free temporary access to its products and services, but it requires that you alter the configuration of your Web browser and/or firewall in order to download the access software.
- A secretary receives a phone call from a person claiming to be a client who is running late to meet the CEO. She asks for the CEO’s private cell phone numbers so she can call him.
- The Help Desk receives a call from an outside line. The caller claims to be a manager of a department who is currently involved in a sales meeting in another city. He claims he forgot his password and needs it to be reset so that he can log in remotely to download his essential presentation.
- Someone who looks like an A/C repairman enters the office and claims a service call was received for a malfunctioning unit in the building. He is sure the unit can be accessed from inside your office work area, and he asks to be given free roam to repair the A/C system.

These are just a few examples of possible social-engineering attacks. These may also be legitimate and benign occurrences, but you can see how they could mask the motives and purposes of an intentional attacker.

Methods to protect against social engineering include the following:

- Training personnel about social-engineering attacks and how to recognize common signs
- Requiring authentication when performing activities for personnel over the phone
- Defining restricted information that is never communicated over the phone
- Always verifying the credentials of a repair person and verifying that a real service call was placed by authorized personnel
- Never following the instructions of an e-mail without verifying the information with at least two independent and trusted sources
- Always erring on the side of caution when dealing with anyone you don't know or recognize, whether in person, over the phone, or over the Internet/network

Exam Essentials

Social-engineering attacks Social engineering is a unique type of attack that attempts to exploit human behavior. Such attacks can take many forms, from skillfully worded websites to clever e-mail messages to personnel impersonations over the phone to face-to-face acting. In just about every case, a social-engineering attack tries to convince the victim to perform some activity or reveal a piece of information that they shouldn't.

1.7 Understanding Auditing

The full name of this section from the Security+ objectives list is “Understand the concept and significance of auditing, logging and system scanning.” The key aspect of this issue is understanding that auditing is the primary means by which security violations are discovered. Through the use of a system's auditing capabilities, audit trails or logs are created. Audit trails enable auditors or administrators to detect when security violating activities have occurred and may assist in understanding how such a violation was allowed to occur.



For more information on this topic, refer to Chapter 2 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Auditing is the process of recording information about various online, electronic, digital events between subjects and objects. It's often synonymous with *logging* and *monitoring*. The goal of auditing is to check compliance with security policy and to discover security violations or system errors. Some common activities that are audited include logging on, logging off, reading files, deleting files, using remote access services, and using applications.

Effective auditing starts with detailed planning. You must know what you want to audit for in order to properly configure a system (if not an entire network) to record the desired information. Auditing everything will result in too much audit output, whereas auditing too little won't gather sufficient information for detection or event reconstruction.

The recorded results of auditing are called *audit trails* or *logs*. Logs are reviewed in order to discover abnormalities, discrepancies, or outright security violations. With sufficiently extensive logging, it's possible to reconstruct events leading up to a security violation. Auditing often enables system administrators to discover the perpetrator of the violation as well as pinpoint the systems and resources involved.

A closely related issue is *system scanning*. System scanning, penetration testing, and vulnerability scanning are all similar concepts. The point is to test the configuration of a system or network to determine if all known security weaknesses have been patched or addressed correctly. System scanning produces an audit report listing all of the weaknesses and vulnerabilities of the scanned system. Often the report includes suggestions or recommendations on how to resolve the discovered problems.

Exam Essentials

Auditing Auditing is the process of recording information about various online, electronic, digital events between subjects and objects. The goal of auditing is to check compliance with security policy and to discover security violations or system errors. Some common activities that are audited include logging on, logging off, reading files, deleting files, using remote access services, and using applications.

System scanning The point of system scanning is to test the configuration of a system or network to determine if all known security weaknesses have been patched or addressed correctly. System scanning produces an audit report listing all of the weaknesses and vulnerabilities of the scanned system. Often the report includes suggestions or recommendations on how to resolve the discovered problems.

Review Questions

1. What method of access control is best suited for environments with a high rate of employee turnover?
 - A. MAC
 - B. DAC
 - C. RBAC
 - D. ACL
2. Which of the following is the strongest form of authentication?
 - A. Biometric
 - B. Two-factor
 - C. Something you have
 - D. Username and password
3. Kerberos is used to perform what security service?
 - A. Authentication protection
 - B. File encryption
 - C. Secure communications
 - D. Protected data transfer
4. What form of authentication periodically reauthenticates the client during a logon session?
 - A. Kerberos
 - B. Certificates
 - C. Multi-factor
 - D. CHAP
5. Which is the strongest form of password?
 - A. More than eight characters
 - B. One-time use
 - C. Static
 - D. Uses different types of keyboard characters
6. Which of the following is commonly found to be a non-essential service on a web server?
 - A. Server service
 - B. DNS service
 - C. FTP service
 - D. Print spooler service

7. Which of the following is a Denial of Service attack that uses network packets that have been spoofed so that the source and destination address are that of the victim?
 - A. Land
 - B. Teardrop
 - C. Smurf
 - D. Fraggle
8. Which is the best countermeasure against malicious code?
 - A. Manage user behavior
 - B. Prevent reuse of external removable media
 - C. Use antivirus software
 - D. Disable mobile code on web browsers
9. Which is the best countermeasure to social-engineering attacks?
 - A. Preventing the download of mobile code from the Internet
 - B. Employee training
 - C. Strong password policies
 - D. Auditing user activities
10. What is the primary goal of auditing?
 - A. Detect virus infections.
 - B. Look for rogue services.
 - C. Scan for open ports.
 - D. Check compliance with security policy.

Answers to Review Questions

1. C. RBAC is best suited for environments with a high rate of employee turnover because access is defined against static job descriptions rather than transitive user accounts (DAC and ACL) or assigned clearances (MAC).
2. B. Two-factor is always more secure than any single factor of authentication.
3. A. Kerberos is a third-party authentication service; thus it provides authentication protection. Kerberos can't be used to encrypt files, secure nonauthentication communications, or protect data transfer.
4. D. CHAP periodically reauthenticates the client during a logon session. Kerberos, certificates, and multi-factor authentication mechanisms don't perform reauthentication.
5. B. A one-time password is always the strongest form of password. A static password is always the weakest form of password. A password with more than eight characters and using different types of keyboard characters is usually strong, but these factors alone are unable to indicate their strength.
6. D. A non-essential service is any element that isn't needed by the primary function of the server. In most cases, a web server doesn't use the print spooler service, but it often uses the server, DNS, and FTP services.
7. A. A land DoS attack uses network packets that have been spoofed so that the source and destination address are that of the victim. A teardrop attack uses fragmented IP packets. Smurf and fraggle attacks use spoofed ICMP and UDP packets, respectively, against an amplification network.
8. C. The most reliable countermeasure against malicious code is an antivirus scanner. User-behavior modification, managing media, and disabling mobile code are all countermeasures against malicious code, but they aren't as reliable and effective as antivirus scanners.
9. B. The only real countermeasure to social engineering is employee training. The other three options are good security measures; however, they aren't countermeasures to social engineering.
10. D. The primary goal of auditing is to check compliance with security policy. Virus infection detection is handled by a virus scanner. Rogue service detection is performed manually or with a sniffer. Port scanning is performed with a port-scanning tool.

Chapter

2

Communication Security

COMPTIA SECURITY+ EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.1 Recognize and understand the administration of the following types of remote access technologies**
 - 802.1x
 - VPN (Virtual Private Network)
 - RADIUS (Remote Authentication Dial-In User Service)
 - TACACS (Terminal Access Controller Access Control System)
 - L2TP/PPTP (Layer Two Tunneling Protocol/Point-to-Point Tunneling Protocol)
 - SSH (Secure Shell)
 - IPSEC (Internet Protocol Security)
 - Vulnerabilities
- ✓ **2.2 Recognize and understand the administration of the following email security concepts**
 - S/MIME (Secure Multipurpose Internet Mail Extensions)
 - PGP (Pretty Good Privacy) like technologies
 - Vulnerabilities
 - SPAM
 - Hoaxes
- ✓ **2.3 Recognize and understand the administration of the following Internet security concepts**
 - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
 - HTTP/S (Hypertext Transfer Protocol/Hypertext Transfer Protocol over Secure Sockets Layer)



- Instant Messaging
 - Vulnerabilities
 - Packet Sniffing
 - Privacy
- Vulnerabilities
 - Java Script
 - ActiveX
 - Buffer Overflows
 - Cookies
 - Signed Applets
 - CGI (Common Gateway Interface)
 - SMTP (Simple Mail Transfer Protocol) Relay
- ✓ **2.4 Recognize and understand the administration of the following directory security concepts**
 - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
 - LDAP (Lightweight Directory Access Protocol)
- ✓ **2.5 Recognize and understand the administration of the following file transfer protocols and concepts**
 - S/FTP (File Transfer Protocol)
 - Blind FTP (File Transfer Protocol)/Anonymous
 - File Sharing
 - Vulnerabilities
 - Packet Sniffing
 - 8.3 Naming Conventions
- ✓ **2.6 Recognize and understand the administration of the following wireless technologies and concepts**
 - WTLS (Wireless Transport Layer Security)
 - 802.11 and 802.11x
 - WEP/ WAP (Wired Equivalent Privacy/Wireless Application Protocol)
 - Vulnerabilities
 - Site Surveys

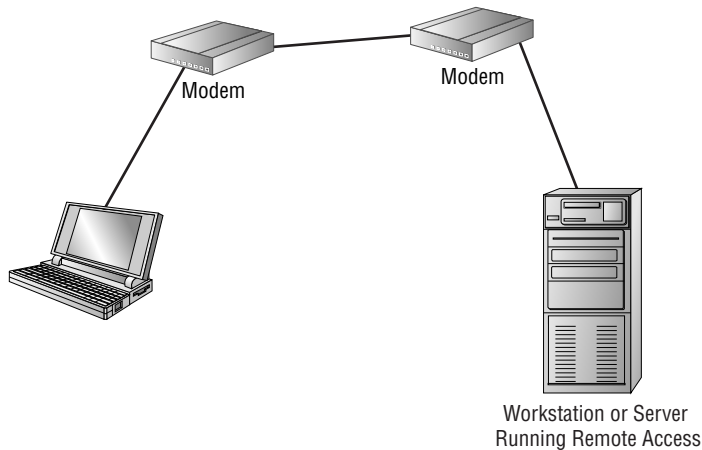


The Security+ exam will test your basic IT security skills—those skills needed to effectively secure stand-alone and networked systems in a corporate environment. To pass the test and be effective in implementing security, you need to understand the basic concepts and terminology related to communications security as detailed in this chapter.

2.1 Remote Access Technologies

The full name of this section from the Security+ objectives list is “Recognize and understand the administration of the following types of remote access technologies.” As networks grow, it becomes more common for them to support remote connections, whether dial-up, wireless WAN, or virtual private network (VPN); see Figure 2.1. The access control and protection issues involved in managing and administering remote access connections are generally termed *communications security*. In this section, we explore the foundational concepts and security issues of remote access connectivity.

FIGURE 2.1 A RAS connection between a remote workstation and a Windows server





For more information on this topic, refer to Chapter 3 of the *Security+ Study Guide, Second Edition*, by Sybex.

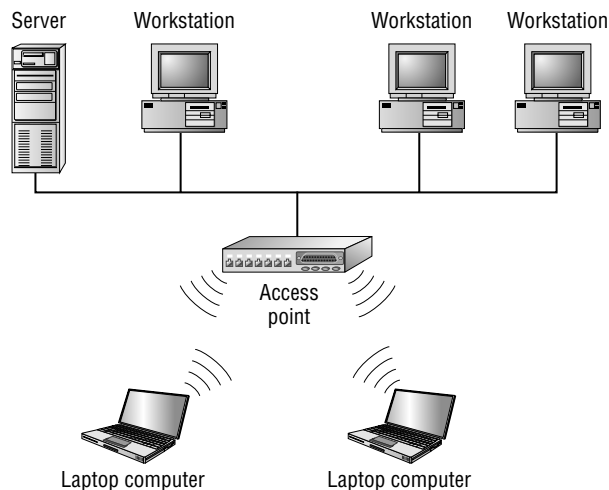
Critical Information

Networks exist to share resources. In order to share resources, all entities on a network must share a common protocol. But in order for the protocol to function, a communication medium must be in place to provide support for the transfer of that protocol and its hosted communication data between one system and another. Often that medium is a network cable, such as a 10BaseT or twisted-pair cable. However, the communication medium could be wireless, a VPN link, a dial-up link, a terminal services link, or even a remote control link. In any case, understanding the technology and the security implications of each of these communication media is an essential part of the Security+ exam.

802.1x

The *IEEE 802.1x* protocols are a collection of wireless protocol standards. Most modern *wireless* network communications follow the specifications outlined by the 802.1x standard. There are two widely used wireless standards: 802.11 and 802.16. However, the Security+ exam only focuses on 802.11 and related wireless networking technologies. Figure 2.2 shows a laptop PC (a network client) using a wireless access card to communicate with the rest of the network through a wireless access point and to a wireless server that offers Internet connectivity.

FIGURE 2.2 A typical wireless network





The bulk of the content for wireless communications is covered in section “2.6 Wireless.”

Virtual Private Network (VPN)

A *virtual private network (VPN)* is a communication *tunnel* between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted. VPNs can be used to connect two networks across the Internet (see Figure 2.3) or to allow distant clients to connect into an office LAN across the Internet (see Figure 2.4). Once a VPN link is established, the network connectivity for the VPN client is exactly the same as a LAN connected by a cable connection. The only difference between a direct LAN cable connection and a VPN link is speed.

FIGURE 2.3 Two LANs being connected using a VPN across the Internet

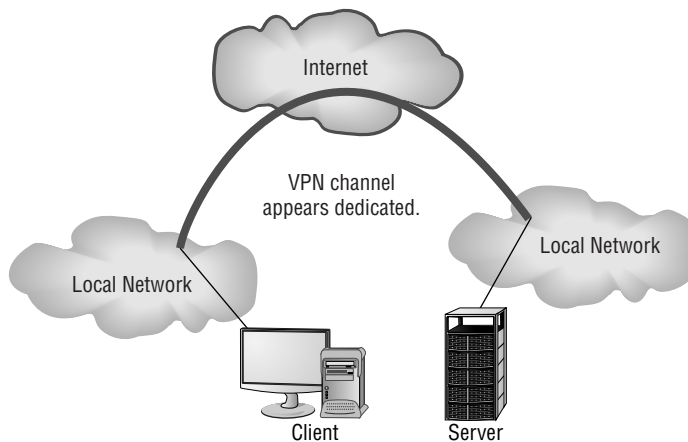
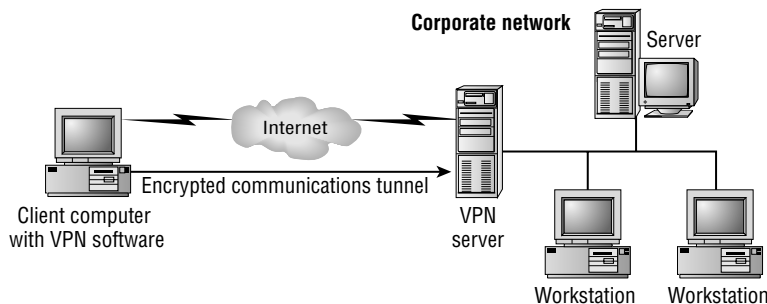


FIGURE 2.4 A client connecting to a network via a VPN across the Internet



VPNs are often the best solution to allow remote users to access resources on a corporate LAN. They have a number of advantages:

- They eliminate the need for expensive dial-up modem banks.
- They do away with long-distance toll charges.
- They allow any user anywhere in the world with an Internet connection to establish a VPN link with the office network.
- They provide security for both authentication and data transmission.

VPN links are established using VPN protocols. There are several VPN protocols, but the three you should recognize are Point-to-Point Tunneling Protocol (*PPTP*), Layer 2 Tunneling Protocol (*L2TP*), and Internet Protocol Security (*IPSec*).



These protocols are discussed in detail later in this section.

Sometimes VPN protocols are called *tunneling protocols*. This naming convention is designed to focus attention on the tunneling capabilities of VPNs.

VPNs work through a process called *encapsulation*. As data is transmitted from one system to another across a VPN link, the normal LAN TCP/IP traffic is encapsulated (encased, or enclosed) in the VPN protocol. The VPN protocol acts like a security envelope that provides special delivery capabilities (for example, across the Internet) as well as security mechanisms (such as data encryption).

When firewalls, intrusion detection systems, antivirus scanners, or other packet-filtering and -monitoring security mechanisms are used, you must realize that the data payload of VPN traffic won't be viewable, accessible, scannable, and so on, since it's encrypted. Thus, in order for these security mechanisms to function against VPN transported data, they must be placed outside of the VPN tunnel to act on the data after it has been decrypted and returned back to normal LAN traffic.

VPNs provide four critical functions:

Access control Restricts users from accessing resources on a network

Authentication Proves the identity of communication partners

Confidentiality Prevents unauthorized disclosure of secured data

Data integrity Prevents unwanted changes of data while in transit

As with any type of remote access connection, VPN clients can be authenticated through RADIUS.

Remote Authentication Dial-In User Service (RADIUS)

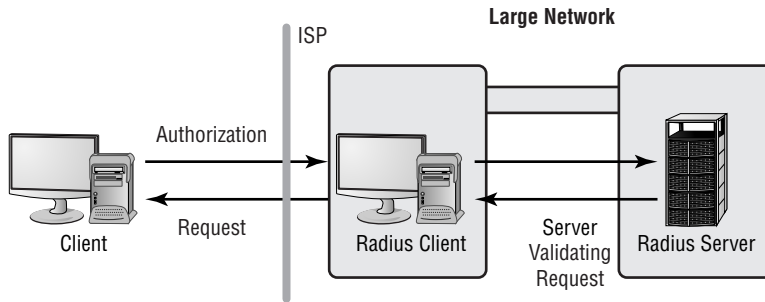
Remote Authentication Dial-In User Service (RADIUS) is a centralized authentication system. It's often deployed to provide an additional layer of security for a network. By offloading authentication of remote access clients from domain controllers or even the remote access server itself to a dedicated authentication server such as RADIUS, you can provide greater protection

against intrusion for the network as a whole. RADIUS can be used with any type of remote access, including dial-up, VPN, and terminal services.

RADIUS is known as an *AAA server*. AAA stands for authentication, authorization (or access control), and auditing. RADIUS provides for distinct AAA functions for remote access clients separate from those of normal local domain clients. RADIUS isn't the only AAA server, but it's the most widely deployed.

When RADIUS is deployed, it's important to understand the terms *RADIUS client* and *RADIUS server*, both of which are depicted in Figure 2.5. The RADIUS server is obviously the system hosting the RADIUS service. However, the RADIUS client is the *Remote Access Server (RAS)*, not the remote system connecting to RAS. As far as the remote access client is concerned, it only sees the RAS server, not the RADIUS server. Thus, the RAS server is the RADIUS client.

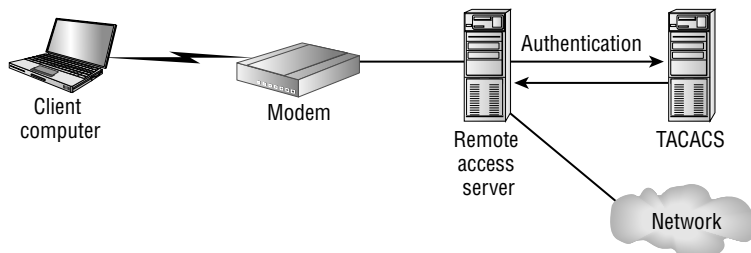
FIGURE 2.5 The RADIUS client manages the local connection and authenticates against a central server.



Terminal Access Controller Access Control System (TACACS)

Terminal Access Controller Access Control System (TACACS) is another example of an AAA server. TACACS is an Internet standard (RFC 1492); however, Cisco's proprietary implementations of *XTACACS* and *TACACS+* have quickly gained in popularity. TACACS is a centralized remote access authentication solution (Figure 2.6) similar to RADIUS; it uses ports TCP 49 and UDP 49.

FIGURE 2.6 Centrally managed remote access authentication with TACACS



Layer 2 Tunneling Protocol/Point-to-Point Tunneling Protocol (L2TP/PPTP)

Layer 2 Tunneling Protocol (L2TP) and *Point-to-Point Tunneling Protocol (PPTP)* are widely used VPN protocols. PPTP was originally developed by Microsoft. Cisco and Microsoft worked together in creating L2TP (based on Cisco's L2F and Microsoft's PPTP). Since its development, L2TP has become an Internet standard (RFC 2661) and is quickly becoming widely supported.

Both L2TP and PPTP are based on Point-to-Point Protocol (PPP) and thus work well over various types of remote access connections, including dial-up. L2TP can support just about any networking protocol. PPTP is limited to IP traffic. L2TP uses UDP port 1701, and PPTP uses TCP port 1723.

PPTP can use any of the authentication methods supported by PPP, including the following:

- *Challenge Handshake Authentication Protocol (CHAP)*
- *Extensible Authentication Protocol (EAP)*
- *Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAP v.1)*
- *Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v.2)*
- *Shiva Password Authentication Protocol (SPAP)*
- *Password Authentication Protocol (PAP)*

Note that PPTP can provide data encryption only when MS-CHAP v.2 is employed for authentication.

L2TP can rely on PPP and thus on PPP's supported authentication protocols. But L2TP also supports other authentication and encryption protocols, such as Internet Protocol Security (IPSec). Although it isn't required, L2TP is most often deployed using IPSec.

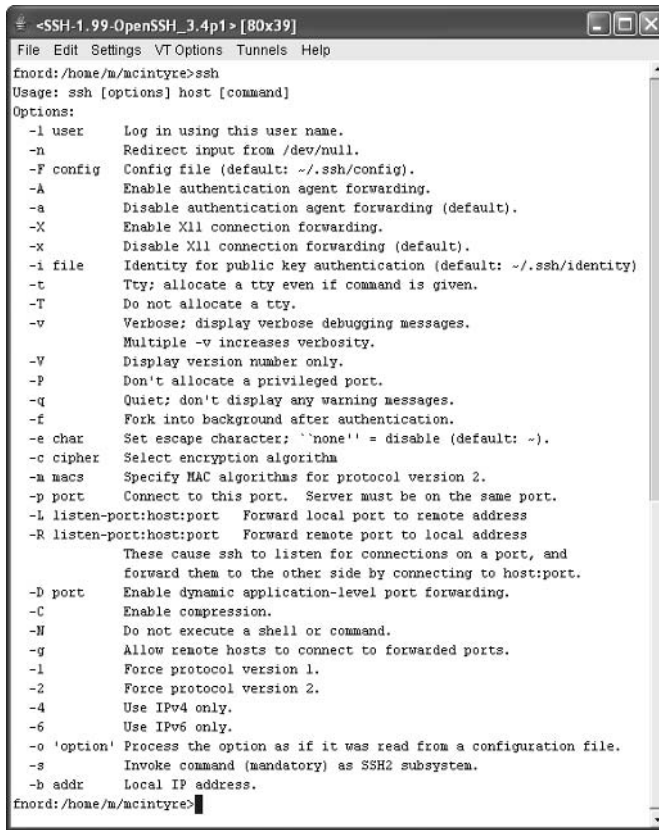
Secure Shell (SSH)

Secure Shell (SSH) is a secure replacement for Telnet, rlogin, rsh, and rcp. SSH can be called a remote access or remote terminal solution. It consists of an SSH server component and an SSH client component. SSH offers a means by which a command-line, text-only interface connection with a server can be established over any distance. Through the SSH connection, you can perform any command-line or scriptable activities. See Figure 2.7.

SSH transmits both authentication traffic and data in a secured encrypted form. Thus, no information is exchanged in clear text. This makes SSH a secure alternative to *Telnet*, which transmits both authentication credentials and data in clear text. SSH operates over TCP port 22.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is both a stand-alone VPN protocol and a module that can be used with L2TP. You can use IPSec in dial-up or network-to-network connections. When it's employed over dial-up, it usually functions as the encryption protocol in an L2TP link. IPSec by itself is more suitable for network-to-network connections across normal LAN connections, high-speed WAN links, and the Internet.

FIGURE 2.7 A Unix version of SSH, showing a list of available command-line options


```

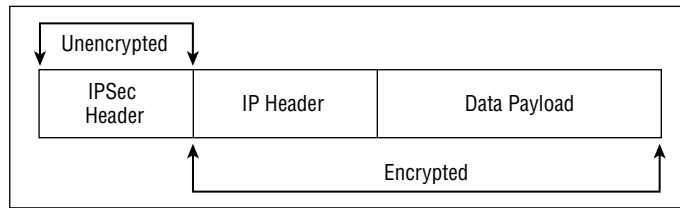
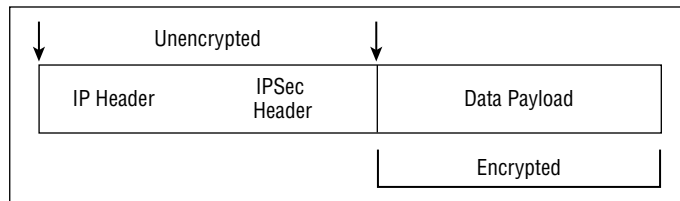
<SSH-1.99-OpenSSH_3.4p1> [80x39]
File Edit Settings VT Options Tunnels Help
fnord:/home/m/mcintyre>ssh
Usage: ssh [options] host [command]
Options:
  -l user      Log in using this user name.
  -n          Redirect input from /dev/null.
  -F config    Config file (default: ~/.ssh/config).
  -A          Enable authentication agent forwarding.
  -a          Disable authentication agent forwarding (default).
  -X          Enable X11 connection forwarding.
  -x          Disable X11 connection forwarding (default).
  -i file      Identity for public key authentication (default: ~/.ssh/identity)
  -t          Tty; allocate a tty even if command is given.
  -T          Do not allocate a tty.
  -v          Verbose; display verbose debugging messages.
               Multiple -v increases verbosity.
  -V          Display version number only.
  -P          Don't allocate a privileged port.
  -q          Quiet; don't display any warning messages.
  -f          Fork into background after authentication.
  -e char      Set escape character; 'none' = disable (default: ~).
  -c cipher    Select encryption algorithm
  -m macs      Specify MAC algorithms for protocol version 2.
  -p port      Connect to this port. Server must be on the same port.
  -L listen-port:host:port Forward local port to remote address
  -R listen-port:host:port Forward remote port to local address
               These cause ssh to listen for connections on a port, and
               forward them to the other side by connecting to host:port.
  -D port      Enable dynamic application-level port forwarding.
  -C          Enable compression.
  -N          Do not execute a shell or command.
  -g          Allow remote hosts to connect to forwarded ports.
  -1          Force protocol version 1.
  -2          Force protocol version 2.
  -4          Use IPv4 only.
  -6          Use IPv6 only.
  -o 'option'  Process the option as if it was read from a configuration file.
  -s          Invoke command (mandatory) as SSH2 subsystem.
  -b addr      Local IP address.
fnord:/home/m/mcintyre>

```

IPSec isn't a single protocol but rather a collection of protocols. Two of the primary protocols of IPSec are *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*. AH provides authentication of the sender's data; ESP provides encryption of the transferred data as well as limited authentication.

IPSec operates at the OSI Model layer 3 (the Network layer). IPSec operates over TCP ports 50 and 51. Thus, if an IPSec tunnel is to cross a firewall, these ports must be opened.

IPSec can operate in two modes: *tunnel mode* and *transport mode*. In tunnel mode (see Figure 2.8), IPSec provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPSec header. In transport mode (see Figure 2.9), IPSec provides encryption protection for just the payload and leaves the original message header intact. Tunnel mode should be used when you're connecting over an untrusted network.

FIGURE 2.8 IPSec's encryption of a packet in tunnel mode**FIGURE 2.9** IPSec's encryption of a packet in transport mode

IPSec provides for encryption security using symmetric cryptography. This means communication partners use shared secret keys to encrypt and decrypt traffic over the IPSec VPN link. One of the mechanisms used by IPSec to manage cryptography is *Internet Key Exchange (IKE)*; it ensures the secure exchange of secret keys between communication partners in order to establish the encrypted VPN tunnel.

IPSec also uses *Internet Security Association and Key Management Protocol (ISAKMP)*, which is known as a *security association manager*. A security association is the agreed-upon method of authentication used by two entities. Without a common method of authentication, a VPN link can't be established. So, ISAKMP is used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner. The four major functional components of ISAKMP are

- Authentication of communications peers
- Threat mitigation
- Security association creation and management
- Cryptographic key establishment and management

Vulnerabilities

Every communications technology, mechanism, or solution is vulnerable to one thing or another. With the implementation of cryptography to provide security through encryption, many forms of communication have become more reliable and now offer dependable protection. When encryption is involved, the issue often distills down to the algorithm in use and the length of

the key. Obviously, using algorithms such as DES, which have been broken, offers weaker security. Likewise, using shorter keys allows a brute-force attack to be more successful.

Outside of the technologies involved with communications, there will always be the weakness of social engineering against the people involved in using those connections. Ultimately, no matter how strong the technology, without reliable physical access control and sufficient employee training, security is little more than a fading wish.

Exam Essentials

VPNs A virtual private network (VPN) is a communication tunnel between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted.

VPN protocols PPTP, L2TP, and IPSec are VPN protocols.

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a centralized authentication system. It's often deployed to provide an additional layer of security for a network. A RADIUS client is the RAS server.

TACACS Terminal Access Controller Access Control System (TACACS) is a centralized remote access authentication solution similar to RADIUS. TACACS uses ports TCP 49 and UDP 49.

PPTP Point-to-Point Tunneling Protocol (PPTP) is based on PPP, limited to IP traffic, and uses TCP port 1723. PPTP supports PAP, SPAP, CHAP, EAP, and MS-CHAP v.1 and v.2.

L2TP Layer Two Tunneling Protocol (L2TP) is based on PPTP and L2F, supports any LAN protocol, uses UDP port 1701, and often uses IPSec for encryption.

SSH Secure Shell (SSH) is a secure replacement for Telnet, rlogin, rsh, and rcp. It can be called a remote access or remote terminal solution. SSH encrypts authentication and data traffic, and it operates over TCP port 22.

IPSec Internet Protocol Security (IPSec) is both a stand-alone VPN protocol and a module that can be used with L2TP. IPSec can be used in dial-up or network-to-network connections. It operates at the OSI Model layer 3 (the Network layer) over TCP ports 50 and 51.

AH and ESP IPSec isn't a single protocol, but rather a collection of protocols. Two of the primary protocols of IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides authentication of the sender's data; ESP provides encryption of the transferred data as well as limited authentication.

Tunnel mode and transport mode In tunnel mode, IPSec provides encryption protection for both the payload and the message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPSec header. In transport mode, IPSec provides encryption protection for just the payload and leaves the original message header intact.

IKE Internet Key Exchange (IKE) ensures the secure exchange of secret keys between communication partners in order to establish the encrypted VPN tunnel.

ISAKMP Internet Security Association and Key Management Protocol (ISAKMP) is used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner. The four major functional components of ISAKMP are authentication of communications peers, threat mitigation, security association creation and management, and cryptographic key establishment and management.

Communication vulnerabilities Every communications technology, mechanism, or solution is vulnerable to one thing or another. With the implementation of cryptography to provide security through encryption, many forms of communication have become more reliable and now offer reliable protection. When encryption is involved, the issue often distills down to the algorithm in use and the length of the key.

2.2 E-mail Security

The full name of this section from the Security+ objectives list is “Recognize and understand the administration of the following email security concepts.” E-mail is the most widely used communication vehicle on the Internet. However, it has also become one of the primary delivery mechanisms for malicious code and social-engineering attacks. Understanding e-mail security issues is essential to the Security+ exam.

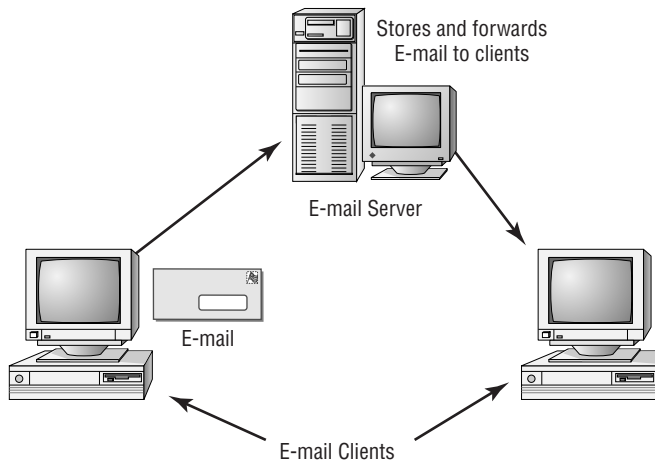


For more information on this topic, refer to Chapters 3 and 8 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Internet-based e-mail relies primarily on a single protocol: *Simple Mail Transport Protocol (SMTP)*. In Figure 2.10, SMTP has proven itself over the last 20+ years as a reliable e-mail delivery system. However, it has one significant flaw: its nearly complete lack of security. SMTP doesn't offer encryption for transmitted messages. Thus, any and all e-mail can be snooped and examined. As e-mail becomes the basis for business communications, clear text communication is no longer a viable option. Fortunately, SMTP supports add-on capabilities that bring encryption and other security services to e-mail. SMTP operates over TCP port 25.

Other protocols are involved with a complete e-mail solution. *Post Office Protocol (POP)* and *Internet Message Access Protocol (IMAP)* are used to pull e-mail from an e-mail server down to a client, but they aren't involved in moving e-mail across the Internet. POP operates over TCP port 110, and IMAP operates over TCP port 143. E-mail is natively insecure. Thus, several encryption options have been developed to add security to e-mail used over the Internet. Two of the most common solutions are S/MIME and PGP.

FIGURE 2.10 E-mail connections between clients and a server

Secure Multipurpose Internet Mail Extensions (S/MIME)

Secure Multipurpose Internet Mail Extensions (S/MIME) is an Internet standard for encrypting e-mail. Many e-mail security products are based on the S/MIME standard. S/MIME takes the standard MIME element of e-mail, which enables e-mail to carry attachments and higher-order textual information (fonts, color, size, layout, and so on), and expands this to include message encryption. S/MIME uses RSA (an asymmetric encryption scheme) to encrypt and protect e-mail.

S/MIME works by taking the original message from the server, encrypting it, and then attaching it to a new blank e-mail as an attachment. The new blank e-mail includes the sender's and receiver's e-mail addresses, to control routing of the message to its destination. The receiver must then strip off the attachment and decrypt it in order to extract the original message. When e-mail encryption is used, confidentiality is protected.

As shown in Figure 2.11, the basic process is as follows:

1. The sender encrypts the message with the recipient's public key.
2. The message is sent to the recipient.
3. The recipient decrypts the message using the recipient's private key.

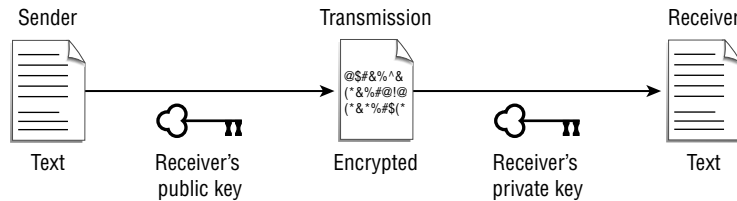


As you'll learn in Chapter 4, "Basics of Cryptography," in an asymmetric cryptography solution, each communication entity has its own private and public key pair. Anything encrypted with the public key can only be decrypted with the corresponding private key, and vice versa.

The process of encrypting e-mail isn't complex; however, it's cumbersome in implementation. Fortunately, an S/MIME add-on package for an e-mail client automates the process. The only restriction to the S/MIME e-mail solutions is that all communication partners must have compatible S/MIME products installed and use a common or compatible source for their asymmetric encryption key pairs.

S/MIME includes the capability to digitally sign e-mails; however, this isn't a widely employed feature. Pretty Good Privacy's (PGP) digital signature feature is much more popular.

FIGURE 2.11 The asymmetric-based e-mail encryption process



Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is another e-mail security and encryption product that functions in much the same way as S/MIME. PGP was developed by Phillip R. Zimmerman in 1991. It has widespread popularity with the general public as well as corporations that wish to use secured private e-mail. PGP uses RSA or Diffie-Hellman asymmetric cryptography solutions. It's similar to S/MIME, but it's a proposed e-mail security standard of its own known as PGP/MIME.

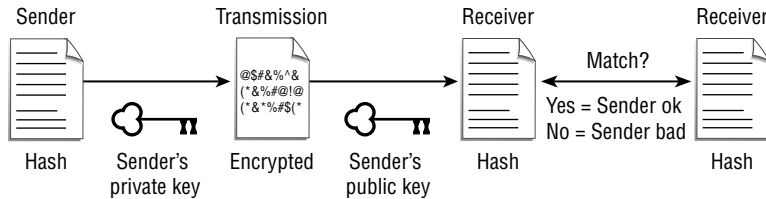
Another popular feature of PGP is *digital signatures*. A digital signature is a means by which PGP users can sign their e-mails so that both PGP and non-PGP using recipients can see the text or body of the message. However, a PGP recipient can then verify or authenticate the message by testing the signature. Digital signatures provide a means to verify the source of a message; this is known as *nonrepudiation*. The digital signature also includes a hash value of the message and allows the recipient to verify that the integrity of the message hasn't been violated while in transit.

The process of using a digital signature is more complex than encrypting a message. It requires not only a shared asymmetric cryptography solution between the communication partners, but also that both parties use the same hashing algorithm. The procedure for employing a digital signature is as follows (see Figure 2.12):

1. The sender creates a hash of the original message.
2. The sender encrypts the hash with the sender's private key.
3. The sender attaches the encrypted hash to the original message and sends it to the recipient. (Note: the original message is in clear text form.)
4. The recipient strips off the encrypted hash.
5. The recipient decrypts the hash using the sender's public key.

6. The recipient generates a hash of the received original message (without the attached encrypted hash).
7. The recipient compares the generated hash with the extracted hash from the sender. If they match, the recipient knows the message hasn't changed and the message is from the identified sender.

FIGURE 2.12 The asymmetric-based e-mail digital signature process



See Chapter 4 to learn more about asymmetric cryptography and hashing.

Vulnerabilities

E-mail allows for fast, efficient communications across the Internet. There are more e-mail addresses than there are actual Internet users, because many people have multiple e-mail addresses whether by chance or by choice. E-mail offers individuals and companies alike a means to communicate without paying any type of per-message fee (such as with snail mail) and allows message to be delivered in seconds rather than days. However, these abilities of e-mail also make it ripe for exploitation by those with malicious or at least nonbenevolent intentions. Some examples include spam and hoaxes, which are discussed in the following sections.



E-mail relaying is also another important issue. That topic is discussed at the end of section "2.3 Internet Security."

Because e-mail is so widely used, it has become the most prevalent delivery vehicle for malicious code such as viruses, logic bombs, and Trojan horses. To combat this threat, you should deploy an antivirus scanner to scan e-mail content and attachments. You should even consider stripping or blocking e-mail attachments (especially those with known extensions of scripts or executables) as they enter your network (on an e-mail gateway, firewall, and so on).

E-mail servers should also check for invalid, corrupted, or malformed messages. An e-mail message with a corrupted *MIME header* can cause an unprepared e-mail server to crash or freeze. Thus, attackers can use invalid e-mail formats as a method of waging a Denial of Service (DoS) attack against your e-mail systems. By keeping e-mail servers properly updated and deploying antivirus scanners and e-mail filters, you can avoid most of the problems and attacks associated with e-mail.

Spam

Spam is any type of e-mail that is undesired and/or unsolicited. Think of spam as the digital equivalent of junk mail and door-to-door solicitations.



Some studies have shown that nearly half of all e-mail now consists of spam.

Spam is a problem for numerous reasons:

- Some spam carries malicious code such as viruses, logic bombs, and Trojan horses.
- Some spam carries a social-engineering attack (also known as hoax e-mail).
- Unwanted e-mail wastes your time while you sort through it looking for legitimate messages.
- Spam wastes Internet resources: storage capacity, computing cycles, and throughput.

The primary countermeasure against spam is an e-mail filter. An e-mail filter is a list of e-mail addresses, domain names, or IP addresses where spam is known to originate. If a message is received from one of the listed spam sources, the e-mail filter blocks or discards it. Some e-mail filters are becoming as sophisticated as antivirus scanners. These e-mail filters can examine the header, subject, and contents of a message to look for key words or phrases that identify it as a known type of spam, and then take the appropriate actions to discard or block the message.

However, e-mail spam filters are problematic. Just because a message includes key words that are typically found in spam doesn't mean that every message with those words is spam. Some legitimate, if not outright essential, messages include spam words. One method of addressing this issue is for the spam-filtering tool to place all suspected spam messages into a quarantine folder. Users can peruse this folder for misidentified messages and retrieve them.

Another important issue to address when managing spam is spoofed e-mail. A *spoofed* e-mail is a message that has a fake or falsified source address. When an e-mail server receives an e-mail message, it should perform a reverse lookup on the source address of the message. If the source address is fake or nonexistent, then the message should be discarded.

Hoaxes

A *hoax* is an e-mail message that includes incorrect or misleading information. This is a written or static form of social-engineering attack. Hoaxes are common and widespread because they expertly prey on human nature. If e-mail recipients aren't prepared for hoaxes, they can be easily caught up in them or persuaded by them. Hoaxes may inform you of intended court cases or legislation and encourage you to support one side or the other with a donation. They may warn you of a quickly spreading virus and provide details on how to sanitize your computer, such as deleting certain files or editing the Registry. Hoaxes also include chain letters that promise good fortune, bypassing of bad luck, or accumulation of wealth by passing the message on to others.

Although a hoax isn't the same as a virus, in that it causes no direct damage, it often ends up causing nearly as much damage as a virus would. When ignorant users follow the instructions of a hoax—especially those that instruct readers to delete files or alter their system configuration

via the Registry—the users usually end up damaging their operating system so severely as to require a reinstall or restoration from backup. Even if the damage isn't immediately or obviously severe, sometimes the instructions in a hoax open up vulnerabilities so that real viruses, remote-control hacker tools, or other forms of malicious code can gain access.

Your primary weapon against hoaxes is education and awareness. E-mail users should be on the lookout for any message that promises the unlikely, seems too good to be true, or has dire warnings that require immediate action.

When you receive a message that you think might be a hoax, whether intentional or not, do the following:

1. Notify your network administrator when you receive a suspected hoax.
2. Check with your antivirus vendor for confirmation of malicious code–related issues.
3. Check with your antivirus vendor for e-mail hoax–related issues (most maintain a database of hoaxes).
4. Find at least three other reliable, public, trusted sources to corroborate any message, especially if it involves legal or monetary issues.
5. Don't forward any message to others if the message specifically directs you to do so. If there is a legitimate security issue spreading across the Internet, the security watchdogs will respond and inform the public appropriately.
6. Never follow the directions in an e-mail from an unknown or untrusted source. Always validate procedures from a trusted, reliable source (such as Microsoft, a software vendor, an antivirus vendor, or your ISP).

If you discover a hoax, especially one that isn't already cataloged in your antivirus vendor's hoax database, send the vendor a copy so it can inform others. Be sure to contact the vendor and ask how to submit examples of hoaxes; don't just forward the message.

Exam Essentials

SMTP Simple Mail Transport Protocol (SMTP) moves e-mail messages across the Internet from sender to recipient. It doesn't include native encryption. It operates over TCP port 25.

POP and IMAP Post Office Protocol (POP) and Internet Mail Access Protocol (IMAP) are used to pull e-mail from an e-mail server down to a client. POP operates over TCP port 110. IMAP operates over TCP port 143.

S/MIME Secure Multipurpose Internet Mail Extensions (S/MIME) is an Internet standard for encrypting and digitally signing e-mail. It uses RSA (an asymmetric encryption scheme) to encrypt and protect e-mail.

PGP Pretty Good Privacy (PGP) is used to encrypt and digitally sign e-mail messages. It uses RSA or Diffie-Hellman asymmetric cryptography solutions.

Malicious code delivery vehicle E-mail is the most prevalent delivery vehicle for malicious code such as viruses, logic bombs, and Trojan horses. Deploy an antivirus scanner to scan e-mail

content and attachments, and block e-mail attachments (especially those with known extensions of scripts or executables).

E-mail DoS attacks E-mail servers should check for invalid, corrupted, or malformed messages. An e-mail message with a corrupted MIME header can cause an unprepared e-mail server to crash or freeze.

Spam Spam is undesired or unsolicited e-mail. It's a problem for numerous reasons. First, some spam is the carrier for malicious code such as viruses, logic bombs, and Trojan horses. Second, some spam is the carrier of a social-engineering attack (hoax e-mail). Third, unwanted e-mail wastes your time while you're sorting through it looking for legitimate messages. Fourth, spam wastes Internet resources such as storage capacity, computing cycles, and throughput.

E-mail filters An e-mail filter is a list of e-mail addresses, domain names, or IP addresses where spam is known to originate.

Spoofed e-mail A spoofed e-mail is a message that has a fake or falsified source address. When an e-mail server receives an e-mail message, it should perform a reverse lookup on the source address of the message.

Hoaxes A hoax is an e-mail message that includes incorrect or misleading information. This is a written or static form of social-engineering attack. Your primary weapons against hoaxes are education and awareness. Notify your network administrator when you receive a suspected hoax.

2.3 Internet Security

The full name of this section from the Security+ objectives list is "Recognize and understand the administration of the following Internet security concepts." The Internet has become a common communication medium for both home users and business users alike. Due to this widespread dependence on such an insecure network, it is important to specifically impose security on all sensitive, confidential, or private communication transmissions occurring over the Internet. This section focuses on SSL, TLS, HTTP, HTTPS, instant messaging, and the vulnerabilities of these common Internet communication mechanisms.



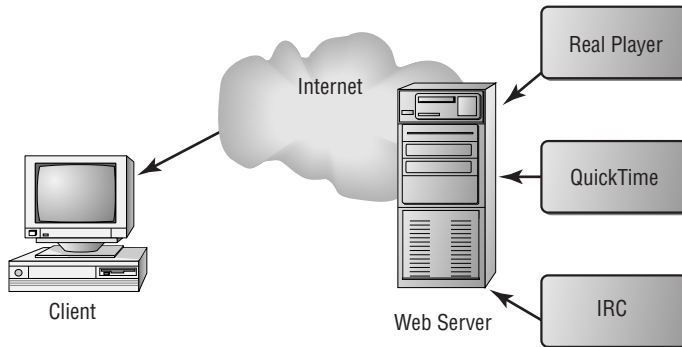
For more information on this topic, refer to Chapters 3 and 4 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

The World Wide Web is a vast, global ad hoc collection of online information and storefronts. The primary protocol that supports the Web is *Hypertext Transfer Protocol (HTTP)*. HTTP enables the transmission of *Hypertext Markup Language (HTML)* documents (the base page elements of a website) and embedded multimedia components such as graphics and mobile code

(see Figure 2.13). Without HTTP, there would be no Web. However, HTTP is an insecure protocol: it doesn't offer anything in the way of authentication or encryption for web communications. Fortunately, numerous add-on protocols and mechanisms provide these and other security service to the information superhighway.

FIGURE 2.13 A web server providing streaming video, animations, and HTML data to a client



Secure Sockets Layer/Transport Layer Security (SSL/TLS)

Secure Sockets Layer (SSL) and *Transport Layer Security (TLS)* are used to encrypt traffic between a web browser and a web server. Through the use of SSL or TLS, web surfers can make online purchases, interact with banks, and access private information without disclosing the contents of their communications. SSL and TLS can make web transactions private and secure. While they aren't true VPN protocols, SSL and TLS operate in much the same manner as VPNs.

SSL was originally developed by Netscape, but it quickly became an Internet standard. Currently SSL version 3.0 is in widespread use across the Internet. TLS is based on SSL, but they aren't interoperable. SSL operates over TCP port 443, whereas TLS can operate over TCP port 443 or 80 (as does HTTP).

SSL can also be used to provide encrypted sessions for other application layer protocols, such as Telnet, FTP, and e-mail. SSL functions at layer 5 (the Session layer) of the OSI Model.

When SSL is to be used to secure the communications between a web browser and web server, a six-step handshake process must be completed to establish the secured session:

1. The client requests a secure connection.
2. The server responds with its certificate, the name of its certifying authority (issuing CA), and its public key.
3. The client verifies the server's certificate, produces a session (symmetric) encryption key, encrypts the key with the server's public key, and then sends the encrypted key to the server.
4. The server unpacks the session key and then sends a summary of the session details to the client encrypted with the session key.

5. The client reviews the summary and then sends its own summary back to the server, likewise encrypted with the session key.
6. Once both entities receive a matching session summary, secured SSL communications are initiated.

SSL uses symmetric keys as the session keys. The session keys are available in 40-bit and 128-bit strengths.

Hypertext Transfer Protocol/Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

HTTP is the standard foundational protocol used on the Web. It operates over TCP port 80. HTTP is a plain text or clear text communication protocol; thus it offers no security or privacy to transactions. When SSL or TLS is used to secure transactions, this is known as *Hypertext Transfer Protocol over SSL (HTTPS)*. You'll be able to recognize when secure web communications are occurring using SSL or TLS because the URL will begin with HTTPS and a locked padlock icon will appear in the status bar at the bottom of the browser window.

It's important not to confuse HTTPS with a similar protocol, Secure HTTP (S-HTTP). S-HTTP isn't in widespread use. The primary differences are that S-HTTP doesn't use SSL, it encrypts individual web page elements rather than the entire web communication session, and it can only be used to support HTTP. Overall, S-HTTP is less secure than HTTPS.

In addition to web pages, SSL can also be used to secure FTP, Network News Transfer Protocol (NNTP), Telnet, and other Application layer TCP/IP protocols. S-HTTP is unable to protect anything other than web traffic.

Instant Messaging

Instant messaging (IM) is a mechanism that allows for real-time text-based chat between two users located anywhere on the Internet. Some IM utilities allow for file transfer, multimedia, voice and video conferencing, and more. However, unlike many Internet information services, such as the Web, FTP, and e-mail, IM is a peer-to-peer based service. There is no need for a centralized controlling server. This makes IM easy for end users to deploy and use, but it's difficult to manage from a corporate perspective. IM is insecure. It has numerous vulnerabilities, such as susceptibility to packet sniffing, it lacks true native security capabilities, and it provides no protection for privacy.

Vulnerabilities

Instant messaging offers little in the way of security or privacy. Many IM clients are susceptible to malicious code deposit or infection through their file transfer capabilities. Also, IM users are often subject to numerous forms of social-engineering attacks, such as impersonation or convincing a victim to reveal information that should remain confidential (such as passwords).

Packet Sniffing

Most IM clients don't use encryption when transmitting messages. Thus, most communications are subject to *packet sniffing* and *eavesdropping* attacks.

Privacy

IM clients do not provide any direct protection for user privacy. The fact that IM clients perform communications in the clear and do not offer encryption or security services, makes all private and confidential transmissions subject to packet sniffing and eavesdropping attacks.

Vulnerabilities

As the capabilities of the Web and other Internet information services expand, the vulnerabilities seem to increase as well. Nearly every form of communication that occurs over the Internet has a wide range of weaknesses. It's important to keep yourself informed about the relevant problems and issues with communication methods you employ and how to resolve or safeguard against them. Some of these issues include JavaScript, ActiveX, buffer overflows, cookies, signed applets, CGI scripts, and SMTP relays.

JavaScript

JavaScript is a scripting programming language that can be embedded directly into the HTML of a web page. It's executed by the web browser and can be used to perform a wide range of functions, both benign and malicious. Unlike its namesake Java, JavaScript doesn't run in a restricted security zone; rather it has nearly unrestricted access to all system resources. Due to its power and unpredictability, it's generally recommended that you disable the download and execution of JavaScript except from websites you're sure you can trust.

ActiveX

ActiveX is a mobile code technology developed by Microsoft. ActiveX controls or components are stand-alone programs that can be attached to or embedded in web documents to perform a wide range of functions. ActiveX components are executed with the same security privileges as the current user. However, the ActiveX component is saved to the hard drive and can be accessed at a later time, even after you've left the website where it was obtained. Thus, ActiveX can be a significant security issue. It's recommended that ActiveX components not be downloaded or executed except from websites you're sure you can trust. In many cases, web browsers can be configured to always allow, always block, or prompt the user each time an ActiveX component is presented by a website.

Buffer Overflows

A *buffer overflow* occurs when a program receives input that is larger than it was designed to accept or process. The extra data received by the program is shunted over onto the CPU without any security restrictions; it's then allowed to execute (assuming it's a valid command, script, system call, and so on) with system-level privileges. The result of a buffer overflow can be anything, such as a program crash, a system freeze or crash, opening a port, disabling a service, creating a user account, elevating the privileges of an existing user account, accessing a website, or executing a utility. A clever attacker can do just about anything they wish if they can execute a command or script unrestricted access to a system.

Sometimes a buffer overflow attack can be labeled as a form of Denial of Service (Dos) attack, since a buffer overflow occurs when a system receives more data than it can handle (a bit like

a flooding attack). This is especially true when the buffer overflow event results in a system no longer being able to process legitimate data or requests.

Poor programming quality controls and not including input validation checks in software lead to buffer overflow attacks. Unfortunately, there is little commercial software that isn't vulnerable to buffer overflow attacks; web server software is attacked most frequently. Fortunately, buffer overflow vulnerabilities are often easily patched with vendor updates.

Cookies

A *cookie* is a tracking mechanism developed for web servers to monitor and respond to a user's serial viewing of multiple web pages. A cookie is often used to maintain an e-commerce shopping cart, focus product placement, or track your visiting habits. However, the benign purposes of cookies have been subverted by malevolent entities. Now, cookies are a common means of violating your privacy by gathering information about your identity, logon credentials, surfing habits, work habits, and much more. A cookie can be easily exploited against a web browser to gather sufficient information about a user to allow the attacker to impersonate the victim online. It's generally recommended that you block cookies from all but the most trusted sites.

Signed Applets

One method that helps reduce the number of malicious elements of mobile code downloaded and executed on a system is a mechanism known as applet signing. A *signed applet* is a piece of mobile code that has been digitally signed using the creator's or owner's certificate. A signed applet clearly indicates to the user the source of the applet. Web browsers can be configured to accept only signed applets or to prompt whenever any applet is offered by a website. It's important to understand that a signed applet only proves the applet's identity or source; it provides no guarantee as to the reliability or quality of the applet. Just because you know where an applet comes from doesn't mean that the applet isn't malicious code or that it won't cause a problem with your computer system.

Common Gateway Interface (CGI)

Common Gateway Interface (CGI) is a mechanism developed early in the life of the Web to allow a web browser to submit information from a user back to a web server for processing by a server-side script or application. Although CGI scripting isn't used as widely as JavaScript or ActiveX today, it's still a default-enabled feature of both web servers and web browsers.

CGI has numerous vulnerabilities, the most prevalent of which is the ability of a user to submit data that results in the script's failure, a buffer overflow attack, or the performance of an unauthorized or unwanted activity (at least from the perspective of the web server owner).

Another issue with CGI is that all directories on the web server that host CGI scripts must be configured to allow web visitors to execute files. If the web server's folder hierarchy isn't properly protected, this could enable a user to upload their own scripts and then execute them.

Simple Mail Transfer Protocol (SMTP) Relay

SMTP relay is the feature or function of an SMTP or e-mail server when it receives an e-mail from a client or other SMTP server and then forwards it on to another SMTP server. The forwarding action is similar to normal network packet routing, in that the purpose is to transmit

the e-mail message to its destination. E-mail relaying is an essential part of the success of Internet e-mail, but it can be abused.

E-mail relaying abuse often leads to DoS attacks or spam. Spam (specifically, spoofed spam) is often sent by rogue solicitors who find e-mail servers on the Internet that aren't properly configured to authenticate clients and servers before accepting e-mail. When an SMTP server fails to authenticate clients and servers before accepting e-mail, it's known as an *open relay*.

When you're deploying and securing an SMTP server, it's important to disable the open relay feature. However, even after an SMTP server has been secured, a clever attacker may be able to reenabling relaying using a Trojan horse, buffer overflow, or remote access attack against the system. Thus, it's important to regularly check the performance logs and configuration settings of e-mail servers. One important item to look for is the presence of a universal accept for the relaying of e-mail. For example, on Unix systems, the e-mail server will have a file in the `/etc/mail/relay` folder that lists all the servers and clients that are authorized to submit e-mail. If this file includes a universal include, which is usually represented by a dot and an asterisk (`. *`), then delete that entry and reboot the system to force the change to take effect.

Exam Essentials

Web basics The Web uses Hypertext Transfer Protocol (HTTP) over TCP port 80 to transmit Hypertext Markup Language (HTML) documents between a web server and a web browser.

SSL Secure Sockets Layer (SSL) is used to encrypt traffic between a web server and a web browser. SSL operates over TCP port 443. It uses a six-step handshake process to establish a secure web session. SSL uses 40- or 128-bit symmetric session keys.

TLS Transport Layer Security (TLS) is used to encrypt traffic between a web server and a web browser in much the same way as SSL. It operates over TCP port 443 or 80. TLS isn't interoperable with SSL.

HTTPS HTTPS is Hypertext Transfer Protocol over SSL. The presence of HTTPS at the beginning of a URL indicates the use of SSL or TLS. HTTPS isn't to be confused with Secure HTTP (S-HTTP).

Instant messaging Instant messaging (IM) is a mechanism that allows for real-time, text-based chat between two users located anywhere on the Internet. IM offers little privacy and is susceptible to malicious code deposit, and users are subject to social-engineering attacks. IM communications can be intercepted by packet sniffers.

JavaScript JavaScript is a scripting programming language that can be imbedded directly into the HTML of a web page. JavaScript, unlike its namesake Java, doesn't run in a restricted security zone; rather, it has nearly unrestricted access to all system resources. Due to its power and unpredictability, it's generally recommended that you disable the download and execution of JavaScript except from those websites you're sure you can trust.

ActiveX ActiveX is a mobile code technology developed by Microsoft. ActiveX components shouldn't be downloaded or executed except from websites you're sure you can trust.

Buffer overflows A buffer overflow occurs when a program receives input that is larger than it was designed to accept or process. The extra data received by the program is shunted over onto the CPU without any security restrictions; it's then allowed to execute. The result of a buffer overflow can be anything, such as a program crash, a system freeze or crash, opening a port, disabling a service, creating a user account, elevating the privileges of an existing user account, accessing a website, or executing a utility.

Cookies Cookies are a common means of violating your privacy by gathering information about your identity, logon credentials, surfing habits, work habits, and much more.

Signed applets A signed applet is a piece of mobile code that has been digitally signed using the creator's or owner's certificate. A signed applet clearly indicates to the user the source of the applet.

CGI Common Gateway Interface (CGI) is the mechanism developed early in the life of the Web to allow a web browser to submit information from a user back to a web server for processing by a server-side script or application. CGI has numerous vulnerabilities, most prevalent of which is the ability for a user to submit data that results in the script's failure, a buffer overflow attack, or the performance of an unauthorized or unwanted activity.

SMTP relay SMTP relay is the function of an SMTP or e-mail server when it receives an e-mail from a client or other SMTP server and then forwards it on to another SMTP server. E-mail relaying abuse often leads to DoS attacks or spam.

2.4 Directory Security

The full name of this section from the Security+ objectives list is "Recognize and understand the administration of the following directory security concepts." A directory service is a managed list of network resources. Through the use of a directory service, large networks are easier to navigate, manage, and secure.



For more information on this topic, refer to Chapters 5 and 8 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Active Directory from Microsoft and eDirectory (or NDS) from Novell are examples of directory services. Both of these products are based on Lightweight Directory Access Protocol (LDAP). Understanding LDAP is an important part of the Security+ exam.

Secure Sockets Layer/Transport Layer Security (SSL/TLS)

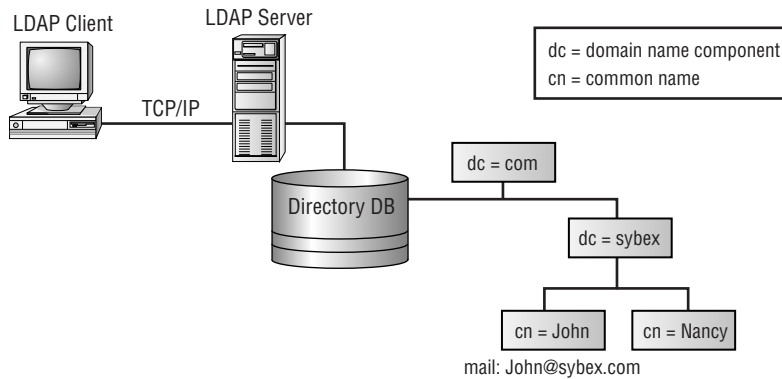
SSL and TLS are covered earlier, in section "2.3 Internet Security."

Lightweight Directory Access Protocol (LDAP)

LDAP is a standardized protocol that enables clients to access resources within a *directory service*. A directory service is a network service that provides access to a central database of information, which contains detailed information about the resources available on a network. LDAP follows the *x.500 standard*, which defines what a directory service is and how it is to be constructed (at least from a foundational infrastructure perspective). Clients can interact with directory service resources through LDAP by using authentication that is at least a minimum of a username and password.

LDAP directory structures are hierarchical data models that use branches like a tree and that have a clearly identified and defined root (see Figure 2.14). LDAP operates over TCP ports 389 and 636. It can employ SSL or TLS to provide authentication and data encryption security.

FIGURE 2.14 An example of an LDAP-based directory services structure



Exam Essentials

LDAP Lightweight Directory Access Protocol (LDAP) is used to allow clients to interact with directory service resources. LDAP is based on x.500 and uses TCP ports 389 and 636. It uses a tree structure with a district root.

2.5 File Transfer Protocols

The full name of this section from the Security+ objectives list is “Recognize and understand the administration of the following file transfer protocols and concepts.” A common activity on the Internet is the exchange of files. Moving files between one system and another can be accomplished using File Transport Protocol (FTP). You should be familiar with the basics about FTP and the secured alternative file transfer solutions.



For more information on this topic, refer to Chapter 3 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

File Transfer Protocol (FTP) is an in-the-clear file exchange solution. It's supported by any computer system using the TCP/IP protocol. An FTP server system is configured to allow authenticated or anonymous FTP clients to log on in order to upload or download files. FTP employs TCP ports 20 and 21 to establish client to server communications; it then uses a randomly selected higher port (above 1023) for file transfers.

The exchange of files is a common practice on the Internet, intranets, and extranets. FTP is platform independent and thus makes file exchanges between different operating systems simple. It's one of the common services deployed in a demilitarized zone (DMZ) (an extension of a private network where Internet users can access services such as Web and e-mail) in order to provide controlled public access to company resources while still allowing internal clients to access the service(s).

Secure File Transfer Protocol (S/FTP)

Secure FTP (S/FTP) is a secured alternative to standard FTP. Standard FTP sends all data, including authentication traffic, in the clear. Thus, there is no confidentiality protection. S/FTP encrypts both authentication and data traffic between the client and server; it employs SSH to provide secure FTP communications.



Other alternatives to standard FTP are to use FTP over an SSL connection or across a VPN link. Either of these options effectively provides protection for all FTP traffic.

No matter what secure FTP solution is employed, both the server and the client must have the same solution. Otherwise, FTP session establishment and subsequent file transfer communications won't be possible.

Blind/Anonymous FTP

Anonymous FTP is a form of nameless logon to an FTP server. Usually, visitors to an FTP site who wish to log on anonymously use the word *anonymous* as the logon name. They're then prompted to provide their e-mail address as the password, but any text string suffices.

Site administrators should carefully configure FTP servers that allow anonymous access. Anonymous users shouldn't be able to download (or, in many cases, view) any files uploaded by anonymous users. Anonymous upload and upload should only be enabled if absolutely necessary. When possible, don't allow both authenticated and anonymous FTP logons on the same FTP site. Most FTP servers have anonymous FTP enabled by default, so usually it must be specifically disabled in order to limit access to authenticated users.

If FTP upload is allowed, especially when anonymous FTP uploading is allowed, ensure that it isn't possible to access upload folders from a web URL. If you don't take this precaution, web visitors may be able to download files from the FTP site through HTTP, or they may be able to execute uploaded files.

Blind FTP is a configuration of anonymous FTP or authenticated FTP where uploaded files are unseen and unreadable by visitors. Thus, users can upload files but not see the resulting uploads. This ensures that your FTP site isn't overrun by file swappers using your system as a file exchange point. File swappers often exchange illegal (unlicensed) copies of software, music, and movies through unsecured FTP servers. Uploaded files on a blind FTP server become accessible only after the administrator has either changed the files' permissions or moved them into a folder configured to allow downloads.

File Sharing

You can support file sharing by deploying an FTP server that allows visitors to upload and download files. Restricting such a site to authenticated logons ensures that only authorized users gain access to the site. Allowing anonymous connections to a file-sharing FTP server encourages the exchange of illegal copies of software, music, and movies.

Vulnerabilities

FTP is an in-the-clear transmission protocol. It's also a fairly old but standardized protocol. This makes FTP servers vulnerable to packet sniffing and possibly naming convention troubles.

Packet Sniffing

Since all FTP traffic is transmitted in the clear, all FTP traffic is vulnerable to packet sniffing and other forms of eavesdropping. It's important not to use the same user account and password on FTP that is used in a secure environment. Otherwise, if an attacker captures your FTP logon traffic, they also obtain the logon credentials needed to log in to your secured network. Always use a separate and distinct user account for FTP logons.

8.3 Naming Conventions

Not all operating systems or file systems support long filenames. If an FTP server's host operating system and file systems only support the 8.3 naming convention, then uploaded files with longer filenames will be automatically truncated to comply with 8.3 restrictions. Likewise, if an FTP client's host operating system and file systems only support the 8.3 naming convention, then downloaded files with longer filenames will be automatically truncated to comply with 8.3 restrictions. In either case, this can result in files that are hard to locate, or filename conflicts.

Exam Essentials

FTP File Transport Protocol (FTP) is an in-the-clear file exchange solution. An FTP server system is configured to allow authenticated or anonymous FTP clients to log on in order to upload or download files. FTP employs TCP ports 20 and 21.

S/FTP Secure FTP (S/FTP) is a secured alternative to standard or basic FTP that encrypts both authentication and data traffic between the client and server. S/FTP employs SSH to provide secure FTP communications.

Anonymous FTP Anonymous FTP is a form of nameless logon to an FTP server. Site administrators should carefully configure FTP servers that allow anonymous access.

Blind FTP Blind FTP is a configuration of anonymous FTP or authenticated FTP where uploaded files are unseen and unreadable by visitors. Thus, users can upload files but not see the resulting uploads.

FTP vulnerabilities Since all FTP traffic is transmitted in the clear, all FTP traffic is vulnerable to packet sniffing and other forms of eavesdropping. Not all operating systems or file systems support long filenames. If an FTP server's host operating system and file systems only support the 8.3 naming convention, then uploaded files with longer filenames will be automatically truncated to comply with 8.3 restrictions.

2.6 Wireless

The full name of this section from the Security+ objectives list is “Recognize and understand the administration of the following wireless technologies and concepts.” Wireless networking has become common on both corporate and home networks. Properly managing wireless networking for reliable access as well as security isn't always an easy or straightforward proposition. This section examines various wireless security issues.



For more information on this topic, refer to Chapter 4 of the *Security+ Study Guide, Second Edition*, by Sybex.

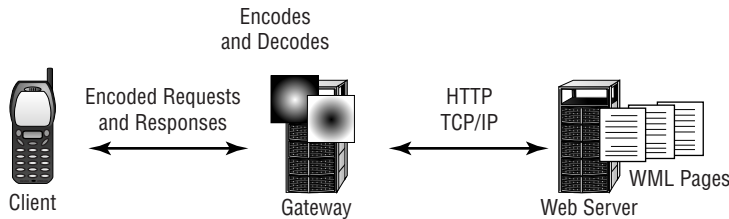
Critical Information

Wireless communication has become an essential part of networking, whether in the home, at the office, or while being mobile about the city. Understanding wireless networking issues and security is an important part of the Security+ exam. This section discusses the following wireless communication issues: WTLS, 802.11, WEP, WAP, wireless vulnerabilities, and site surveys.

Wireless Transport Layer Security (WTLS)

Wireless Transport Layer Security (WTLS) is the security layer for the *Wireless Application Protocol (WAP)*. It provides the security services of privacy, integrity, and authentication for WAP-supporting networks. WTLS is based on TLS. It provides for encrypted traffic between a mobile device and a WAP gateway (see Figure 2.15). WAP is often deployed to support wireless handheld devices like PDAs and cell phones.

FIGURE 2.15 A WAP gateway enables secure communications between an information server (a web server) and a portable handheld device.



802.11 and 802.11x

802.11 is the IEEE standard for wireless network communications. Various versions of the standard have been implemented in wireless networking hardware, including 802.11a, 802.11b, and 802.11g. 802.11x is often used to collectively refer to all of these specific implementations as a group, however 802.11 and 802.11x may be used interchangeably when discussing standard wireless issues. Each version offered slightly better throughput: 2MB, 11MB, and 54MB, respectively. The 802.11 standard also defines Wired Equivalent Privacy (WEP), which provides eavesdropping protection for wireless communications.

Wired Equivalent Privacy/Wireless Application Protocol (WEP/WAP)

Wired Equivalent Privacy (WEP) is defined by the IEEE 802.11 standard. It was designed to provide the same level of security and encryption on wireless networks as is found on wired or cabled networks. WEP provides protection from packet sniffing and eavesdropping against wireless transmissions.

A secondary benefit of WEP is that it can be configured to prevent unauthorized access to the wireless network. WEP uses a predefined shared secret key; however, rather than being a typical symmetric cryptography solution, the shared key is static and shared among all wireless access points and device interfaces. This key is used to encrypt packets before they are transmitted over the wireless link, thus providing confidentiality protection. A hash value is used to verify that received packets weren't modified or corrupted while in transit; thus WEP also provides integrity protection. Knowledge or possession of the key not only allows encrypted communication but also serves as a rudimentary form of authentication, since without it, access to the wireless network is prohibited.

Wireless Application Protocol (WAP) is often deployed to support wireless handheld devices like PDAs and cell phones. WAP employs WTLS for security. WAP environments function using a WAP gateway between the mobile client and the information server.

Vulnerabilities

Wireless networking has made networking more versatile than ever before. Workstations and portable systems are no longer tied to a cable, but can roam freely around an office or environment—anywhere within the signal range of the deployed wireless access points. However, this freedom comes at the cost of additional vulnerabilities. Wireless networks are subject to the same vulnerabilities, threats, and risks as any cabled network, plus there are the additional issues of distance eavesdropping and packet sniffing as well as new forms of DoS and intrusion.

When you're deploying wireless networks, you should deploy wireless access points configured to use *infrastructure mode* rather than *ad hoc mode*. Ad hoc mode means that any two wireless networking devices, including two wireless Network Interface Cards (NICs), can communicate without a centralized control authority. Infrastructure mode means that a wireless access point is required, wireless NICs on systems can't interact directly, and the restrictions of the wireless access point for wireless network access are enforced.

One method used to discover areas of a physical environment where unwanted wireless access might be possible is to perform a site survey.

Site Surveys

A *site survey* is the process of investigating the presence, strength, and reach of wireless access points deployed in an environment. This task usually involves walking around with a portable wireless device, taking note of the wireless signal strength, and mapping this on a plot or schematic of the building. Site surveys should be conducted to ensure that sufficient signal strength is available at all locations that are likely locations for wireless device usage, while at the same time minimizing or eliminating the wireless signal from locations where wireless access shouldn't be permitted (public areas, across floors, into other rooms, or outside the building). A site survey is useful for evaluating existing wireless network deployments, planning expansion of current deployments, and planning for future deployments.

One vulnerability commonly discovered during a site survey is the presence of rogue wireless access points. A wireless access point can be connected to any open network port or cable. Such unauthorized access points usually aren't configured for security or, if they are, aren't configured properly or in line with approved access points. Rogue wireless access points should be discovered and removed in order to eliminate an unregulated access path into your otherwise secured network.

Exam Essentials

WTLS Wireless Transport Layer Security (WTLS) is the security layer for the Wireless Application Protocol (WAP). It provides the security services of privacy, integrity, and authentication for WAP supporting networks. WTLS provides for encrypted traffic between a mobile device and a WAP gateway.

802.11 and 802.11x 802.11 is the IEEE standard for wireless network communications. Versions include 802.11a (2 MB), 802.11b (11 MB), and 802.11g (54 MB). The 802.11 standard also defines Wired Equivalent Privacy (WEP).

WEP Wired Equivalent Privacy (WEP) is defined by the IEEE 802.11 standard. It was designed to provide the same level of security and encryption on wireless networks as is found on wired or cabled networks. WEP provides protection from packet sniffing and eavesdropping against wireless transmissions. A secondary benefit of WEP is that it can be configured to prevent unauthorized access to the wireless network. WEP uses a predefined shared secret key.

WAP Wireless Application Protocol (WAP) employs Wireless Transport Layer Security (WTLS) for security. WAP environments function using a WAP gateway between the mobile client and the information server.

Site surveys A site survey is the process of investigating the presence, strength, and reach of wireless access points deployed in an environment. Site surveys should be conducted to ensure that sufficient signal strength is available at all locations that are likely locations for wireless device usage, while at the same time minimizing or eliminating the wireless signal from locations where wireless access shouldn't be permitted.

Review Questions

1. Which of the following isn't an example of a VPN protocol?
 - A. IPSec
 - B. L2TP
 - C. WTLS
 - D. PPTP
2. Which of the following technologies can be used to add an additional layer of protection between a directory services-based network and remote clients?
 - A. SMTP
 - B. RADIUS
 - C. PGP
 - D. VLAN
3. What TCP port does IMAP function over?
 - A. 143
 - B. 25
 - C. 110
 - D. 443
4. What is the first action you should take when you receive an e-mail that describes a removal process to clean your system from a rapidly spreading high-risk virus?
 - A. Follow the instructions immediately.
 - B. Forward the message to everyone you know.
 - C. Open any attachment enclosed with the message.
 - D. Report the message to your network administrator.
5. Which of the following technologies uses a six-step handshake process to establish a secured session between a web server and a web client?
 - A. IPSec
 - B. TACACS
 - C. SSL
 - D. S/MIME

6. Which of the following threats is eliminated when only signed applets are allowed to download through a web browser?
 - A. CGI
 - B. ActiveX
 - C. Cookies
 - D. Instant messaging
7. LDAP operates over what TCP ports?
 - A. 636 and 389
 - B. 110 and 25
 - C. 443 and 80
 - D. 20 and 21
8. What is a blind FTP site?
 - A. A site where users don't authenticate
 - B. A site where all traffic is encrypted
 - C. A site where only anonymous access is allowed
 - D. A site where users can upload but not download
9. Which is WTLS part of?
 - A. WEP
 - B. L2TP
 - C. WAP
 - D. RADIUS
10. What is the purpose of a site survey?
 - A. Improve wireless signal strength.
 - B. Eliminate unwanted access locations.
 - C. Distribute WEP keys.
 - D. Plan the design of a wired network.

Answers to Review Questions

1. C. WTLS is the security component of WAP. It isn't a VPN protocol. IPSec, L2TP, and PPTP are all VPN protocols.
2. B. RADIUS is a centralized authentication solution that adds an additional layer of security between a network and remote clients. SMTP is the e-mail forwarding protocol used on the Internet and intranets. PGP is a security solution for e-mail. VLANs are created by switches to logically divide a network into subnets.
3. A. IMAP functions over TCP port 143. SMTP functions over TCP port 25. POP functions over TCP port 110. SSL and TLS function over TCP port 443.
4. D. This e-mail is likely a hoax. When you receive an e-mail hoax, the first step is to inform your network administrator. Don't follow its directions, forward it to others, or open any attachments.
5. C. SSL uses a six-step handshake process to establish a secured session between a web server and a web client. IPSec doesn't use a six-step process to establish a secured session between two systems. IPSec is a VPN protocol. TACACS doesn't use a six-step process, nor does it create an encrypted session; TACACS is a centralized authentication system for remote access. S/MIME doesn't use a six-step process, nor does it create an encrypted session; S/MIME is an e-mail encryption solution.
6. B. If only signed applets are allowed to download through a web browser, then you gain protection from unknown sourced ActiveX components. Applet signing doesn't affect CGI, cookies, or IM.
7. A. LDAP operates over TCP ports 636 and 389. POP and SMTP operate over TCP ports 110 and 25, respectively. TLS operates over TCP ports 443 and 80 (SSL operates only over TCP port 443; HTTP operates only over TCP port 80). FTP operates over TCP ports 20 and 21.
8. D. At a blind FTP site, users can upload but not download. An anonymous FTP site is one where users don't authenticate and possibly where only anonymous access is allowed. Only through S/FTP or by using FTP inside SSL or a VPN link is all traffic encrypted.
9. C. WTLS is part of WAP. WEP is a part of 802.11. L2TP is a VPN protocol. RADIUS is a centralized authentication service for remote clients.
10. B. The purpose of a site survey is to eliminate unwanted access locations. Site surveys aren't used to improve wireless signal strength, distribute WEP keys, or plan the design of a wired network.



Chapter

3

Infrastructure Security

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **3.1 Understand security concerns and concepts of the following types of devices**
 - Firewalls
 - Routers
 - Switches
 - Wireless
 - Modems
 - RAS (Remote Access Server)
 - Telecom/PBX (Private Branch Exchange)
 - VPN (Virtual Private Network)
 - IDS (Intrusion Detection System)
 - Network Monitoring/Diagnostics
 - Workstations
 - Servers
 - Mobile Devices
- ✓ **3.2 Understand the security concerns for the following types of media**
 - Coaxial Cable
 - UTP/STP (Unshielded Twisted Pair/Shielded Twisted Pair)
 - Fiber Optic Cable



- Removable Media
 - Tape
 - CD-R (Recordable Compact Disks)
 - Hard Drives
 - Diskettes
 - Flashcards
 - Smartcards

✓ **3.3 Understand the concepts behind the following kinds of Security Topologies**

- Security Zones
 - DMZ (Demilitarized Zone)
 - Intranet
 - Extranet
- VLANs (Virtual Local Area Network)
- NAT (Network Address Translation)
- Tunneling

✓ **3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system**

- Network Based
 - Active Detection
 - Passive Detection
- Host Based
 - Active Detection
 - Passive Detection
- Honey Pots
- Incident Response

✓ **3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system**

- OS/NOS (Operating System/Network Operating System) Hardening
 - File System
 - Updates (Hotfixes, Service Packs, Patches)
- Network Hardening
 - Updates (Firmware)
 - Configuration
 - Enabling and Disabling Services and Protocols
 - Access Control Lists
- Application Hardening
 - Updates (Hotfixes, Service Packs, Patches)
 - Web Servers
 - E-mail Servers
 - FTP (File Transfer Protocol) Servers
 - DNS (Domain Name Service) Servers
 - NNTP (Network News Transfer Protocol) Servers
 - File/Print Servers
 - DHCP (Dynamic Host Configuration Protocol) Servers
 - Data Repositories
 - Directory Services
 - Databases



The Security+ exam tests your knowledge of network concepts and how they relate to implementing and maintaining security. This chapter looks at common network devices, network cabling, network topologies, intrusion detection systems, security baselines, and system hardening. To pass the test and be effective in implementing security, you need to understand the basic concepts and terminology in this chapter.

3.1 Security Devices

The full name of this section from the Security+ objectives list is “Understand security concerns and concepts of the following types of devices.” The devices, primarily hardware, that form a network infrastructure are an essential part of the security of that network. Familiarity with each of the common devices in this section is important for the Security+ exam.

Critical Information

A network is constructed of a wide range of components, including computers, wiring, routers, firewalls, and so on (see Figure 3.1). A clear understanding of these components and their security implications is foundational to understanding security in general. This section examines the security issues of several common networking components.

Firewalls

A *firewall* is a hardware or software component designed to protect one network from another (see Figure 3.2). Often, firewalls are deployed between a private trusted network and a public untrusted network (such as the Internet) or between two networks that belong to the same organization but are from different departments. Firewalls provide protection by controlling traffic entering and leaving a network.

Firewalls manage traffic using *filters*. A filter is just a rule. If a packet meets the identification criteria of a rule, then the action of that rule is applied. If a packet doesn't meet the criteria of a rule, then no action from that rule is applied, and the next rule is checked.

Firewalls usually have lots of filters, which are defined in a priority order. The first rule to match criteria with a packet defines the action to take against that packet; no other subsequent rules are checked. Thus, the first rule to apply to a packet is the only rule applied to a packet.

Filter lists are created with the most specific and detailed rules first, followed by successively more general rules, until a final default universal rule is reached, which specifies denial. Therefore, if a packet fails to meet the criteria of any earlier rule, the last “deny” rule will always be used. This way, only packets meeting the custom-defined filters or rules are allowed to cross the security barrier.

FIGURE 3.1 A typical network infrastructure

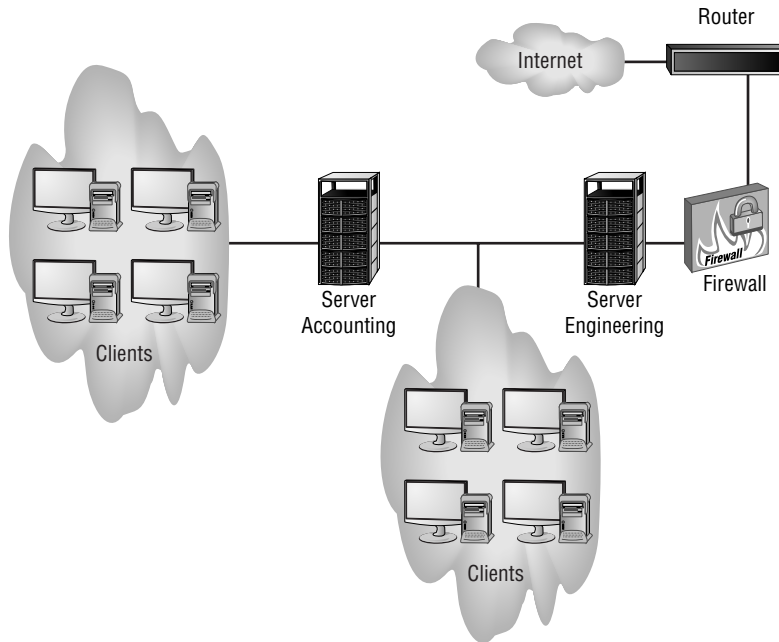
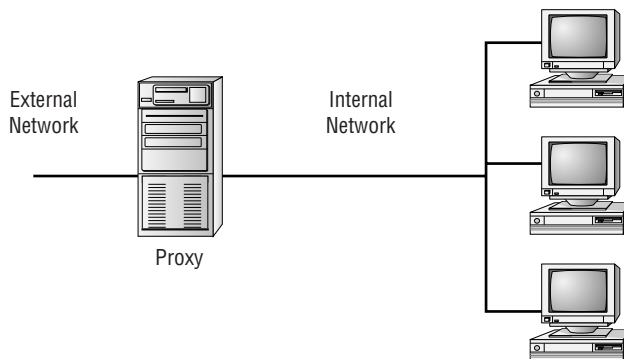


FIGURE 3.2 A proxy firewall blocking network access from external networks



There are three basic types of firewalls, plus an additional form (stateful inspection) that combines the features of the first three:

Packet filter A *packet filter firewall* filters traffic based on basic identification items found in a network packet's header. This includes source and destination address, port numbers, and protocols used. Packet-filtering firewalls operate at the Network layer (layer 3) of the OSI model. They can also be called *common routers*.

Circuit-level gateway A *circuit-level gateway firewall* filters traffic by monitoring the activity within a session between an internal trusted host and an external untrusted host. This monitoring occurs at the Session layer (layer 5) of the OSI model. This type of firewall ensures that the packets involved in establishing and maintaining the circuit (a virtual circuit or session) are valid and used in the proper manner.

Application-level gateway An *application-level gateway firewall* filters traffic based on user access, group membership, the application or service used, or even the type of resources being transmitted. This type of firewall operates at the Application layer (layer 7) of the OSI model. Such a firewall can be called a *proxy*.

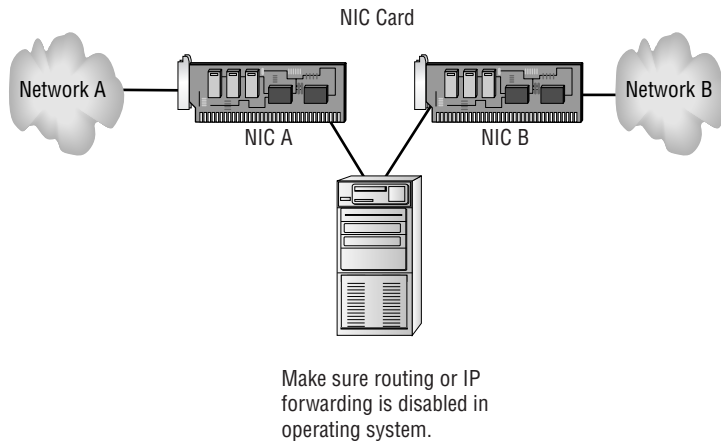
Stateful inspection firewall A *stateful inspection firewall* combines features of the three basic firewall types and includes the ability to understand the context of communications across multiple packets and across multiple layers. Thus a stateful inspection firewall can make more intelligent and complex filtering decisions based on higher-order information. One of the key functions of this type of firewall is to ensure that each packet is part of an established TCP communication session. All rogue, or unassociated, packets are blocked.

The first step in effectively designing, deploying, and implementing a firewall is to design or develop a *firewall policy*: a security policy that focuses on the purposes, uses, functions, and security of the firewalls in an organization. This policy clearly defines how the firewall should filter traffic and the types of traffic that should be blocked or allowed.

Most firewalls are deployed with at least two network interfaces. Such firewalls are called *dual-homed* (see Figure 3.3) or *multi-homed* (for two or more NICs). Dual- or multi-homed firewalls provide a clear security distinction between one network and another; thus packets must successfully pass the filters of a firewall in order to move from one network to another. In this manner, firewalls provide strong and reliable security.

Some firewalls with three or more network interfaces can manage access to multiple networks simultaneously. One common deployment uses one of these additional network interfaces to connect to a demilitarized zone (DMZ). The DMZ hosts publicly accessible servers, such as web or FTP. The firewall provides secured but public access to the DMZ, but it prevents unauthorized access to the private network. If such a multi-homed firewall is compromised, only the systems in the DMZ are directly threatened or exposed.

When a port is opened in a firewall to allow a virtual private network (VPN) connection to take place, keep in mind that all encrypted data will pass through the firewall without being inspected or filtered. A firewall, unless it's the intended communication partner, is unable to view and inspect the contents of encrypted data.

FIGURE 3.3 A dual-homed firewall segregating two networks from each other

Routers

A *router* (see Figure 3.4) is used to connect several network segments. Routers enable traffic from one network segment to traverse into another network segment (see Figure 3.5). However, the traffic must pass through the router's filters in order to make the transition. A common router is basically a packet filtering firewall. Routers direct traffic based on a routing table and grant or deny access using access control lists (ACLs), such as rules or filters. The routing table informs the router which direction to transmit a received packet based on the best-known pathway (route).

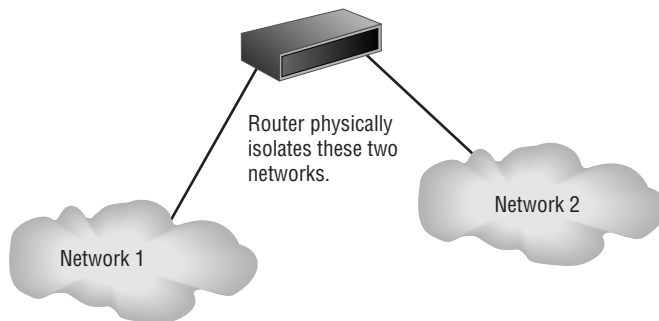
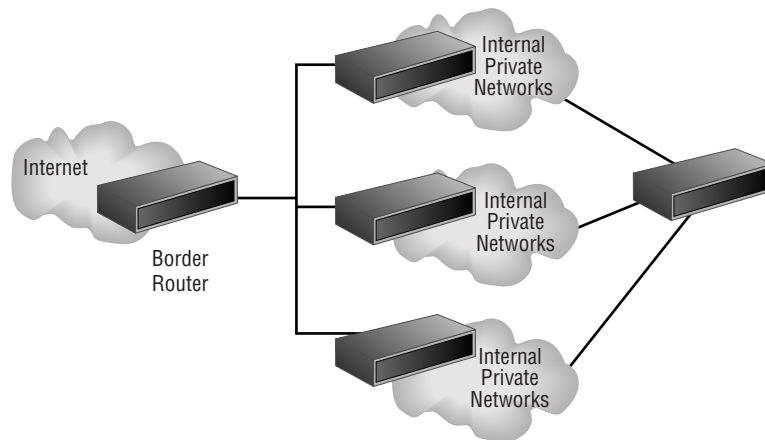
FIGURE 3.4 Router connecting a LAN to a WAN

FIGURE 3.5 A corporate network implementing routers for segmentation and security

Routers can manage traffic for both inbound and outbound communications. An *ingress filter* is a traffic filter on packets coming into a secured area from outside (inbound communications). They're the best defense against IP spoofing attacks. An ingress filter should drop any packet received from an outside source that claims to have originated from an inside source.

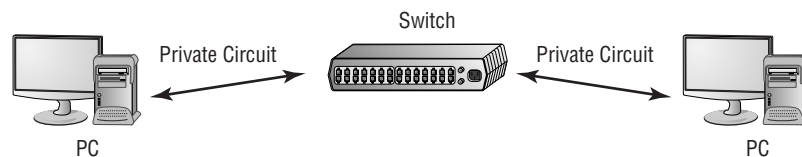
Switches

A *switch* (see Figure 3.6) is like an intelligent multi-port repeater. It receives signals in one port and transmits them out the port where the intended recipient is connected. Switches can be used to connect individual systems or subnets together. They're often used to create *virtual LANs* (VLANs).



See section "3.3 Security Topologies," for a discussion of VLANs.

Switches are good defenses against *sniffing attacks*. A switch transmits messages only on those specific network links between the source and destination systems. A sniffer could only intercept traffic that happened to be transmitted on the segment it was connected to. Thus, using switches instead of hubs is a great defense against sniffing.

FIGURE 3.6 Switching between two systems

Wireless

The Security+ exam focuses on 802.11 and related wireless networking technologies. This includes WTLS, WEP, WAP, 802.11x, related vulnerabilities, and site surveys.



Wireless communications are discussed in more detail in Chapter 2, “Communication Security,” in section “2.6 Wireless.”

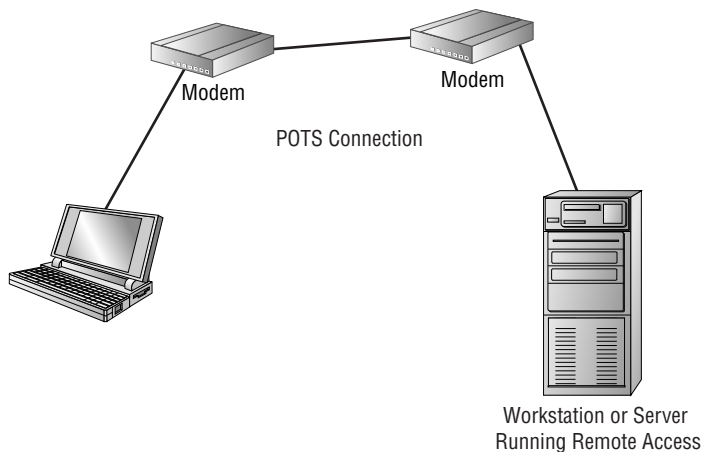
Modems

A *modem* (see Figure 3.7) is a device that creates a network communication link between two computers (or networks) over a telephone line. Modems are one of the slowest remote connection methods still widely supported by operating systems. Most connections are limited to a maximum throughput of 56Kbps. However, since portable systems can use them to connect to corporate offices using any available telephone line, modems will probably be around for years to come.

A common security protection added to dial-in modems is *callback*: a feature that disconnects the remote user immediately after authentication and then calls the remote user back at a predefined number. Callback ensures that the authenticated user is located at the correct phone number before access to the network is granted.

War dialing is a common attack against dial-in modems on a company network. Such an attack dials all the numbers in a prefix range in order to locate modems connected to computer systems. Once attackers locate a modem that answers a computer call, they can focus their efforts on breaking through the logon security barrier.

FIGURE 3.7 A RAS connection between a remote workstation and a Windows server using modems



RAS (Remote Access Server)

A *Remote Access Server (RAS)* is a network server that supports connections from distant users or systems. RAS systems often support modem banks, VPN links, and even Terminal Services connections.



The various types of RAS connections are discussed in Chapter 2, in section “2.1 Remote Access Technologies.”

Telecom/PBX (Private Branch Exchange)

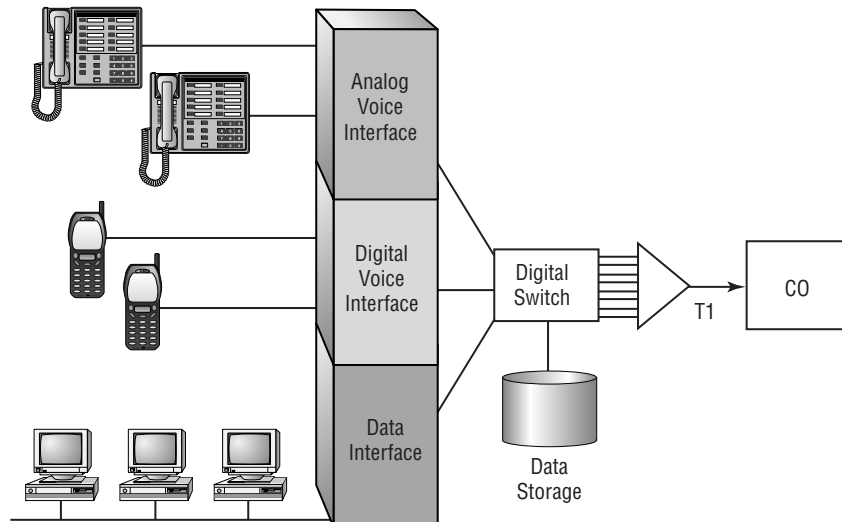
A *private branch exchange (PBX)* (also known as telecom), shown in Figure 3.8, is a computer- or network-controlled telephone system. PBXs are deployed in large organizations; they offer a wide range of telephone services, features, and capabilities including conference calls, call forwarding, paging, call logging, voicemail, call routing, and remote calling.

Remote calling is the ability to dial in to a PBX system from outside and then access a dial tone in order to place a call. The second call can be long distance, and all toll charges are accumulated on the PBX system, not on the user’s telephone. This is a commonly attacked feature of PBX systems.

Methods to secure PBX systems include the following:

- Disabling maintenance features
- Changing all default passwords, accounts, and access codes
- Enabling logging
- Restricting long-distance calling

FIGURE 3.8 A modern digital PBX system integrating voice and data onto a single network connection



VPN (Virtual Private Network)

A *Virtual Private Network (VPN)* is a communication *tunnel* between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted.



Virtual Private Networks (VPNs) are discussed in Chapter 2 in section “2.1 Remote Access Technologies.”

IDS (Intrusion Detection System)

An IDS can detect malicious activity that occurs within the network (it doesn’t cross the firewall) and activity that is able to pass through the firewall. Intrusion Detection Systems (IDSs) are discussed in detail later in this chapter, in section 3.4.

Network Monitoring/Diagnostics

Network monitoring and *diagnostics* are terms for watching the activity of an environment, looking for problems, abnormalities, intrusions, or security policy violations. This topic was discussed in Chapter 1, “General Security Concepts,” in section “1.7 Understanding Auditing.”

In addition to the coverage in Chapter 1 we need to mention *Simple Network Management Protocol (SNMP)*, which is a protocol and problem-management solution. SNMP was designed as a network health-monitoring solution that allowed centralized management of a network environment. SNMP can gather audit-like data on a network level, such as throughput, bandwidth utilization, packet sizes, protocols in use, CPU utilization, open TCP sessions, IP configuration, free disk space, and so on. This information is reported back to the central management console, where the health of the network and individual components is evaluated. SNMP operates over UDP port 161.

Workstations

Workstations are the computer systems that people use to interact with a network. Workstations are also called *clients*, *terminals*, or *end-user computers*.

Access to workstations should be restricted to authorized personnel. One method to accomplish this is to use strong authentication, such as two-factor authentication with a smartcard and a password or PIN.

Servers

Servers are the computer systems on a network that support and maintain the network. Servers provide services or share resources with the network. They require greater physical and logical security protections than workstations because they represent a concentration of assets, value, and capabilities. End users should be restricted from physically accessing servers, and they should have no reason to log on directly to a server—they should interact with servers over a network through their workstations.

Mobile Devices

A *mobile device* is any computer device that doesn't need to be permanently connected to a cable. These may include wireless devices as well as portable systems that can be connected to or disconnected from the network via a cable (such as notebook computers).

Wireless devices, a.k.a. mobile devices, were discussed in Chapter 2, in section “2.6 Wireless.”

Exam Essentials

Firewalls Firewalls provide protection by controlling traffic entering and leaving a network. They manage traffic using filters or rules.

Types of firewalls The three basic types of firewalls are packet filtering, circuit-level gateway, and application-level gateway. A fourth type combines features from these three and is called a stateful inspection firewall.

Routers Routers enable traffic from one network segment to traverse into another network segment. However, the traffic must pass through the router's filters in order to make the transition.

Switches A switch is like an intelligent multi-port repeater. It receives signals in one port and transmits them out the port where the intended recipient is connected. Switches are often used to create VLANs.

Modems A modem is a device that creates a network communication link between two computers (or networks) over a telephone line. Modems are often secured using callback. They're often attacked using war dialing.

PBX A Private Branch Exchange (PBX) (also known as telecom) is a computer- or network-controlled telephone system. Protections for PBX include disabling maintenance features, changing defaults, logging, and restricting long-distance calling.

3.2 Media Security

The full name of this section from the Security+ objectives list is “Understand the security concerns for the following types of media.” Media is a collection of both network communication links as well as commonly recognized removable media types. Understanding each of these types of components and how they affect security is an important part of the Security+ exam.

Critical Information

This section discusses the security implications of network cabling and removable media. You should be familiar with each of these components.

Coaxial Cable

Coaxial cable (see Figure 3.9), commonly known as *coax*, is type of cable that uses a center conductor surrounded by an insulation sheath, which is surrounded by a metal braid that serves as the second conductor. This conductor, in turn, is surrounded by a final insulation covering. Coax cable used in networking is similar to that used by cable television.

Networking coax cable comes in two forms: *10Base2* and *10Base5*. *10Base2*, also known as *ThinNet*, supports communications of 10Mbps, is a *baseband* form of connection, and has a maximum usage length of 185 meters (hence the 2, which is 1.85 hectometers rounded up). *10Base5*, also known as *ThickNet*, supports communications of 10Mbps, is a baseband form of connection, and has a maximum use length of 500 meters. *ThinNet* uses BNC connectors (see Figure 3.10) to connect directly to a NIC or networking device. *ThickNet* uses vampire taps (see Figure 3.11) to connect to an external attachment unit interface (AUI), which is connected to a NIC or networking device.

Common problems with coax cable include bending it past its minimum arc radius, which breaks the center conductor; deploying it past its maximum use length, which causes *attenuation* (loss of signal strength due to excess cable length); and failing to properly terminate the cable (see Figure 3.12), which results in an inability to support communications.

FIGURE 3.9 Coaxial cable construction

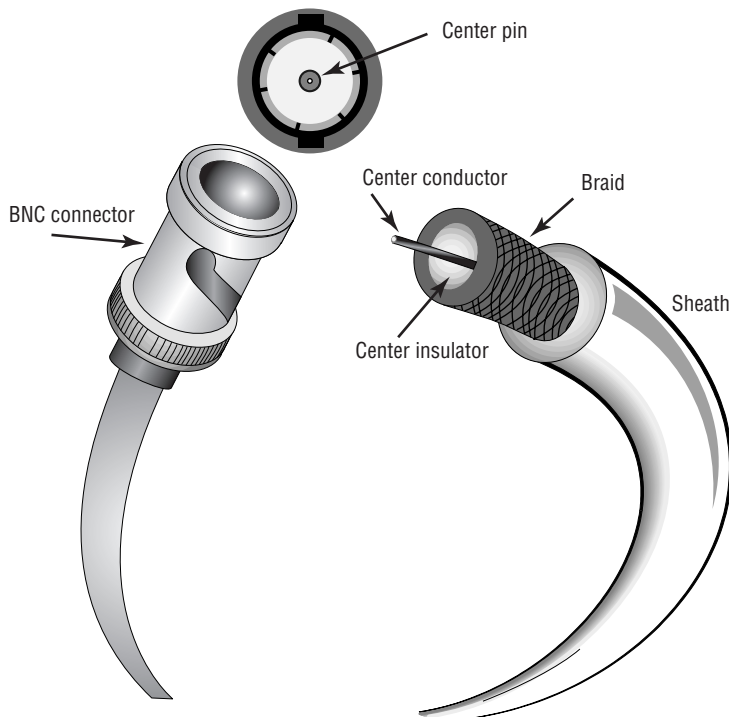


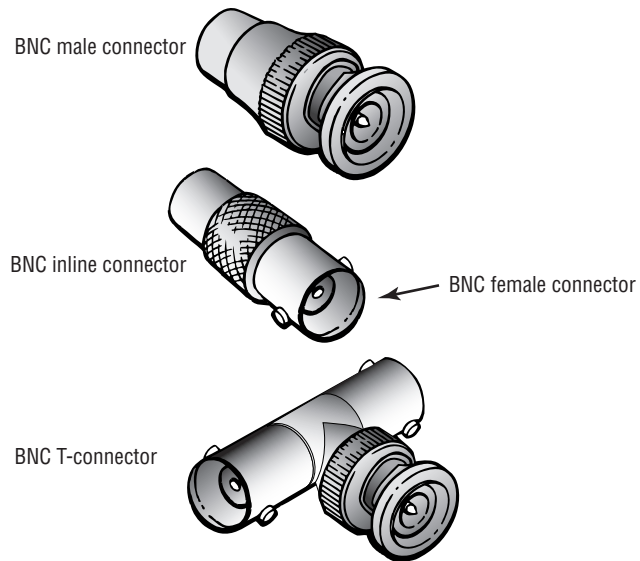
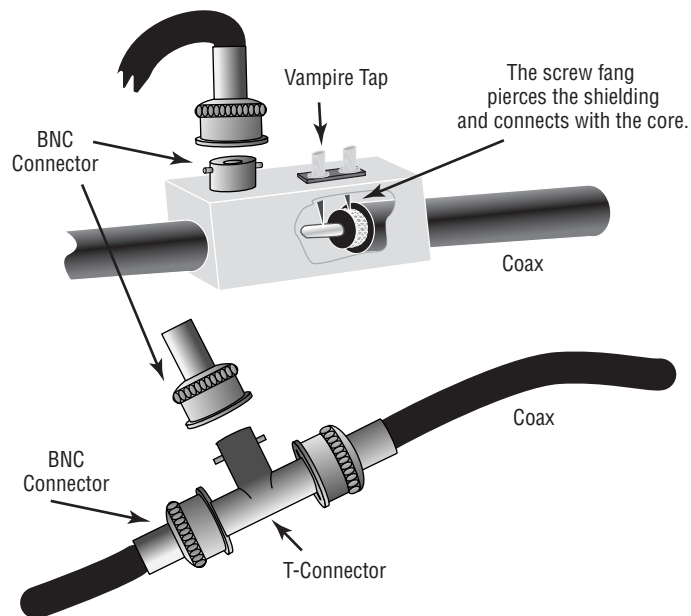
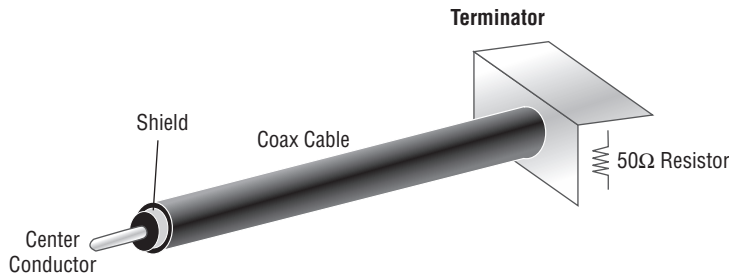
FIGURE 3.10 Common BNC connectors**FIGURE 3.11** A vampire tap and a T-connector on a coax

FIGURE 3.12 Network termination in a coax network

UTP/STP (Unshielded Twisted Pair/Shielded Twisted Pair)

Twisted pair is the most common form of networking cable. It looks similar to a telephone cable, but twisted pair cabling has more wires, and its RJ-45 connector is slightly larger than the RJ-11 or RJ-14 connectors used by telephone cables. Twisted pair cabling is known as *10BaseT*. It supports 10Mbps of throughput, is a baseband form of connection (see Figure 3.13), and has a maximum use length of 100 meters. The *T* in the name indicates that the cable conductors are twisted rather than the maximum use length as was the case for 10Base2 and 10Base5.

There are two forms of 10BaseT wiring: *unshielded twisted pair (UTP)* and *shielded twisted pair (STP)* (see Figure 3.14). The only difference between the two is that STP has a metal foil insulator wrapped around it just under its exterior plastic sleeve. This provides STP with a slightly greater resistance to electromagnetic interference (EMI) and reduces the effect of EMI on other cables.

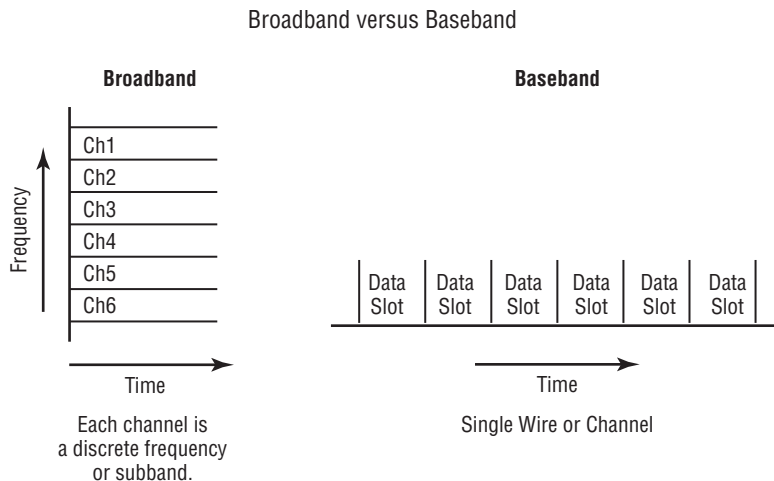
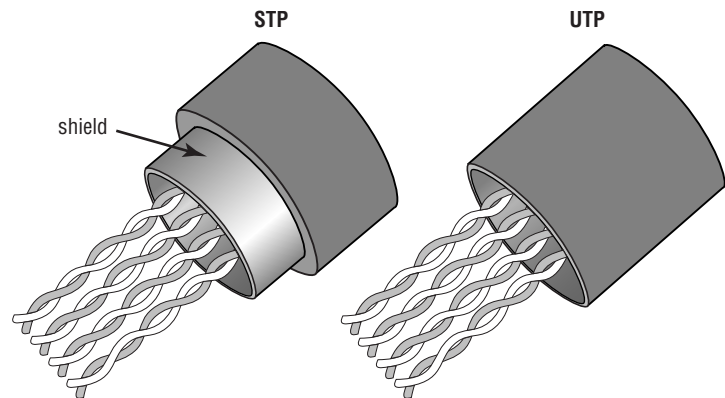
FIGURE 3.13 Baseband versus broadband signaling

FIGURE 3.14 UTP and STP cable construction



Higher throughput forms of twisted pair include 100BaseT and 1,000BaseT, which are 100Mbps (megabit Ethernet) and 1Gbps (gigabit Ethernet) respectively.

UTP and STP are commonly categorized according to their ability to support various speeds of throughput (bandwidth) for communications. Table 3.1 shows the common UTP/STP cable specifications.

Generally, twisted pair wiring is more susceptible to EMI than coax, with UTP the more vulnerable of the two. Twisted pair wiring is also vulnerable to excess cable length, which causes attenuation.

TABLE 3.1 Common UTP/STP Cable Specifications

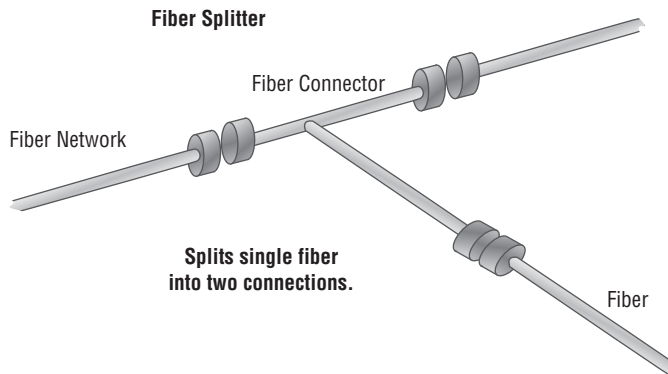
Category	Speed	Usage
Category 1	Voice-grade cable	Used strictly for telephone and modems.
Category 2	4Mbps speed	Used extensively in older mainframe systems.
Category 3	10Mbps Ethernet	Used in 10BaseT networks.
Category 4	16Mbps	Used extensively in Token Ring networks.
Category 5	1,000Mbps	Used in 10-, 100-, and 1,000BaseT and similar networks. The most common wiring in newer networks.
Category 6	1,000Mbps	Used in high-speed network installations. Not yet common.
Category 7	1Gbps	Used in very-high-speed network installations. Not available—a proposed standard.

Fiber Optic Cable

Fiber optic cable (see Figure 3.15) uses pulses of light instead of electric pulses to transmit data. Thus, fiber optic cable isn't susceptible to EMI. It's also considered invulnerable to most eavesdropping and interception attacks.

Fiber optic cabling offers throughputs in excess of 1Gbps and has maximum deployment lengths of 2km to 26km. The drawbacks of fiber optic cabling include its expense; the difficulty of installing it; and its susceptibility to breakage due to cable stress, stretching, and bending.

FIGURE 3.15 Commonly used fiber connectors



Removable Media

Removable media drives are generally considered both a convenience and a security vulnerability. The ability to add and remove storage media to a computer system makes it more versatile. However, it also makes it vulnerable to data theft and malicious code planting.

Removable media include the electronic, logical, or digital storage mechanisms listed in the following sections as well as printed materials. Any time media is no longer needed, it should be properly destroyed to prevent disclosure of sensitive and confidential information to unauthorized entities. For example, failing to destroy printouts or burned CDs may provide dumpster-diving attackers with treasures.

Tape

Tape is a form of removable media commonly used for backup purposes. It's a form of sequential storage, so data elements are written and read in sequential order rather than semirandomly as with hard drives. Tape media often support larger storage capacities than most removable media, excluding hard drives. This makes them suited for backup operations.

Backups will be covered in more detail in Chapter 5, "Operational/Organizational Security," in section "5.2 Disaster Recovery."

CD-R (Recordable Compact Disks)

The topic of CD-Rs or recordable compact disks includes the wide range of optical media that can be written to. This includes CDR, CD-RW, DVD-R, and DVD-RW (plus numerous other variants). Writable CDs and DVDs are often inappropriate for network backups due to their size (a maximum of 650MB or ~4GB), but they're often useful for personal (home) or client level backups. However, the data on a CD isn't protected and thus is vulnerable to unauthorized access if you don't maintain physical control over the media.

Hard Drives

Hard drives are usually thought of as the permanent internal storage devices of a computer. This is true, but hard drives are also available in removable formats. These include hard drives that are plugged into the case or attached by SCSI, USB, or IEEE 1394 (FireWire) connections with their own external power supply connections.

Diskettes

Diskettes, or floppies, are removable media that can store only a small amount of data (about 1.4MB). However, even though they're small, they represent a significant security threat to a protected environment if they get into the wrong hands.

Flashcards

A *flashcard*, or memory card, is a form of storage that uses EEPROM-like memory chips in a small form-factor case. Flashcards often use USB connectors or are themselves inserted into devices like MP3 players and digital cameras. Some flashcards are almost as small as a quarter and are therefore easy to conceal.

Smartcards

Smartcards can be used for a wide variety of purposes. They can be used as an authentication factor (specifically, "something you have"). When used as such, the smartcard hosts a memory chip that stores a password, PIN, certificate, private key, or digital signature. The authentication system uses this stored data item used to verify a user's identity. Smartcards are used as an authentication mechanism by networks, portable computers, PDAs, satellite phones, PKI devices, and more. A smartcard can even function as a credit card (like the American Express Blue card).

A smartcard can also be used as a storage device. Most smartcards have a very limited amount of storage, but sometimes being able to move a few kilobytes of data is all someone needs to steal something of great value. Account numbers, credit card numbers, or a user's private key are all small items that can be very valuable.

Exam Essentials

Cable interference Copper-based cables—coax and twisted pair—are vulnerable to EMI. Fiber optic cable isn't.

Cable eavesdropping Copper-based cables—coax and twisted pair—are vulnerable to eavesdropping. Fiber optic cable isn't.

Removable media Removable media include the electronic, logical, or digital storage mechanisms listed here as well as printed materials. Any time media is no longer needed, it should be properly destroyed to prevent disclosure of sensitive and confidential information to unauthorized entities.

Smartcards Smartcards can be used as an authentication factor (Something You Have). When used as such, the smartcard hosts a memory chip that stores a password, PIN, certificate, private key, or digital signature.

3.3 Security Topologies

The full name of this section from the Security+ objectives list is “Understand the concepts behind the following kinds of Security Topologies.” Knowing how to use security topologies to manage assets of different values is an essential tool in designing, implementing, and sustaining a secure environment.

Critical Information

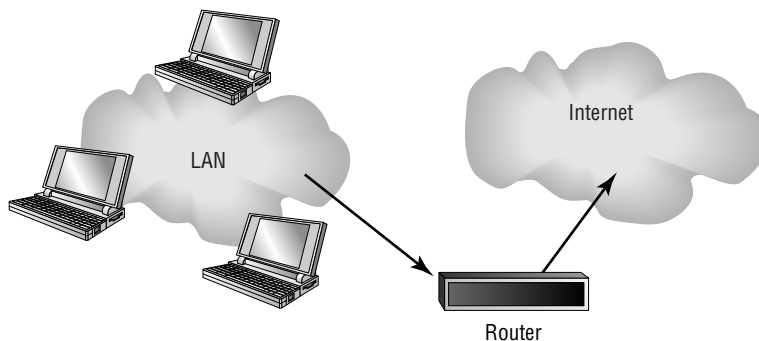
Security topologies are areas, whether physical or logical, that have different levels of security, privacy, protection, sensitivity, or capabilities. The following sections discuss the key security topologies covered on the Security+ exam.

Security Zones

Security zones are additional divisions or segments of a basic LAN-to-Internet connection that allow for supplementary layers of security and control (see Figure 3.16). Each security zone is an area of a network that has a single defined level of security. That security may focus on authorized access, preventing access, protecting confidentiality and integrity, or limiting traffic flow. Different security zones usually host different types of resources with different levels of sensitivity.

The Security+ exam focuses on three specific zones: DMZ, intranet, and extranet.

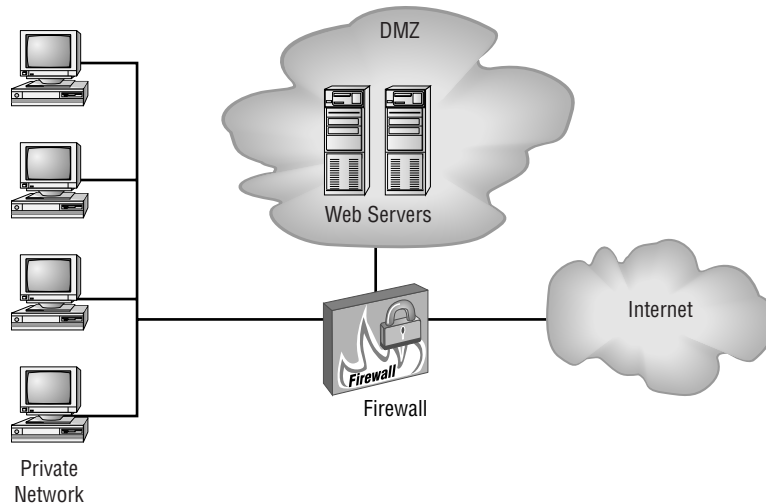
FIGURE 3.16 A typical LAN connection to the Internet



DMZ (Demilitarized Zone)

A *demilitarized zone* (DMZ) (see Figure 3.17) is an area of a network that is designed specifically for public users to access. Access to a DMZ is usually controlled or restricted by a firewall and router system. The DMZ acts as a buffer network between the public untrusted Internet and the private trusted LAN. If the DMZ as a whole or individual systems within the DMZ are compromised, the private LAN is unaffected and uncompromised.

FIGURE 3.17 A typical DMZ



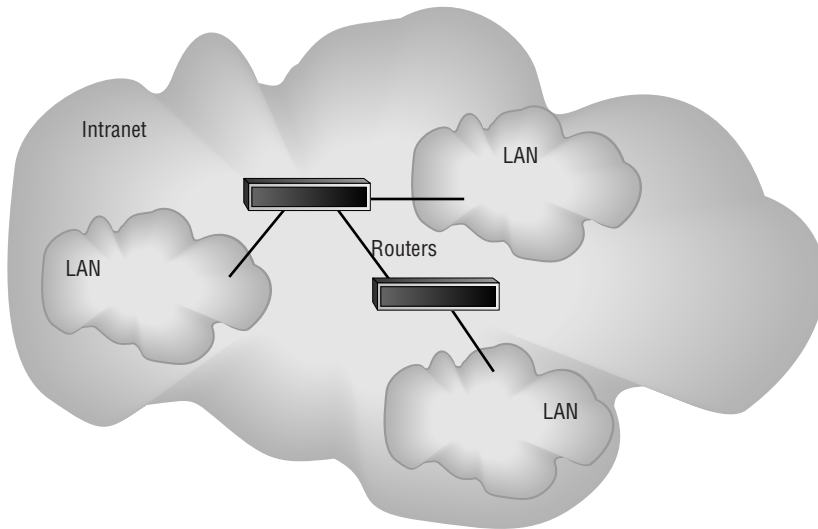
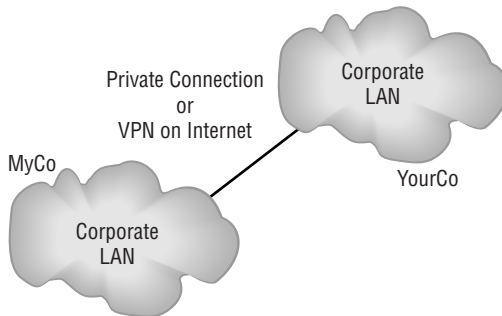
A DMZ gives an organization the ability to offer information services, such as Web, FTP, and e-mail, to both the public and internal clients without compromising the security of the private LAN. Often a DMZ is deployed through the use of a multihomed firewall. Such a firewall has three interfaces: one to the Internet, one to the private LAN, and one to the DMZ.

Intranet

An *intranet* (see Figure 3.18) is any private LAN that uses the same protocol and information services as the Internet. Thus, any private network that uses TCP/IP and offers services such as Web, FTP, e-mail, and so on is an intranet.

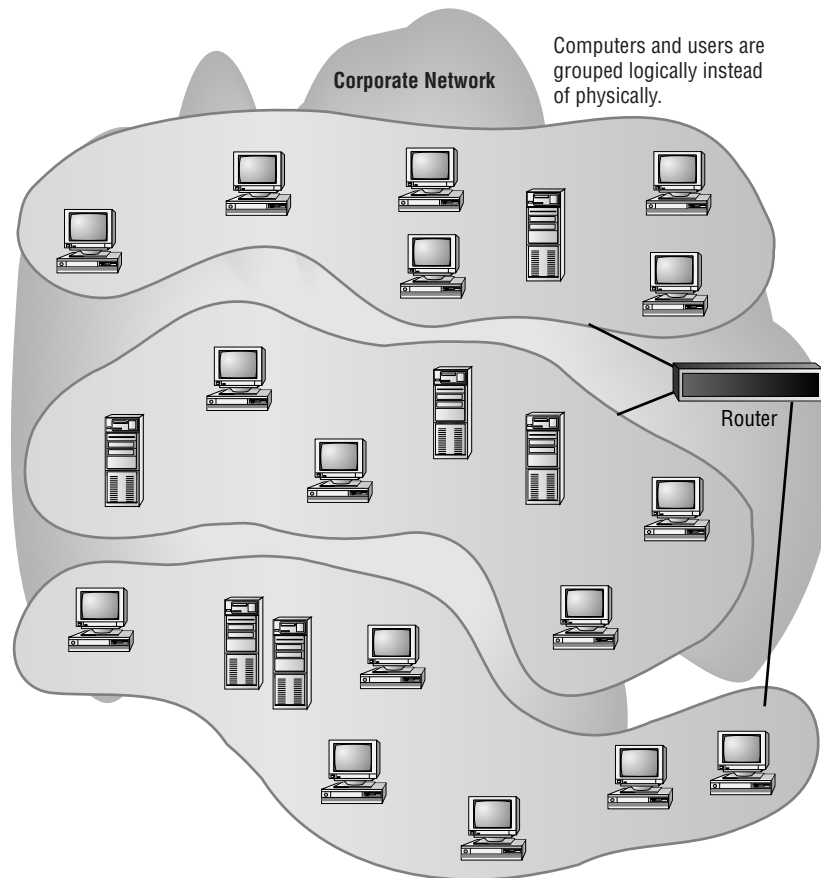
Extranet

An *extranet* (see Figure 3.19) is an intranet that functions as a DMZ for business-to-business transactions. It allows an organization to offer specialized services to business partners, suppliers, distributors, or customers. Extranets are based on TCP/IP and often use the common Internet information services, such as Web, FTP, and e-mail. Extranets aren't accessible to the general public.

FIGURE 3.18 An intranet network**FIGURE 3.19** A typical extranet between two organizations

VLANS (Virtual Local Area Network)

A *virtual local area network (VLAN)* consists of subnets that are logically created out of a single physical network. They're often created using switches (see Figure 3.20). Basically, the ports on a switch are numbered; each port is assigned the designation VLAN1 by default. By assigning ports other designations, such as VLAN2 or VLAN3, you can create additional virtual networks.

FIGURE 3.20 A typical segmented VLAN

VLANs function in much the same way as traditional subnets. In order for communications to travel from one VLAN to another, the switch operates as a router to control and filter traffic between its VLANs.

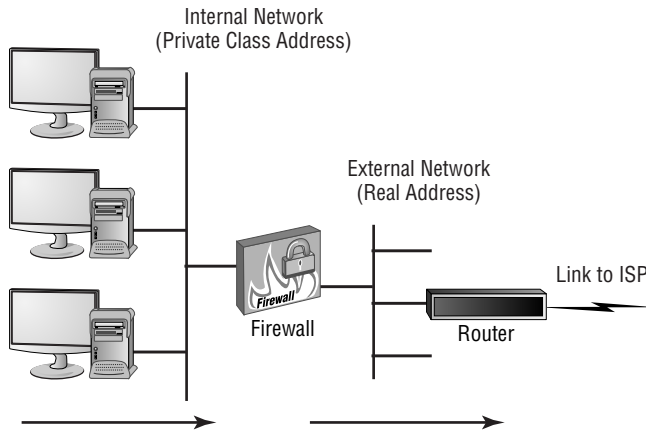
VLANs are used to logically segment a network without altering its physical topology. They're easy to implement, have little administrative overhead, and are a hardware-based solution.

VLANs let you control and restrict broadcast traffic and reduce a network's vulnerability to sniffers. Broadcast traffic isn't automatically forwarded from one VLAN to another, and the sniffer can only see traffic on the segment to which it's connected. This feature of a switch to block broadcasts between VLANs helps protect against broadcast storms. A broadcast storm is a flood of unwanted broadcast network traffic.

NAT (Network Address Translation)

In order for systems to communicate across the Internet, they must have an Internet-capable TCP/IP address. Unfortunately, leasing a sufficient number of public IP addresses to assign one to every system on a network is expensive. Plus, assigning public IP addresses to every system on the network means those systems can be accessed (or at least addressed) directly by external benign and malicious entities. One method around this issue is to use *network address translation* (NAT) (see Figure 3.21).

FIGURE 3.21 A typical Internet connection to a local network



NAT converts the private IP addresses of internal systems found in the header of network packets into public IP addresses. It performs this operation on a one-to-one basis: Thus a single leased public IP address can allow a single internal system to access the Internet. Since Internet communications aren't usually permanent or dedicated connections, a single public IP address could effectively support three or four internal systems if they never needed Internet access simultaneously. So, when NAT is used, a larger network only needs to lease a small number of public IP addresses.

NAT provides several benefits:

- It hides the IP addressing scheme and structure from external entities.
- It serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.
- It reduces expense by requiring fewer leased public IP addresses.
- It allows the use of *private IP addresses* (RFC 1918).

RFC 1918

RFC 1918 defines the ranges of private IP addresses that aren't routable across the Internet. These ranges of addresses were specifically reserved for use by private networks. Anyone can use them at no expense; however, a NAT gateway must be deployed in order for systems using RFC 1918 addresses to communicate with the Internet. The ranges of IP addresses reserved for this purpose by RFC 1918 are

- 10.0.0.0–10.255.255.255 (10/8 prefix): 1 Class A range
- 172.16.0.0–172.31.255.255 (172.16/12 prefix): 16 Class B ranges
- 192.168.0.0–192.168.255.255 (192.168/16 prefix): 255 Class C ranges

Closely related to NAT is *port address translation (PAT)*, which allows a single public IP address to host up to 65,536 simultaneous communications from internal clients (a theoretical maximum, practically you should limit the number to 10 or less in most cases). Instead of mapping IP addresses on a one-to-one basis, PAT also uses the TCP port numbers to host multiple simultaneous communications across each public IP address.

The use of the term *NAT* in the IT industry has come to include the concept of PAT. Thus, when you hear or read about NAT, you can assume that the material is referring to PAT. This is true for most Microsoft Windows operating systems and services; it's also true of the Security+ exam.

Tunneling

Using a special protocol, such as a VPN protocol, to create a communication pathway, known as a tunnel, across an intermediary, often untrusted, network. The concept of tunneling is the basis of VPNs.



Tunneling is discussed in Chapter 2, in section “2.1 Remote Access Technologies.”

Exam Essentials

Security zones A security zone is an area of a network that has a single defined level of security. That security may focus on authorized access, preventing access, protecting confidentiality and integrity, or limiting traffic flow. Different security zones usually host different types of resources with different levels of sensitivity.

DMZs A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet

and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Intranets An intranet is any private LAN that uses the same protocol and information services as the Internet.

Extranets An extranet is an intranet that functions as a DMZ for business-to-business transactions. Extranets let organizations offer specialized services to business partners, suppliers, distributors, or customers.

VLANs Switches are often used to create virtual LANs (VLANs)—a logical creation of subnets out of a single physical network. VLANs are used to logically segment a network without altering its physical topology. They're easy to implement, have little administrative overhead, and are a hardware-based solution.

NAT NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. It hides the IP addressing scheme and structure from external entities. NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request. It reduces expense by requiring fewer leased public IP addresses, and it allows the use of the private IP addresses (RFC 1918).

RFC 1918 RFC 1918 defines the ranges of private IP addresses that aren't routable across the Internet: 10.0.0.0–10.255.255.255 (10/8 prefix), one Class A range; 172.16.0.0–172.31.255.255 (172.16/12 prefix), 16 Class B ranges; and 192.168.0.0–192.168.255.255 (192.168/16 prefix), 255 Class C ranges.

3.4 Intrusion Detection

The full name of this section from the Security+ objectives list is “Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system.” Intrusion detection is the ability to detect security violations occurring across the network or individual systems.

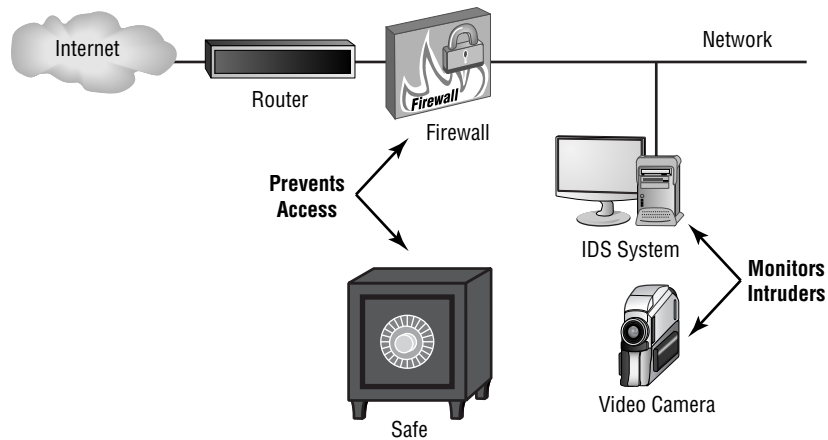
Critical Information

Intrusion detection is an important security capability. *Intrusion Detection Systems (IDS)* are considered complementary security solutions to firewalls (see Figure 3.22). An IDS can detect malicious activity that occurs within the network (it doesn't cross the firewall) and activity that is able to pass through the firewall.

The most common problem with an IDS, excluding misconfiguration, is the occurrence of false positives. A *false positive* occurs when legitimate traffic or user activity is mistaken for intruder activity.

There are two primary forms or types of IDS: network based and host based.

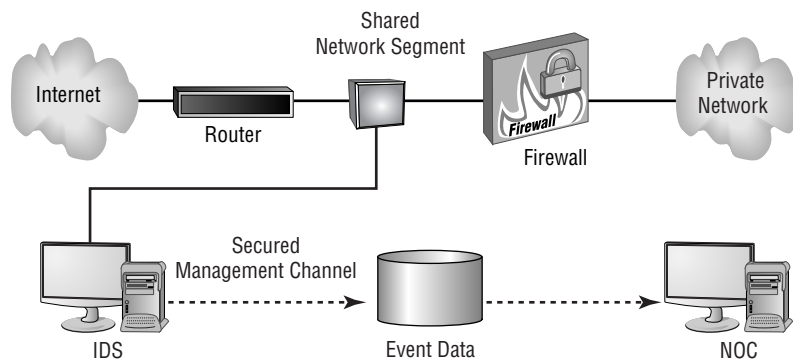
FIGURE 3.22 An IDS and a firewall working together to secure a network



Network Based

A *network-based IDS* (Figure 3.23) watches network traffic in real time. It monitors network traffic patterns, scans packet header information, and may examine the contents of packets to detect security violations or attacks. A network-based IDS is reliable for detecting network-focused attacks, such as bandwidth-based Denial of Service (DoS) attacks.

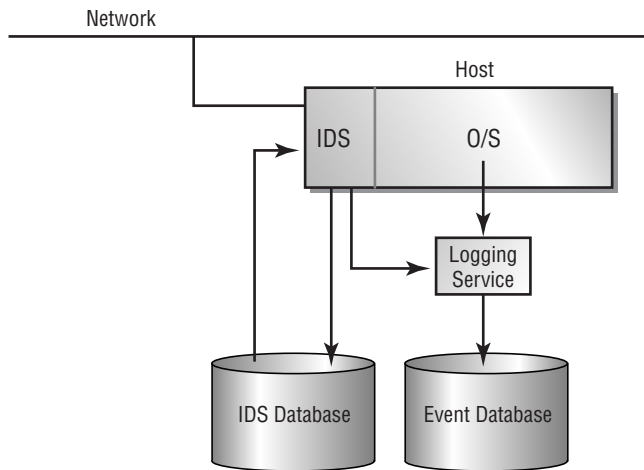
FIGURE 3.23 A network-based IDS placement in a network determines what data will be analyzed.



Host Based

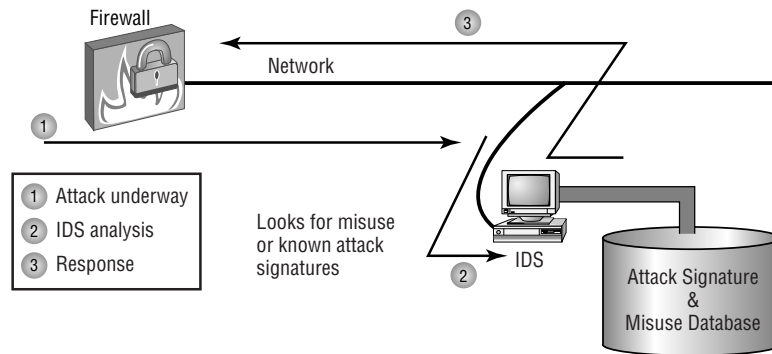
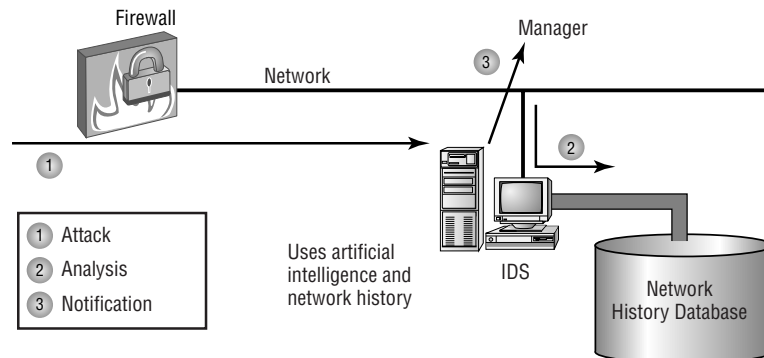
A *host-based IDS* (Figure 3.24) watches the audit trails and log files of a host system. This type of IDS is limited to the auditing and logging capabilities of the host system (which includes the operating system and installed applications and services). A host-based IDS can detect problems only if sufficient information is captured by the host's auditing capabilities. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are perpetrated by a user locally logged in to the host.

FIGURE 3.24 A host-based IDS interacting with the operating system



Active Detection and Passive Detection

As we've just explained, an IDS is an automated system that either watches activity in real time (network-based IDS) or reviews the contents of audit logs (host-based IDS) in order to detect intrusions or security policy violations. There are two common forms of IDS detection mechanisms: *signature detection* and *anomaly detection*. Signature detection (see Figure 3.25) compares event patterns against known attack patterns (signatures) stored in the IDS database. Anomaly detection (Figure 3.26) watches the ongoing activity of the environment and looks for abnormal occurrences. In other words, anomaly-detection IDS is trained on normal activity—it looks for anything that isn't normal.

FIGURE 3.25 A signature-detection IDS in action**FIGURE 3.26** An anomaly-detection IDS using expert system technology to evaluate risks

An IDS (Figure 3.27) with active detection and response is designed to take the quickest action to reduce the potential damage caused by an intruder. This response may include shutting down the server or just the affected service or disconnecting suspicious connections (Figures 3.28 and 3.29).

An IDS with passive detection and response will take no direct action against the intruder; instead it may increase the amount of data being audited and recorded and notify the administrators about the intrusion. IDS is good at detecting DoS attacks; exploitation of bugs, flaws, or hidden features; and port scanning. It isn't reliable for detecting spoofed e-mail.

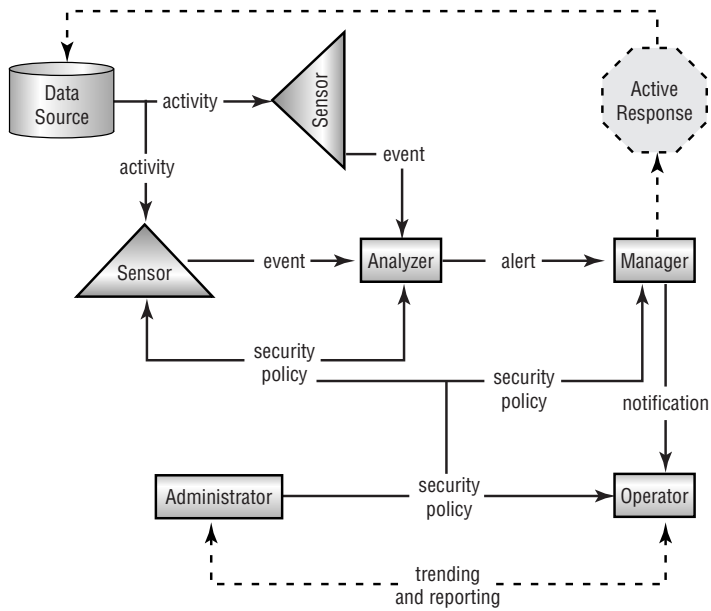
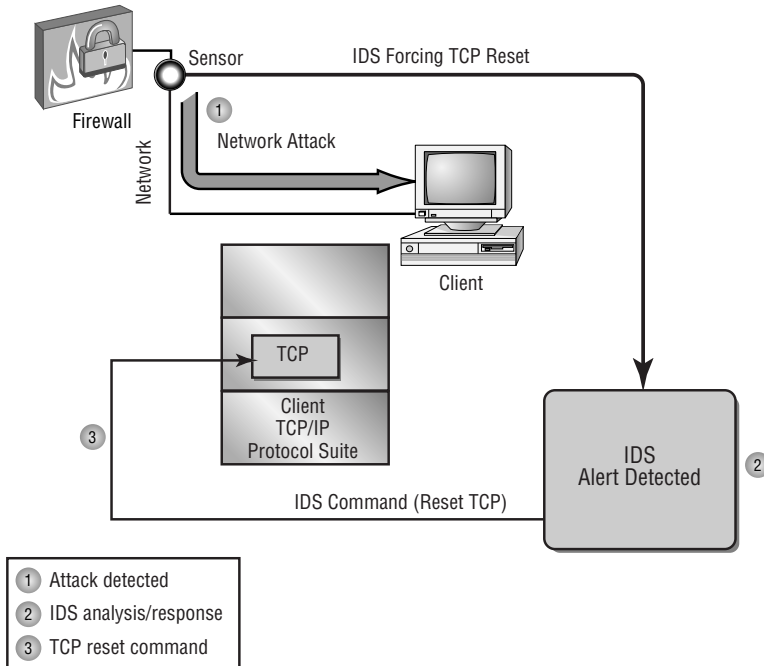
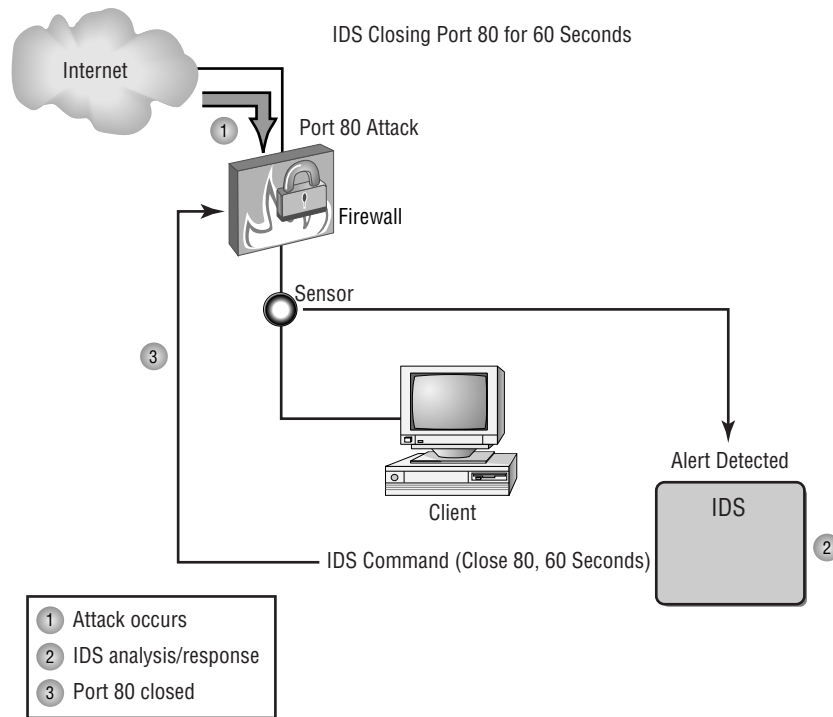
FIGURE 3.27 The components of an IDS working together to provide network monitoring**FIGURE 3.28** IDS instructing TCP to reset all connections

FIGURE 3.29 IDS instructing the firewall to close port 80 for 60 seconds to thwart an Internet Information Server (IIS) attack

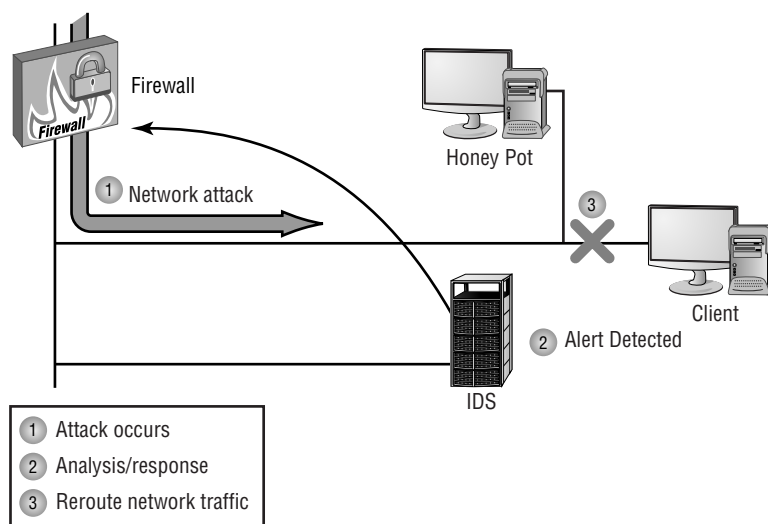


Honey Pots

A *honey pot* (Figure 3.30) is a fictitious environment designed to fool and lure attackers and intruders away from the private secured network. A honey pot is often deployed as a buffer network between an untrusted network, such as the Internet, business partners, or a DMZ, and the private network.

The honey pot looks and acts like a real system or network, but it contains no valuable or legitimate data or resources. Intruders may be fooled into wasting their time attacking and infiltrating a honey pot instead of your actual network. All the activity in the honey pot is monitored and recorded.

The purpose of deploying a honey pot is to provide an extra layer of protection for your private network and to gather sufficient evidence for prosecution against malicious intruders and attackers. A honey pot can often gather sufficient information to determine the identity of the intruder; the type of data, resource, or system being attacked or focused on; and the methods and tools of attack.

FIGURE 3.30 A network honey pot deceives an attacker and gathers intelligence.

Incident Response

When a security breach or perimeter violation is detected, *incident response* must be initiated. The goal of a planned and documented incident response is to limit the amount of damage caused by the incident, to recover the environment as quickly as possible, and to gather information about the incident and the perpetrator in order to prevent a reoccurrence and pursue legal prosecution.



Evidence gathering and forensics are discussed in Chapter 5 “Operational/ Organizational Security,” in section “5.6 Forensics.”

The best way to respond to security violations is to have an incident response plan to follow. This plan defines and describes the procedures to perform in the event of an incident. One of the first steps that should occur when an incident is detected or suspected is to contact the incident response team, which will then follow the procedures in the incident response plan.

Some of the elements commonly found in an incident response plan include:

- Documenting everything, include anything seen on screen
- Making backup copies of all affected files, often using a bit-level drive image duplication process
- Collecting all audit logs (often by creating copies) and securing them against alteration

It’s important not to log off the system or shut down the computer, since these actions may damage or alter evidence.

In the process of responding to an incident, an important goal is to contain the problem. *Containment* means to limit the scope of damage and to prevent other systems or resources from being negatively affected. Containment is especially important when the incident includes virus infection, remote control access, a Trojan horse, a logic bomb, or the use of hacker tools. Malicious use of these components may leave residual elements that are activated at a later time.

Depending on the type of incident (for example, an intrusion attack across a Internet link), the incident response team may choose to disconnect or terminate a network segment or ISP connection. Once an incident has been contained, the incident response team is responsible for documenting the incident and making recommendations about how to improve the environment to prevent a reoccurrence. A final step in incident response is to evaluate the response plan and procedures and improve them as necessary.

Exam Essentials

IDS An Intrusion Detection System (IDS) is an automated system that either watches activity in real time or reviews the contents of audit logs in order to detect intrusions or security policy violations. The two types of IDS are network based and host based.

Network-based IDS A network-based IDS watches network traffic in real time. It's reliable for detecting network-focused attacks, such as bandwidth-based DoS attacks.

Host-based IDS A host-based IDS watches the audit trails and log files of a host system. It's reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

Detection mechanisms Signature detection compares event patterns against known attack patterns (signatures) stored in the IDS database. Anomaly detection watches the ongoing activity of the environment and looks for abnormal occurrences.

Response methods An IDS with active detection and response is designed to take the quickest action to reduce potential damage caused by an intruder. This response may include shutting down the server or the affected service or disconnecting suspicious connections. An IDS with passive detection and response takes no direct action against the intruder; instead it may increase the amount of data being audited and recorded and notify the administrators about the intrusion.

Honey pots A honey pot is a fictitious environment designed to fool and lure attackers and intruders away from the private secured network. The purpose of deploying a honey pot is to provide an extra layer of protection for your private network and to gather sufficient evidence for prosecution against malicious intruders and attackers.

Incident response The goal of a planned and documented incident response is to limit the amount of damage caused by an incident, to recover the environment as quickly as possible, and to gather information about the incident and the perpetrator in order to prevent a reoccurrence and pursue legal prosecution.

3.5 Environment Hardening

The full name of this section from the Security+ objectives list is “Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system.” This section discusses the various aspects of security baselines and system hardening as listed on the Security+ objectives list.

Critical Information

A *security baseline* is a standardized minimal level of security that all systems in an organization must comply with. This lowest common denominator establishes a firm and reliable security structure on which to build trust and assurance. The security baseline is defined by the organization’s security policy. It may include requirements of specific hardware components, operating system versions, service packs, patches/upgrades, configuration settings, add-on applications, service settings, and more.

The basic procedures for establishing a security baseline or hardening a system are as follows:

1. Remove unneeded components, such as protocols, applications, services, and hardware (including device drivers).
2. Update and patch the operating system and all installed applications, services, and protocols.
3. Configure all installed software as securely as possible.
4. Impose restrictions on information distribution for the system, its active services, and its hosted resources.

Documentation is an important aspect of establishing a security baseline and implementing security in an environment. Every aspect of a system, from design to implementation, tuning, and securing, should be documented. Failing to have sufficient documentation is often the primary cause of difficulty in locking down or securing a server. Without proper documentation, all the details about the operating system, hardware configuration, applications, services, updates, patches, configuration, and so on must be discovered before security improvements can be implemented. With proper documentation, a security professional can quickly add to the existing security without having to reexamine the entire environment.

Creating or defining a baseline requires that you examine three key areas of an environment: the operating system, the network, and the applications. The following sections examine issues related to security baseline establishment for these areas.

OS/NOS (Operating System/Network Operating System) Hardening

Operating system hardening is the process of reducing vulnerabilities, managing risk, and improving the security provided by or for an operating system. This is usually accomplished by taking advantage of an operating system’s native security features and supplementing them with add-on applications, such as firewalls, antivirus software, and malicious-code scanners.

Hardening an operating system includes protecting the system from both intentional directed attacks and unintentional or accidental damage. This can include implementing security countermeasures as well as fault-tolerant solutions for both hardware and software. Some of the actions that are often included in a system hardening procedure include :

- Deploy the latest version of the operating system.
- Apply any service packs or updates to the operating system.
- Update the versions of all device drivers.
- Verify that all remote-management or remote-connectivity solutions that are active are secure. Avoid FTP, Telnet, and so on.
- Disable all unnecessary services, protocols, and applications.
- Remove or securely configure Simple Network Management Protocol (SNMP).
- Synchronize time zones across the network and time clock with an official Internet time server.
- Configure event viewer log settings to maximize capture and storage of audit events.
- Rename default accounts.
- Enforce strong passwords on all accounts.
- Force password changes on a periodic basis.
- Restrict access to administrative groups and accounts.
- Hide the last-logged-on user's account name.
- Enforce account lockout.
- Configure a legal warning message that's displayed at logon.
- If file sharing is used, force the use of secure sharing protocols or use VPNs.
- Use a security and vulnerability scanner against the system.
- Scan for open ports.
- Disable *Internet Control Message Protocol* (ICMP) functionality on publicly accessible systems.
- Consider disabling NetBIOS.
- Configure auditing.
- Configure backups.

Two aspects of operating system hardening that should not be overlooked are the file system and updates.

File System

The file system in use on a system greatly affects the security offered by that system. A file system that incorporates security, such as access control and auditing, is a more secure choice than a file system without incorporated security. One great example of a secured file system is the

Microsoft New Technology File System (NTFS). NTFS was first deployed under Windows NT, but it's now found in Windows 2000, Windows XP, and Windows Server 2003. It offers file- and folder-level access permissions and auditing capabilities. An example of a file system that doesn't include security is File Allocation Table (FAT or FAT32); FAT and FAT32 have no security features.

Updates (Hotfixes, Service Packs, Patches)

Security is always a moving target. A system that is secure today may be vulnerable tomorrow. New methods of attacks, new attack tools, new viruses, new weaknesses, accidents in your environment, and much more can cause new risks, threats, and vulnerabilities at any time. Staying vigilant against new security issues is essential in today's business environment. One method to stay as secure as possible is to install updates from vendors.

Vendor *updates* to operating systems, applications, services, protocols, device drivers, and any other software are the absolute best way to protect your environment from known attacks and vulnerabilities. Not all vendor updates are security related, but any error, bug, or flaw that can be exploited to result in damaged data, disclosure of information, or obstructed access to resources should be addressed.

The best procedure to keep your systems updated is as follows:

1. Watch vendor websites for information about updates.
2. Sign up for newsletters, discussion groups, or notifications.
3. Download all updates as they're made available.
4. Test all updates on nonproduction systems.
5. Document changes to your test systems and plan the implementation on production systems.
6. Back up production systems before implementing updates.
7. Implement updates on production systems.
8. Evaluate the effect of the updates on the production systems.
9. If negative effects are discovered, roll back the update.

At least three types of updates are usually discussed as a collective:

Hotfixes A *hotfix* is a single-issue update that corrects a single problem. Hotfixes aren't as thoroughly tested as other updates; they're quickly designed and released to deal with immediate issues and problems. You should install them if you're experiencing the problem they're designed to correct or you're threatened by the vulnerability they're designed to address.

Service packs *Service packs* are collections of hotfixes and other nonreleased updates as a single entity. They're thoroughly tested and generally should be applied to all systems once they're made available. Service packs are cumulative, so you only need to apply the most recent service pack to keep your systems current.

Patches A *patch* is an update that corrects programming flaws that cause security vulnerabilities. Patches are single-issue utilities that are more thoroughly tested than hotfixes.

Network Hardening

Network hardening takes the concept of operating system hardening and applies it to the network. In this instance, the network includes those components on each system that support network communications: the NIC, device drivers, and protocols, as well as the network media (cables or wireless) and network devices (routers, switches, hubs, and so on). Every aspect of a network should be as secure as possible to minimize the potential entry points for an intruder or malicious code. By improving the security of the network, you gain security for each individual system.

Network hardening includes the activities of applying firmware updates and managing configuration issues.

Updates (Firmware)

The issue of updates for network hardening includes all the information discussed earlier for operating system hardening. You must also consider the issue of updating firmware. *Firmware* is the software code stored on memory chips in network devices (such as NIC, routers, and switches). This software code is similar to an operating system but is specifically for network devices. Keeping the firmware updated on all devices is an important part of maintaining a network's security.

Configuration

Proper configuration of systems connected to the network directly affects the security of the overall network. A weak system serves as the weak link in an environment. If one system is compromised, it could lead to the compromise of other systems on the network. It's important to impose strong security on every computer system and device connected to a network. This includes securing systems using the aspects of operating system hardening and application hardening.

In addition to operating system hardening and application hardening, network hardening procedures should include or address the following:

- Limit access to network devices to administrators.
- Password-protect or account-lock all configuration consoles on network devices.
- Restrict and monitor access to logical and physical console access to network devices.
- Use secure remote network devices administration tools, such as Secure Shell (SSH), instead of Telnet.
- Disable all unneeded network services, applications, and protocols.
- Disable all unneeded interfaces or connections.
- Close all unused ports.
- Use a firewall to monitor and control use of ports at network borders.
- Use access control lists on all network border devices to manage access and limit network traffic.
- Consider using static routing instead of dynamic routing.
- Use updated routing protocols.

- Log network activity, especially on network border devices.
- Keep all network devices time synchronized.
- Securely configure or remove SNMP.

ENABLING AND DISABLING SERVICES AND PROTOCOLS

Disabling unnecessary services and protocols will reduce a system's vulnerability to external attacks. This topic is discussed in Chapter 1, in section "1.3 Identify Non-Essential Services."

ACCESS CONTROL LISTS

Access control lists (ACLs) for networking hardening are similar to those used to manage access to file resources. You can use ACLs to strictly control which users can communicate across the network using the services, applications, protocols, and ports enabled on the network.

Application Hardening

Application hardening is the task of imposing security on required applications and services. This usually involves tuning and configuring the native security features of the installed software and installing supportive security applications as needed. When you're developing new applications in house, it's also important to include security design, implementation, and integration throughout the development process.

Application hardening is often seen as a subelement of operating system hardening. In fact, many of the same steps and procedures used to lock down an operating system are used to harden an application or service. In addition to the general notion of disabling any unneeded protocols and services, you should also disable any unneeded features, functions, or capabilities of a service or protocol based on the server's role and the capabilities your organization needs.

In addition to the hardening steps already discussed, you should be familiar with the additional steps to secure common roles found on a network. These include:

- Web
- E-mail
- FTP
- Domain Name Service (DNS)
- Network News Transfer Protocol (NNTP)
- File and printer sharing
- Dynamic Host Configuration Protocol (DHCP)
- Databases

The following sections detail additional steps relevant to the server function that haven't already been included in the previous discussions of operating system, networking, and application hardening.

Updates (Hotfixes, Service Packs, Patches)

The issue of updates for application hardening is exactly the same as that for operating system hardening.

Web Servers

Web servers are used to offer web resources to public and/or private visitors. Web communications can be secured by requiring authenticated access instead of anonymous access. Web traffic can be secured by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) (for more information, see Chapter 2, in section “2.3 Internet Security”).

For web servers hosting CGI scripts, the folder hosting those scripts should be executable. No other folder in the web resource folder hierarchy should be executable. Visitors to the website should not have write access to any folder in the web resource folder hierarchy.

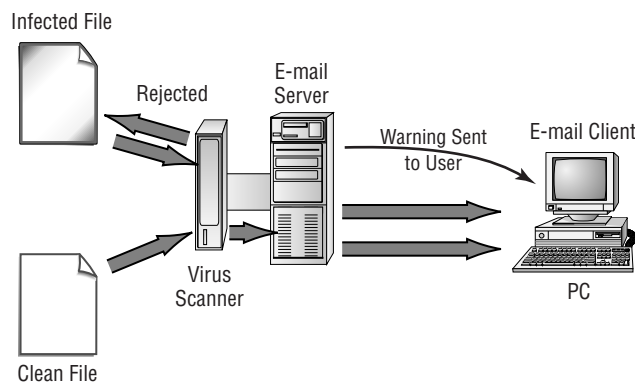
Buffer overflow attacks are common against web servers. Once vulnerabilities are discovered in a commonly used web server application, exploitations of those vulnerabilities are quick to spread across the Internet. It's important to keep web server software patched whenever the vendor releases updates.

Even though access to web resources can be anonymous, you can still control access at a file system level using ACLs. Anonymous visitors without the minimum of read access to web resources will be unable to view or access those resources. Likewise, on web servers using authenticated access, only those resources to which the specific user (whether directly or through group memberships) is granted access can be viewed and accessed through the user's web browser.

E-mail Servers

A common problem with e-mail is that it's the most prevalent distribution mechanism for malicious code on the Internet. Rigid antivirus scanning (see Figure 3.31) and attachment monitoring are necessary to prevent this essential business communication tool from being a serious vulnerability.

FIGURE 3.31 E-mail virus scanner on an e-mail server



To prevent the transmission of e-mails from nonexistent domains (spoofed source addresses), an e-mail server should perform a reverse DNS lookup on all received messages before transmitting or forwarding them.

E-mail should be protected through the use of software and logical security mechanisms as well as an acceptable use policy. The acceptable use policy will reduce the level of user misuse and abuse of the company's e-mail capabilities.



Most of the general e-mail security issues, especially those related to SMTP and encryption, are discussed in Chapter 2.

FTP (File Transfer Protocol) Servers

FTP is used to transfer files to and from a designated FTP server. FTP is often used over the Internet, but it offers no security.



FTP issues are discussed in Chapter 2, in section "2.5 File Transfer Protocols."

DNS (Domain Name Service) Servers

Domain Name Service (DNS) resolves human-friendly domain names, like `microsoft.com`, into IP addresses. The Network layer (layer 3 of the OSI model) uses the IP address to direct network traffic from source to destination. This resolution activity is essential to the proper working of all Internet and intranet communications. DNS is also a critical component of Microsoft's Active Directory.

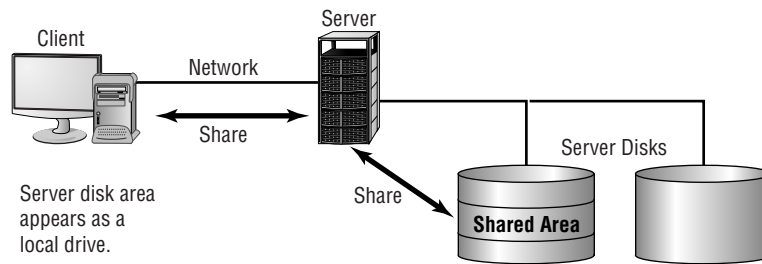
In many cases, multiple DNS servers are deployed on a network to provide fault tolerance and load balancing. When a change occurs on one DNS system, it's sent to the other servers on the network through a mechanism known as *zone transfer*. Zone transfers occur automatically and can be initiated manually. Illegal zone transfers can corrupt the DNS database or give an external entity information about the infrastructure of your private network. Zone transfers should be secured so that they only occur between trusted systems and only authorized users can initiate them.

NNTP (Network News Transfer Protocol) Servers

If your company hosts a Network News Transfer Protocol (NNTP) server, you can secure it by allowing only authorized user access. Activity on the NNTP server should be monitored and logged for signs of malicious activity or abuse of the service.

File/Print Servers

A *file server* is a network server that offers file access to network clients (see Figure 3.32). An FTP server is an example of a public or Internet file server, but any type of server that users can use to upload and/or download files is a file server. Methods to secure file servers include restricting access to authorized users, logging activity, and imposing quota limits on storage space usage.

FIGURE 3.32 Network share connection

A *print server* is a network server offering a shared network printer for use by network users. Methods to secure print servers include restricting access to authorized users and logging activity. The ability to manage printers, especially to update device drivers, should be restricted to administrators.

DHCP (Dynamic Host Configuration Protocol) Servers

Dynamic Host Configuration Protocol (DHCP) is used to assign IP address configuration to systems upon connecting to a network. DHCP allows centralized management of IP addressing schemes. This in turn simplifies administration when subnets, gateways, and DNS server addresses change.

You can secure DHCP servers by limiting DHCP traffic outside of the subnets or networks where it's used. It's especially important to prevent DHCP traffic from leaving your network and entering the Internet. The DHCP protocol functions over TCP ports 67 and 68; these two ports should be blocked on every border device.

Data Repositories

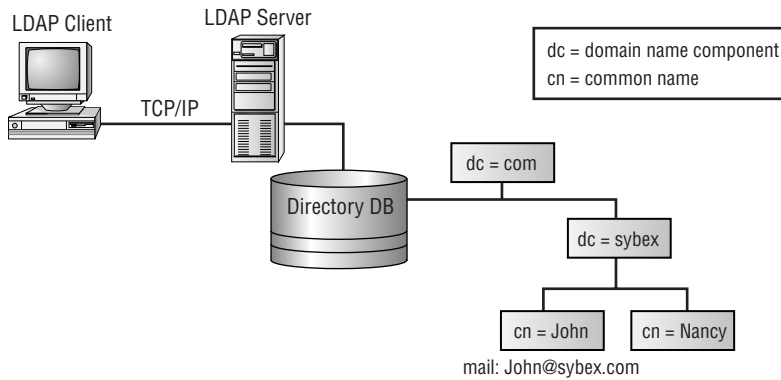
A *data repository server* is any type of server that hosts a service or application that offers resources to users. This includes all the types of servers already mentioned, but the Security+ exam specifically uses this term to refer to directory service servers and database servers.

DIRECTORY SERVICES

A *directory service server* is often called a *domain controller* or an *authentication server*. It's responsible for managing access to the resources of a network (Figure 3.33). A directory service is a form of telephone directory for the resources within a network. It includes a list of all servers, clients, users, groups, and shared resources such as files and printers.



Directory services are discussed in Chapter 2, in section "2.4 Directory Security."

FIGURE 3.33 Directory structure showing the unique identification of a user

DATABASES

A database server hosts a database application where significant amounts of data are stored. Database servers grant users access to the data stored in them through a limited or restricted interface. This interface, sometimes called a *view*, gives the user access only to those functions they're authorized to perform and only to those elements of data they're authorized to see, view, read, or otherwise interact with. In most cases, user access to databases is indirect. This indirect access mechanism provides environment designers and administrators with an additional layer of security and protection. Through indirect access, you can protect the data in a database from integrity violations as well as confidentiality violations.

Exam Essentials

Security baselines A security baseline is a standardized minimal level of security that all systems in an organization must comply with. This lowest common denominator establishes a firm and reliable security structure upon which to build trust and assurance. The security baseline is defined by the organization's security policy.

Documentation Documentation is an important aspect of establishing a security baseline and implementing security in an environment. Every aspect of a system, from design through implementation, tuning, and securing, should be documented. Failing to have sufficient documentation is often the primary cause of difficulty in locking down or securing a server.

Operating system hardening Operating system hardening is the process of reducing vulnerabilities, managing risk, and improving the security provided by or for an operating system. This is usually accomplished by taking advantage of the native security features of an operating system and supplementing them with add-on applications, such as firewalls, antivirus software, and malicious-code scanners.

File system security The file system in use on a system greatly affects the security offered by that system. A file system that incorporates security, such as access control and auditing, is a more secure choice than a file system without incorporated security.

Updates Vendor updates to operating systems, applications, services, protocols, device drivers, or any other software is the absolute best way to protect your environment from known attacks and vulnerabilities. Updates include hotfixes, service packs, and patches. All updates should be tested before deployment in a production environment.

Network hardening Network hardening takes the concept of operating system hardening and applies it to the network. In this instance, the network consists of those components on each system that support network communications, which includes the NIC, device drivers, and protocols, as well as the network media (cables or wireless) and network devices (such as routers, switches, hubs, and so on).

Network configuration security Proper configuration of systems connected to the network directly affects the security of the overall network. A weak system serves as the weak link in an environment. If one system is compromised, it could lead to the compromise of other systems on the network.

ACLs on a network Access control lists (ACLs) for networking hardening are similar to those used to manage access to file resources. You can use ACLs to strictly control which users can communication across the network using the various services, applications, protocols, and ports enabled on the network.

Application hardening Application hardening is the task of imposing security on required applications and services. This usually involves tuning and configuring the native security features of the installed software and installing supportive security applications as needed. When you're developing new applications in house, it's also important to include security design, implementation, and integration throughout the development process.

Web server hardening You can improve web server security through the use of SSL or TLS. Only CGI folders should have execute permissions. Web servers should be patched against buffer overflow attacks. Web resource access can be controlled through file-level ACLs.

E-mail server hardening To prevent the transmission of e-mails from nonexistent domains (spoofed source addresses), an e-mail server should perform a reverse DNS lookup on all received messages before transmitting or forwarding them. E-mail should be protected through the use of software and logical security mechanisms as well as an acceptable use policy.

DNS server hardening Illegal zone transfers can corrupt the DNS database or give an external entity information about the infrastructure of your private network. Zone transfers should be secured so that they only occur between trusted systems and only authorized users can initiate them.

Review Questions

1. Firewalls provide security through what mechanism?
 - A. Watching for intrusions
 - B. Controlling traffic entering and leaving a network
 - C. Requiring strong passwords
 - D. Preventing misuse of company resources
2. A switch can be used to prevent broadcast storms between connected systems through the use of what?
 - A. SSL
 - B. S/MIME
 - C. VLANs
 - D. LDAP
3. Which form of cable media that is least vulnerable to eavesdropping?
 - A. Fiber optic
 - B. STP
 - C. Coax
 - D. Wireless
4. Smartcards are useful for storing all but which of the following types of data?
 - A. Digital signatures
 - B. Digital certificates
 - C. Biometric reference profile
 - D. System backups
5. Which of the following allows the deployment of a publicly accessible web server without compromising the security of the private network?
 - A. Intranet
 - B. DMZ
 - C. Extranet
 - D. Switch

6. Which of the following is *not* one of the IP address ranges reserved for private use by RFC 1918?
 - A. 10.0.0.0–10.255.255.255
 - B. 192.168.0.0–192.168.255.255
 - C. 169.0.0.0–169.255.255.255
 - D. 172.16.0.0–172.31.255.255
7. A network-based IDS is *not* suitable for detecting or protecting against which of the following?
 - A. E-mail spoofing
 - B. Denial of Service attacks
 - C. Attacks against the network
 - D. Attacks against an environment that produce significant traffic
8. What tool is used to lure or retain intruders in order to gather sufficient evidence without compromising the security of the private network?
 - A. Firewall
 - B. IDS
 - C. Router
 - D. Honey pot
9. Which of the following actions in operating system hardening should come earliest in the process?
 - A. Enable secure remote administration.
 - B. Remove unneeded services and protocols.
 - C. Enable logging and auditing.
 - D. Connect the system to the network/Internet.
10. Illegal or unauthorized zone transfers are a significant and direct threat to what type of network server?
 - A. Web
 - B. DHCP
 - C. DNS
 - D. Database

Answers to Review Questions

1. B. Firewalls provide protection by controlling traffic entering and leaving a network.
2. C. Switches can create VLANs. Broadcast storms aren't transmitted between one VLAN and another.
3. A. Fiber optic cable is nearly invulnerable to eavesdropping.
4. D. A smartcard has only a small amount of memory; thus it isn't suited to store system backups.
5. B. A DMZ provides a network segment where publicly accessible servers can be deployed without compromising the security of the private network.
6. C. The 169.x.y.z range is the Automatic Private IP Addresses (APIPA) range of addresses that are automatically assigned to Windows clients when a DHCP server isn't reachable.
7. A. Network-based IDSs aren't suitable for protecting against e-mail spoofing.
8. D. A honey pot is used to lure or retain intruders in order to gather sufficient evidence without compromising the security of the private network.
9. B. Removing unneeded services and protocols is an operating system hardening step that should come before any of the other three.
10. C. Illegal or unauthorized zone transfers are a significant and direct threat to DNS servers.



Chapter

4

Basics of Cryptography

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **4.1 Be able to identify and explain the following different kinds of cryptographic algorithms**
 - Hashing
 - Symmetric
 - Asymmetric
- ✓ **4.2 Understand how cryptography addresses the following security concepts**
 - Confidentiality
 - Integrity
 - Digital Signatures
 - Authentication
 - Nonrepudiation
 - Digital Signatures
 - Access Control
- ✓ **4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure)**
 - Certificates
 - Certificate Policies
 - Certificate Practice Statements
 - Revocation
 - Trust Models
- ✓ **4.4 Identify and be able to differentiate different cryptographic standards and protocols**

✓ **4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles**

- Centralized vs. Decentralized
- Storage
 - Hardware vs. Software
 - Private Key Protection
- Escrow
- Expiration
- Revocation
 - Status Checking
- Suspension
 - Status Checking
- Recovery
 - M of N Control (Of M appropriate individuals, N must be present to authorize recovery)
- Renewal
- Destruction
- Key Usage
 - Multiple Key Pairs (Single, Dual)



The Security+ exam will test your knowledge of cryptography. You will need to be familiar with both symmetric and asymmetric cryptography as well as hashing, certificates, and digital signatures.

Make the effort to memorize the various examples of cryptography discussed in this chapter.

4.1 Cryptographic Algorithms

The full name of this section from the Security+ objectives list is “Be able to identify and explain the of the following different kinds of cryptographic algorithms.” This first section in the cryptography domain is an introduction to the three basic divisions of cryptography. A firm grasp of these initial concepts will assist you in understanding the more complex issues presented in later sections of this domain.



For more information on the various cryptography algorithms, see Chapter 7 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

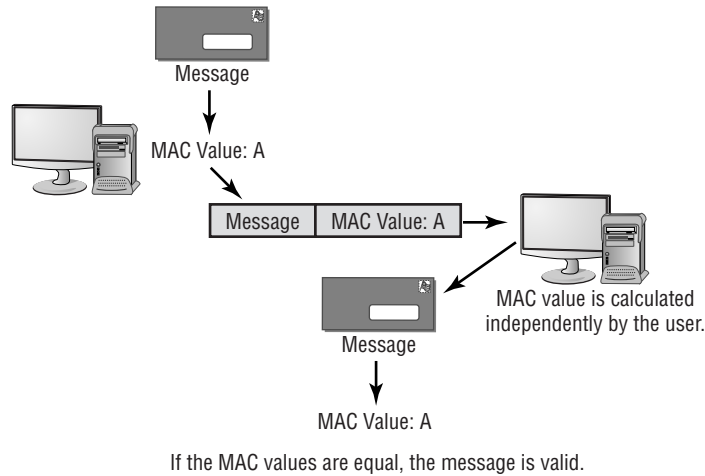
There are three basic divisions in cryptography: hashing, symmetric cryptography, and asymmetric cryptography. Hashing relates to a form of digital ID. The latter two relate to the type of encryption and decryption processes. You need to be familiar with each of these cryptography concepts and recognize examples of them.

Hashing

Hashing is a type of cryptography that isn't an encryption algorithm. Instead, hashing is used to produce a unique identifier—known as a hash value, hash, checksum, message authentication code (MAC), fingerprint, or message digest—of data. The data could be a file, a hard drive, a network traffic packet, or an e-mail message. The hash value is used to detect when changes have been made to a resource. In other words, hashing is used to detect violations of data integrity.

For example, a hash value computed now may be compared with a hash value created last week. If the two values are the same, the data hasn't been changed. If the two values are different, then the data has been modified. Figure 4.1 shows the basic functionality of a hash or MAC value.

FIGURE 4.1 The MAC value is calculated by the sender and the receiver using the same algorithm.



Unlike traditional cryptography, which transforms data into ciphertext, hashing produces a hash value without modifying the original data. Because of this special feature, hashing can be used to protect or verify data integrity. It can also be used to verify whether a copy procedure produced an exact duplicate of a data set. For example, when a hard drive is being imaged to create an exact duplicate (as is done in forensic investigations), a hash is produced of the original drive before the duplication process. Then a hash is produced of the original drive and the duplicate drive after the duplication process. If the two hashes of the original drive are the same, no modifications have occurred to the original drive. If the duplicate drive's hash value is the same as the original drive's, then that proves the duplicate is an exact copy of the original.

Hashing takes a variable-length input and produces a fixed-length output. For example, Message Digest 5 (MD5) is a 128-bit hash algorithm. This means that no matter what the size of the input data, the output hash will always be 128 bits long.

The strength of hashing is its one way-ness: It can be performed in only one direction. It isn't mathematically possible to convert a hash value back to its original data. Thus, if someone obtains your hash value, they won't be able to re-create the original data that produced the hash.

However, that isn't to say that hashing is totally attack proof. Hashing can be attacked using a method known as reverse engineering, reverse hash matching, or a birthday attack. These attack methods are commonly used by password-cracking tools. Most secure systems store passwords in their accounts database in hashed form. Hashes can't be performed in reverse, so this is generally a secure solution. However, since the hash algorithm used by commercial software is known (or can be easily discovered), password crackers can be written to exploit the stored password hashes. Attack tools compare hashes from potential passwords with the hashes stored in the accounts database. Potential passwords are either generated on the fly using all possible combinations of characters or pulled from a precompiled list of passwords (known as dictionary

lists). Each potential password is hashed, and then that hash value is compared with the accounts database. If a match is found, the password cracker tool has discovered a password for a user account.

This form of hashing attack exploits the mathematical characteristic that if two messages are hashed and their hashes are the same, the messages must be the same. This can be written $H(M)=H(M')$ then $M=M'$.

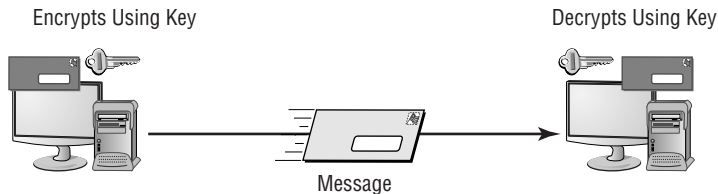
The most common or widely used hashing algorithms are as follows:

- *Secure Hash Algorithm (SHA-1)*—160-bit hash value
- *Message Digest 5 (MD5)*—128-bit hash value
- *Message Digest 4 (MD4)*—128-bit hash value
- *Message Digest 2 (MD2)*—128-bit hash value

Symmetric

Symmetric cryptography is also called private key cryptography or secret key cryptography. It uses a single shared encryption key to encrypt and decrypt data (see Figure 4.2). When symmetric cryptography is used to encrypt files on a hard drive, the user is the only person in possession of the single secret key. When symmetric cryptography is used to encrypt communications traffic, the two communication partners each have a copy of the one shared secret key. For example, the secure communication session protocol of Secure Socket Layer (SSL) uses symmetric cryptography. In either use, symmetric cryptography protects confidentiality.

FIGURE 4.2 A symmetric encryption system



Symmetric cryptography is very fast in comparison to asymmetric cryptography (discussed next). Its speed is due to the way its algorithms are designed and the fact that a single key is used to encrypt and decrypt data.

Symmetric cryptography provides for strong encryption protection when larger keys are used. However, the protection is secure only as long as the keys are kept private. If a symmetric key is compromised or stolen, it no longer offers true protection (just as your door lock no longer provides security if someone gets a copy of your house key).

Key exchange or distribution under symmetric cryptography is a common problem. To use symmetric cryptography to encrypt communications traffic between you and someone else over the Internet (or some other untrusted network), you must have a means to securely exchange the secret keys. If you already have a means to exchange the secret keys securely, why aren't you using that mechanism to communicate? Thus, some out-of-band communication solution must

be implemented to securely exchange keys. Mechanisms include shipping a floppy with a key, reading it over the phone, or using a different network to transmit the key. However, the preferred method is to deploy a complete Public Key Infrastructure (PKI) solution that employs asymmetric cryptography to exchange symmetric cryptographic keys. The exchanged secret keys are used to encrypt the traffic for a single communication session; then they're discarded. PKI is simply a concept of how to deploy different aspects of various cryptography mechanisms into a single complete real-world solution.

Since each member of a network in a symmetric cryptography solution needs to have a shared secret key with every other member in order to support secure communications, $n(n-1)/2$ keys are needed. Thus, symmetric cryptography isn't scalable when used alone.

Symmetric cryptography is divided into two forms:

Block cipher A block cipher is a solution that works against a complete static data set. That data set is broken into fixed-length segments called blocks, and each block is encrypted separately.

Stream cipher A stream cipher is a solution that works against data that is constantly being produced on the fly. A buffer, much like a block, waits to be filled by data as it's produced. Once the buffer block is full, that block is encrypted and then transmitted to the receiver.

Other than the basic difference in whether the original data is preexisting and static or produced on the fly, both ciphers function in much the same manner. Unless the symmetric cryptography solution is based around a one-time pad (meaning every key is used only once), the same encryption key is used on each block or buffer block for a given data set or communication session.

The most widely used symmetric cryptography solutions are listed in Table 4.1.

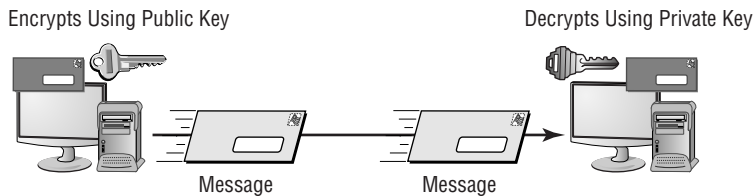
TABLE 4.1 Common Symmetric Cryptography Solutions

Name	Block Size	Key Size (in bits)
Advanced Encryption Standard (AES; uses the Rijndael block cipher algorithm)	Variable	128, 192, and 256
Triple Data Encryption Standard (3DES)	64	168
Data Encryption Standard (DES)	64	56
International Data Encryption Algorithm (IDEA)	64	128
Blowfish	Variable	1–448
Twofish	128	1–256
Rivest Cipher 5 (RC5)	32, 64, 128	0–2048
Carlisle Adams/Stafford Tavares (CAST-128)	64	128

Asymmetric

Asymmetric cryptography is also called public key cryptography. It uses key pairs consisting of a public key and a private key (see Figure 4.3). Each communication partner in an asymmetric cryptography solution needs their own unique key pair set (i.e. a private key and a public key); this makes asymmetric cryptography much more scalable than symmetric. The private key of the key pair must be kept private and secure. The public key of the key pair is distributed freely and openly.

FIGURE 4.3 An asymmetric encryption system



The public and private keys are related mathematically, but possession of the public key doesn't allow someone to generate the private key. Thus, the integrity of the private key is protected. In addition, the keys always work in unison: If the public key is used to encrypt data, only the private key can decrypt it. Likewise, if the private key is used to encrypt data, only the public key can decrypt it.

Asymmetric cryptography functions as follows:

1. The sender writes a message.
2. The sender encrypts the message with the sender's private key to produce the interim message package.
3. The sender encrypts the interim message package with the recipient's public key to produce the message package.
4. The sender transmits the message package to the recipient.
5. The recipient decrypts the message package using the sender's public key to produce the interim message package.
6. The recipient decrypts the interim message package using recipient's private key to extract the original message.

Asymmetric cryptography is much slower than symmetric cryptography, so it isn't generally suited for encrypting large amount of data. It's often used as the secure exchange mechanism for symmetric cryptographic keys. It provides several security services: authentication, integrity protection, and nonrepudiation.

The most widely used asymmetric cryptography solutions are as follows:

- Rivest Shamir Adleman (RSA)
- Diffie-Hellman
- Error Correcting Code (ECC)
- El Gamal

Exam Essentials

Hashing Hashing is used to produce a unique data identifier. Hashing takes a variable-length input and produces a fixed-length output. It can be performed in only one direction. The hash value is used to detect violations of data integrity.

Hashing attacks Hashing can be attacked using a method known as reverse engineering, reverse hash matching, or a birthday attack. These attack methods are commonly used by password-cracking tools.

Common hash algorithms The common hash algorithms are Secure Hash Algorithm (SHA-1), which is a 160-bit hash value; Message Digest 5 (MD5), which is a 128-bit hash value; Message Digest 4 (MD4), which is a 128-bit hash value; and Message Digest 2 (MD2), which is a 128-bit hash value.

Symmetric cryptography Symmetric cryptography is also called private key cryptography or secret key cryptography. Symmetric cryptography uses a single shared encryption key to encrypt and decrypt data. It provides the security service of confidentiality protection.

Strengths and weaknesses of symmetric cryptography Symmetric cryptography is very fast in comparison to asymmetric cryptography. It provides for strong encryption protection when larger keys are used. However, the protection is secure only as long as the keys are kept private. Key exchange under symmetric cryptography is a common problem. Symmetric cryptography isn't scalable when used alone.

Block ciphers A block cipher is a solution that works against a complete static data set. That data set is broken into fixed-length segments called blocks, and each block is encrypted separately.

Stream ciphers A stream cipher is a solution that works against data that is constantly being produced on the fly. A buffer, much like a block, waits to be filled by data as it's produced. Once the buffer block is full, that block is encrypted and then transmitted to the receiver.

Common symmetric cryptography solutions The common symmetric solutions are Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Blowfish, Twofish, Rivest Cipher 5 (RC5), and Carlisle Adams/Stafford Tavares (CAST-128).

Asymmetric cryptography Asymmetric cryptography is also called public key cryptography. It uses key pairs consisting of a public key and a private key. Each communication partner in an asymmetric cryptography solution needs only a key pair.

Strengths and weaknesses of asymmetric cryptography Asymmetric cryptography is scalable. The private key of the key pair must be kept private and secure. The public key of the key pair is distributed freely and openly. Possession of the public key doesn't allow someone to generate the private key. Asymmetric cryptography is much slower than symmetric cryptography. It provides three security services: authentication, integrity protection, and nonrepudiation.

Common asymmetric cryptography solutions The common asymmetric solutions are Rivest Shamir Adleman (RSA), Diffie-Hellman, Error Correcting Code (ECC), and El Gamal.

4.2 Cryptography Security Concepts

The full name of this section from the Security+ objectives list is “Understand how cryptography addresses the following security concepts.” Cryptography may provide one or more of the following security services: confidentiality, integrity, authentication, nonrepudiation, and access control. We’ll discuss each of these in the following sections.



For more information on how cryptography addresses the various security concepts, see Chapter 7 of *Security+ Study Guide, Second Edition*, by Sybex.

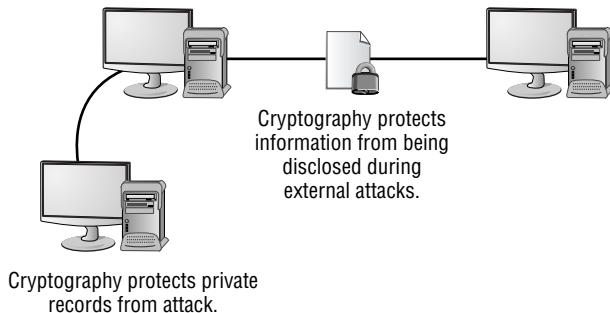
Critical Information

There are several security services that a cryptographic solution may provide. Familiarity with these services will assist you on the exam.

Confidentiality

Confidentiality protects the secrecy of data, information, or resources. It prevents or minimizes unauthorized access to data (see Figure 4.4). It ensures that no one other than the intended recipient of a message receives it or is able to read it. Confidentiality protection provides a means for authorized users to access and interact with resources, but it actively prevents unauthorized users from doing so.

FIGURE 4.4 Cryptographic systems protect data from internal and external disclosure.

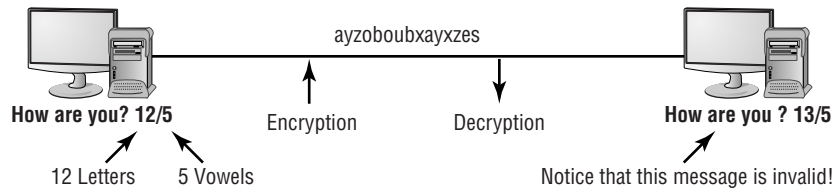


Integrity

Integrity is the security service that protects the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data (see Figure 4.5). It ensures that data remains correct, unaltered, and preserved. Integrity protection provides a means for authorized changes to be implemented, but it actively prevents unauthorized changes to protected data. Integrity

protection resists changes by unauthorized activities (such as viruses or intrusions) and accidents by authorized users (such as mistakes or oversights). Often an integrity check uses a hashing function to verify that data remains unchanged in storage or after transit.

FIGURE 4.5 A simple integrity-checking process for an encrypted message



One common example of a cryptographic solution that provides for integrity protection is a digital signature.

Digital Signatures

A digital signature is an electronic mechanism to prove that a message was sent from a specific user (that is, it provides for nonrepudiation) and that the message wasn't changed while in transit (it also provides integrity). Digital signatures operate using a hashing algorithm and either a symmetric or an asymmetric encryption solution.

Digital signatures using asymmetric encryption solutions operate as follows:

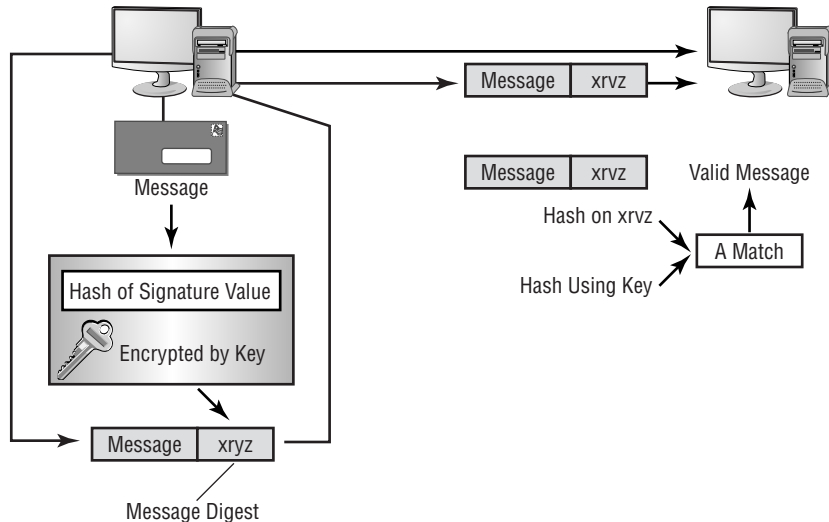
1. The sender writes a message.
2. The sender computes a hash of the message.
3. The sender uses the sender's private key to encrypt the hash.
4. The sender attaches the encrypted hash to the message.
5. The complete message package is sent to the receiver.
6. The receiver strips off the encrypted hash.
7. The receiver uses the sender's public key to decrypt the hash.
8. The receiver computes a hash of the message.
9. The receiver compares the two hash values.

Digital signatures using symmetric encryption solutions (see Figure 4.6) operate as follows:

1. The sender writes a message.
2. The sender computes a hash of the message.
3. The sender uses the shared secret key to encrypt the hash.
4. The sender attaches the encrypted hash to the message.
5. The complete message package is sent to the receiver.
6. The receiver strips off the encrypted hash.
7. The receiver uses the shared secret key to decrypt the hash.

8. The receiver computes a hash of the message.
9. The receiver compares the two hash values.

FIGURE 4.6 A digital signature process using symmetric encryption



In either case, if the hash values match, then the recipient gets verification that integrity was maintained and that the sender did send the message (nonrepudiation). If the hash values don't match, then the recipient doesn't have verification of either integrity protection or non-repudiation.

Authentication

Authentication verifies the identity of the sender or recipient of a message. In cryptography terms, authentication occurs differently in symmetric cryptography than it does in asymmetric cryptography. In symmetric cryptography, a single shared secret key is held only by the two communication partners. Thus, when an encrypted message is received and is properly decrypted by the recipient's copy of the shared secret key, authentication occurs. The recipient is authenticated because possession of the correct key proves that this is the correct recipient of the encrypted message. Likewise, the sender is authenticated because the recipient's ability to extract an intelligible message from the received encrypted material using the secret key proves that the sender, the only other user with possession of the same secret key, encrypted and sent the message.

In asymmetric cryptography, a sender uses the recipient's public key to encrypt data. This forces authentication of the recipient since the recipient is the only user in possession of the corresponding private key. Likewise, when the sender's private key is used to encrypt data, then any recipient can verify the sender's identity by decrypting that data with the sender's public key.

Nonrepudiation

Nonrepudiation prevents the sender of a message or the perpetrator of an activity from being able to deny that they sent the message or performed the activity. In symmetric cryptography, nonrepudiation is supported when a recipient is able to decrypt a message using the shared secret key. This proves that the other holder of the shared secret key is the actual sender who sent the message. In asymmetric cryptography, nonrepudiation is supported when a sender's private key is used to successfully decrypt a message. This proves that the sender's private key was used to encrypt the data. Since the sender is the only user who has possession of the sender's private key, no one else could have encrypted and sent the message.

One common example of a cryptographic solution that provides for nonrepudiation is a digital signature.

Digital Signatures



Digital signatures are discussed earlier in this section under the "Integrity" heading.

Access Control

Access control restricts access to secured data to authorized users. Cryptographic access control is enforced through the concept of possession of encryption keys. In a symmetric cryptography solution, a maximum of two people have valid possession of the shared secret key. Thus possession of the shared secret key is proof of authorization: The holder of the shared secret key is authorized to access anything encrypted with that key. In asymmetric cryptography, only one person is in valid possession of the private key. Thus, possession of the private key is proof of authorization: The holder of the private key is authorized to access anything encrypted with the corresponding public key.

Exam Essentials

Confidentiality Confidentiality prevents or minimizes unauthorized access to data. It ensures that no one other than the intended recipient of a message receives it or is able to read it.

Integrity Integrity protection prevents unauthorized alterations of data. It ensures that data remains correct, unaltered, and preserved. Integrity protection provides a means for authorized changes to be implemented, but it actively prevents unauthorized changes to protected data.

Digital signatures A digital signature is an electronic mechanism to prove that a message was sent from a specific user and that the message wasn't changed while in transit. Digital signatures operate using a hashing algorithm and either a symmetric or an asymmetric encryption solution.

Authentication The security service that verifies the identity of the sender or receiver of a message is authentication.

Nonrepudiation Nonrepudiation prevents the sender of a message or the perpetrator of an activity from being able to deny that they sent the message or performed the activity.

Access control Access control restricts access to secured data to authorized users. Cryptographic access control is enforced through the possession of encryption keys.

4.3 Public Key Infrastructure

The full name of this section from the Security+ objectives list is “Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).” Public Key Infrastructure (PKI) isn’t a product; rather, it’s a blueprint or concept for a solution. It dictates what should happen and which standards to comply with, but it doesn’t indicate which technologies or algorithms to use.



For more information on PKI, see Chapter 7 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

PKI focuses on proving the identity of communication partners, providing a means to securely exchange session-based symmetric encryption keys through asymmetric cryptographic solutions, and providing a means to protect message integrity through the use of hashing. Most PKI solutions are based around certificates and the use of a certificate authority (CA). The issue of certificates includes concepts of revocation and trust models.

Certificates

Certificates serve a single purpose: proving the identity of a user or the source of an object. They don’t provide proof as to the reliability or quality of the object or service to which they’re attached; they only provide proof of where that product or service originated.

Certificates work under a theory known as the trusted third party. This theory states that if user A trusts user C and user B trusts user C, then user A can trust B and vice versa. With certificates, the trusted third party is a certificate authority (CA) (see Figure 4.7). If two users have certificates issued by the CA, then the two users can trust each other’s identity. Certificates work this way on the Internet and within private organizations.

Most certificates used on the Internet and within private networks are based on the X.509 version 3 certificate standard. This standard dictates how certificates are to be constructed and their required components, such as the subject’s public key, the CA’s distinguishing name, a unique serial number, and the type of symmetric algorithm used for the certificate’s encryption (see Figure 4.8).

FIGURE 4.7 The certificate authority process

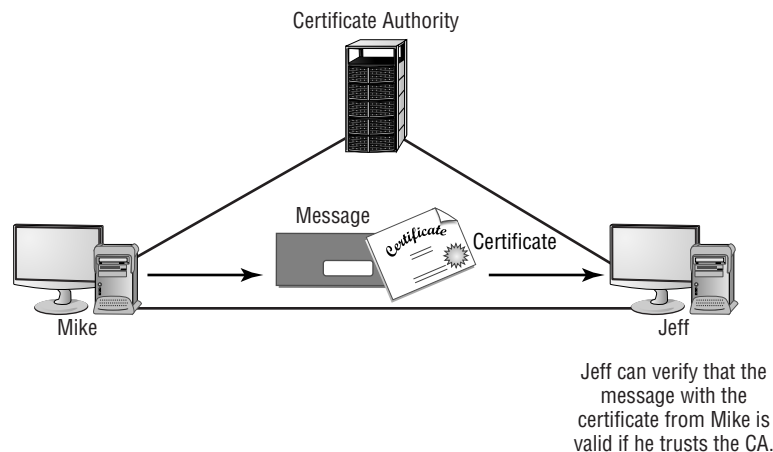


FIGURE 4.8 A certificate illustrating some of the information it stores

Version	V3
Serial Number	1234 D123 4567 ...
Signature Algorithm	Md2RSA
CA's name	Sample Certificate
Valid from:	Sunday, September 8, 2005
Valid to:	Sunday, September 15, 2005
Subject	Mr. Your Name Here, Myco
Public Key	Encrypted Value of Key
Extensions	Subject Type = End Entity
Signature Algorithm Signature	sha1 Encrypted Data

↑ ↑
Fields of a Simple X.509 Certificate

← Digital Signature Area

A user or a subject uses the following procedure to obtain a certificate:

1. The subject requests a certificate from a CA.
2. The request process includes proof of the subject's identity and the subject's public key.
3. The CA verifies the identity of the subject.
4. The CA creates the certificate.

5. The CA validates the certificate by signing it with the CA's private key.
6. The CA issues the certificate to the subject.

Another entity known as a registration authority (RA) may be deployed in a CA solution. The RA can't create new certificates; rather it serves as a distribution point for the certificate revocation list (CRL) and possibly as an Online Certificate Status Protocol (OCSP) host (see the later section "Revocation"). CAs must have defined certificate policies and certificate practice statements.

Certificate Policies

A certificate policy is a PKI document that serves as the basis for common interoperability standards and common assurance criteria. Certificate policies are acceptable use policies for certificates: They dictate what is and isn't acceptable with regard to how certificates can be used in an organization. The policies are a set of rules that control how certificates are used, managed, and deployed.

Certificate policies must

- be clear and concise.
- be endorsed by senior management.
- be restricted to a maximum length of two pages.
- be written in bullet-point statements.
- be able to provide users (also referred to as subjects) with a clear understanding of the acceptable use policies with regard to certificates.

Certificate Practice Statements

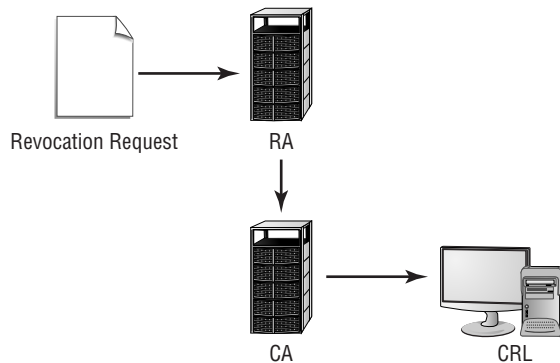
A certificate practice statement (CPS) describes how a CA will manage the certificates it issues. The CPS details how certificate management is performed, how security is maintained, and the procedures the CA must follow to perform any type of certificate management from creation to revocation.

Revocation

Certificates have a specific expiration date, which is sometimes called the lifetime date. Once that date is reached, a certificate is automatically rejected as invalid. However, a CA may have cause to revoke or invalidate a certificate before its predefined expiration date. Revocation is the process by which a CA invalidates a certificate.

Revocation may occur because the subject's identity information has changed, the subject used the certificate to commit a crime, or the subject used the certificate in such a way as to violate the CA's certificate policy.

When a certificate is revoked, it's added to the CA's CRL. Once a certificate's expiration date is reached, it's removed from the CRL, since the timestamp automatically invalidates the certificate. Thus, the CRL contains only those certificates that have been revoked but have yet to expire. Figure 4.9 shows the certification revocation process.

FIGURE 4.9 Certification revocation process

The CRL is freely distributed to all users and applications. You should always consult it before accepting a certificate. When issued to a requesting user or application, a CRL is assigned a lifetime date as well. When the CRL exceeds this lifetime, it can no longer be relied on, and you should obtain a new, updated version of the CRL.

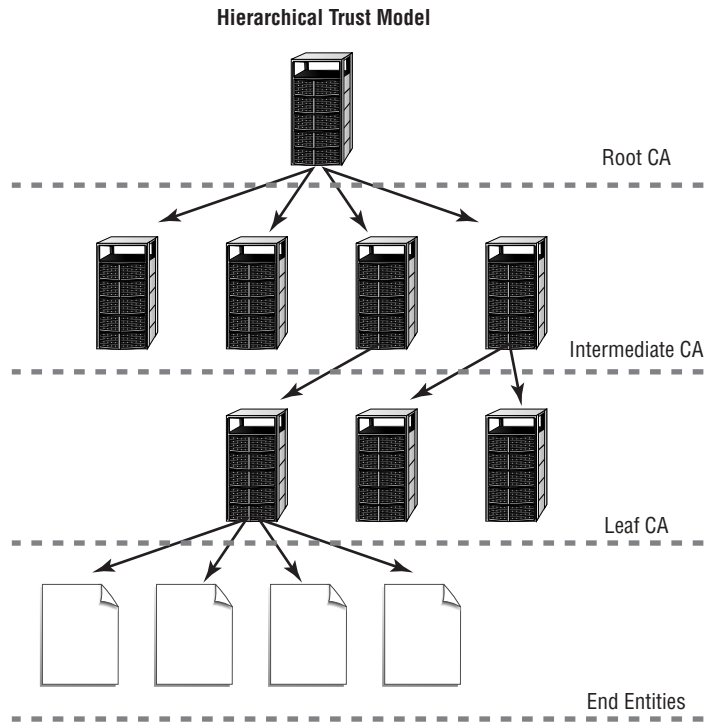
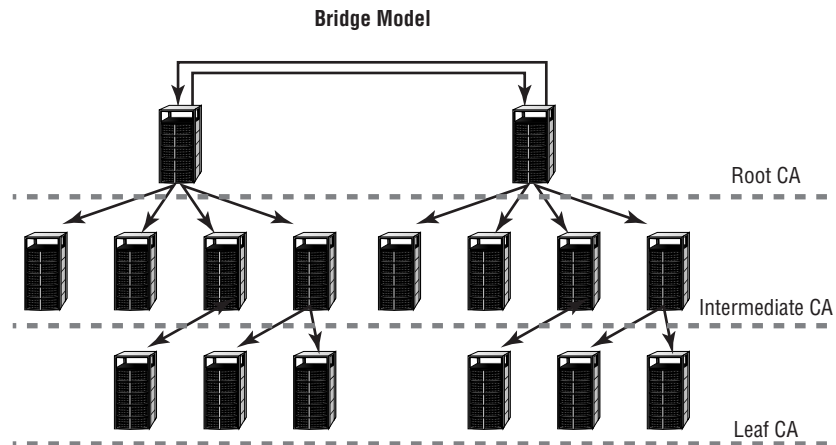
When a user application, such as a web browser, receives a certificate from a server, such as a web server, the application first verifies that the date on the certificate is still valid. Next, it checks the local copy of the CA's CRL. If the CRL is no longer valid, an updated copy of the CRL is obtained. The application checks to see whether the certificate appears on the CRL. If it doesn't, the application presents the certificate to the user for a final acceptance choice. The user can elect to accept or reject the certificate as well as indicate whether to make this same acceptance or rejection choice for all future instances of this certificate.

The CRL process is widely used, but it isn't the only mechanism for informing users and applications about the status of certificates. Online Certificate Status Protocol (OCSP) is another solution that functions on a direct query basis. Each time an application receives a new certificate, it sends a query to an OCSP CA server. The CA responds directly to indicate whether the certificate is still valid or has been revoked. By using OCSP, large CRLs aren't transmitted repeatedly to every requesting system, and queries are direct, immediate, and current.

Trust Models

The term *trust model* refers to the structure of the trust hierarchy used by a certificate authority system. The basic trust model scheme used by CAs is a hierarchical structure with a single top-level root CA. Below the root CA are one, two, or more subordinate CAs. Below each subordinate CA may be one, two, or more subordinate CAs, and so on. Subordinate CA's can sometimes be called intermediate or leaf CAs. In this model, all CAs have a single parent CA, but they may have multiple child CAs (see Figure 4.10). The root CA is the start of trust; all CAs and participants in a hierarchical trust model ultimately rely on the trustworthiness of the root CA.

Cross-certification occurs when a CA from one organization elects to trust a CA from another organization (see Figure 4.11). This is also called a bridge trust structure. In this way, certificates from either organization are accepted by the other organization. In most cases, the root CA is configured to trust the other root CA.

FIGURE 4.10 A hierarchical trust structure**FIGURE 4.11** A cross or bridge trust structure

A trust list is a form of trust model where a web browser or similar application is provided a list of root certificates of trusted CAs. The web browser trusts numerous sources of certificates because of the presence of the trusted CA's root certificate on the list of trusted CAs.

Exam Essentials

PKI PKI focuses on proving the identity of communication partners, providing a means to securely exchange session-based symmetric encryption keys through asymmetric cryptographic solutions, and providing a means to protect message integrity through the use of hashing.

Certificates Certificates serve a single purpose: proving the identity of a user or the source of an object. Certificates don't provide any proof as to the reliability or quality of the object or service to which they're attached; they only provide proof of where that product or service originated.

Trusted third parties Certificates work under a theory known as the trusted third party: If user A trusts user C and user B trusts user C, then user A can trust B and vice versa. With certificates, the trusted third party is a certificate authority (CA).

x.509 version 3 certificate standard Most certificates are based on the X.509 version 3 certificate standard. Some of the required components are the subject's public key, the CA's distinguishing name, a unique serial number, and the type of symmetric algorithm used for the certificate's encryption.

Procedure for requesting a certificate To request a certificate, a subject submits a request to a CA with proof of their identity and their public key.

Certificate policies A certificate policy is a PKI document that serves as the basis for common interoperability standards and common assurance criteria. It's a statement that governs the use of digital certificates within an organization. Certificate policies are acceptable use policies for certificates.

Certificate practice statements (CPS) A CPS describes how a CA will manage the certificates it issues. It details how certificate management is performed, how security is maintained, and the procedures the CA must follow to perform any type of certificate management from creation to revocation.

Revocation A CA may have cause to revoke or invalidate a certificate before its predefined expiration date. Revocation may occur because the subject's identity information has changed, the subject used the certificate to commit a crime, or the subject used the certificate in such a way as to violate the CA's certificate policy.

Certificate revocation lists (CRL) When a certificate is revoked, it's added to the CA's CRL. The CRL is freely distributed to all users and applications. It should always be consulted before accepting a certificate.

How a web browser handles new certificates When a web browser receives a certificate from a web server, it verifies that the date on the certificate is still valid. Next, it checks the local copy

of the CA's CRL. If the CRL is no longer valid, an updated copy of the CRL is obtained. The application checks to see if the certificate appears on the CRL. If it doesn't, the application presents the certificate to the user for a final acceptance choice.

Online Certificate Status Protocol (OCSP) OCSP is a revocation solution that functions on a direct query basis. Each time an application receives a new certificate, it sends a query to an OCSP CA server. The CA responds directly to indicate whether the certificate is still valid or has been revoked.

Trust models The term *trust model* refers to the structure of the trust hierarchy used by a certificate authority system. The basic trust model scheme used by CAs is a hierarchical structure.

Hierarchical trust models A hierarchical structure has a single top-level root CA. Below the root CA are one, two, or more subordinate CAs. The root CA is the start of trust. All CAs and participants in a hierarchical trust model ultimately rely on the trustworthiness of the root CA.

Cross certification Cross certification occurs when a CA from one organization elects to trust a CA from another organization. In this way, certificates from either organization are accepted by the other organization. In most cases, the root CA is configured to trust the other root CA.

Trust lists A trust list is a form of trust model where a web browser or similar application is provided with a list of root certificates of trusted CAs. The web browser trusts numerous sources of certificates because of the presence of the trusted CA's root certificate on the list of trusted CAs.

4.4 Cryptographic Standards and Protocols

The full name of this section from the Security+ objectives list is "Identify and be able to differentiate different cryptographic standards and protocols." The Security+ exam assumes you'll be able to differentiate between symmetric and asymmetric cryptography systems as well as hashing algorithms. You should be able to recognize specific examples of all three forms of cryptography.



This section is purposefully brief because all of the issues and concepts that should appear here are already discussed in other objective areas where they are specifically named.



For more information on identifying and differentiating cryptography standards and protocols, see Chapter 8 of the *Security+ Study Guide, Second Edition*, by Sybex.

4.5 Key Management and Certificate Life Cycles

The full name of this section from the Security+ objectives list is “Understand and be able to explain the following concepts of key management and certificate life cycles.” This section addresses the various aspects of controlling and handling cryptographic keys and digital certificates.



For more information on key management and certification lifecycles, see Chapter 8 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Key management is the term used to describe the various mechanisms, techniques, and processes used to protect, use, distribute, store, and control cryptographic keys. A key management solution should follow these basic rules:

- The key should be long enough to provide the necessary level of protection.
- Keys should be stored and transmitted securely.
- Keys should be truly random, should use the full spectrum of the keyspace (the range of valid values that can be used as a key for a specific algorithm), and should never repeat.
- The lifetime of a key should correspond to the sensitivity of the data it's protecting.
- The more a key is used, the shorter its lifetime should be.
- Keys should be backed up or escrowed in case of emergency.
- Keys should be properly destroyed at the end of their lifetime.

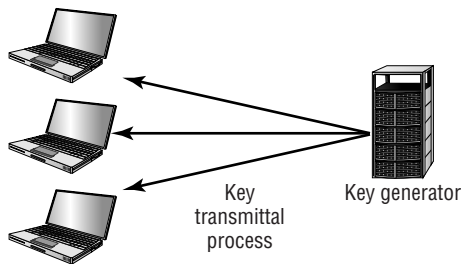
In addition to these basic concepts, the remainder of this section discusses other important issues in regard to key management.

Centralized vs. Decentralized

Centralized key management gives complete control of cryptographic keys to the organization and takes control away from the end users. A centralized key-management solution requires a significant investment in infrastructure, processing capabilities, administrative oversight, and communication bandwidth.

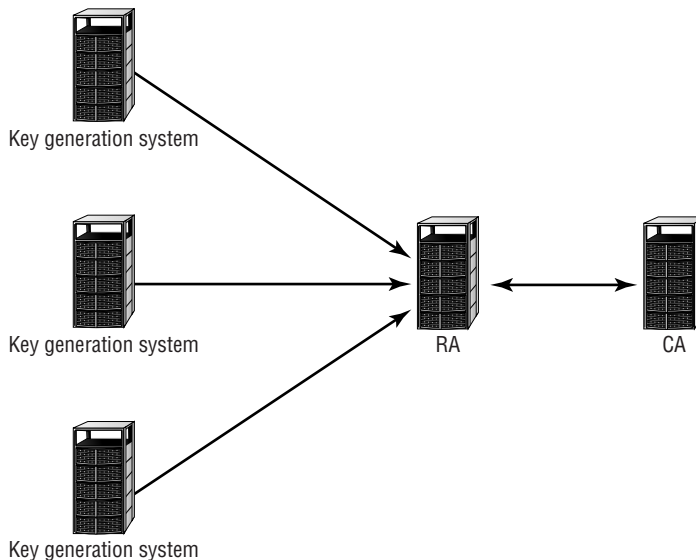
In a centralized management solution, copies of all cryptographic keys are stored in escrow. This allows administrators to recover keys in the event that a user loses their key, but it also allows management to access encrypted data whenever it chooses.

Other important aspects of centralized key management are that keys must be created only on secured, dedicated servers; keys can be distributed only to authorized users and only in a secure fashion; keys can be modified only by administrators; and revocation of keys and corresponding digital certificates is at the discretion of the organization. Figure 4.12 shows an example of a centralized key management solution.

FIGURE 4.12 A centralized key-generating facility

Centralized key management is often unacceptable to a user community since it provides them with no control over their privacy, confidentiality, or integrity. In fact, every key generated by the centralized system is stored in escrow. Therefore, nothing encrypted by an end user is completely private, since an administrator could extract the key from escrow and use it to decrypt a message or file.

An alternate scheme is known as decentralized key management. In this type of environment, end users generate their keys (whether symmetric or asymmetric) and submit keys only as needed to centralized authorities (see Figure 4.13). For example, to request a digital certificate, an end user would transmit only their public key to the CA. The end user's private key is always kept private so they're the only entity in possession of it. Plus, since the public key is already public, its compromise won't result in a complete compromise of the end user's secured solution.

FIGURE 4.13 A decentralized key-generating system

In a decentralized key management system, end users are ultimately responsible for managing their own keys and using escrow to provide fault tolerance. If an end user fails to take the necessary precautions, a lost or corrupted key could mean the loss of all data encrypted with that key.

Storage

Cryptographic keys and digital certificates should be stored securely. If a private key (asymmetric) or a secret key (symmetric) is ever compromised, then the security of all data encrypted with those keys is lost. Reliable storage mechanisms must be used to protect cryptographic keys. There are two methods or mechanisms for storing keys: hardware based or software based.

Hardware vs. Software

Keys can be stored in either software solutions or hardware solutions. Both offer unique benefits and shortcomings. A software solution offers flexible storage mechanisms and, often, customizable options. However, such a solution is vulnerable to electronic attacks (viruses or intrusions), may not properly control access (privilege-elevation attacks), and may be deleted or destroyed. Most software solutions rely on the security of the host operating system, which may not be sufficient.

Hardware solutions aren't as flexible. However, they're more reliable and more secure than software solutions. Hardware solutions may be expensive and are subject to physical theft. If a user isn't in physical possession of the hardware storage solution, they can't gain access to the secured or encrypted resources. Some common examples of hardware key storage solutions include smartcards and flash memory drives.

Private Key Protection

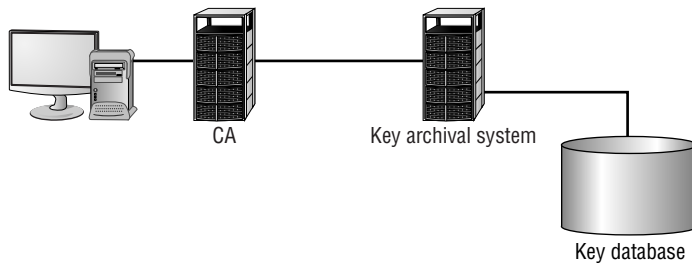
In a symmetric system, all entities in possession of the shared secret key must protect the privacy and secrecy of that key. If the key is compromised anywhere or by anyone, the entire solution (all entities using the same key) is compromised (everything protected by that key).

In an asymmetric system, each end user must protect their private key. If an end user's private key is ever compromised, then only that one end user's security is lost. All other users in the environment aren't directly affected by the key compromise.

Escrow

Key escrow is a storage process by which copies of private keys and/or secret keys are retained by a centralized management system (see Figure 4.14). This system securely stores the encryption keys as a means of insurance or recovery in the event of a disaster. In terms of cryptography, a *disaster* is when a key is lost or damaged. If such a key is stored in escrow, it can be recovered by a key escrow agent and used to recover any data encrypted with the damaged or lost key.

However, escrow can be seen in another light if you're an end user intent on obtaining complete and total security. If you're assigned your private key or secret key, then the issuing CA (or cryptographic server) probably retains a copy of the key in escrow. This means that at any time a key recovery agent could pull your key out of escrow and use it to decrypt anything you've encrypted with your public key or your secret key without your permission. Obviously, key escrow works great in private corporate environments, but it doesn't apply well to the public Internet.

FIGURE 4.14 A key archiving or escrow system

An important aspect of key escrow is key recovery. That topic is covered in a later, in the section “Recovery.”

Expiration

Most cryptographic keys and all certificates have a built-in expiration date. Upon reaching that date, the key or certificate becomes invalid, and no system will accept it. Keys and certificates are assigned a lifetime with control settings known as *valid from* and *valid to* dates. Keys and certificates past their valid to dates should be discarded or destroyed.

If the *valid to* date for a key or certificate is approaching, you should request a renewal. If you fail to renew before the lifetime expires, then you must perform the complete request process from scratch.

Revocation

Keys and certificates can be revoked before they reach their lifetime expiration date.



This topic was discussed in section “4.3 Revocation.”

Status Checking

Status checking is the process of checking the lifetime dates against the current system date, checking the CRL, and/or querying an OCSP server.



This topic is discussed in sections “4.3 Certificates” and “4.3 Revocation.”

Suspension

Suspension is an alternative to revocation. Suspension can be used when a key or certificate will be temporarily removed from active use but the subject (or the CA) doesn't wish to invalidate it. When a key or certificate is suspended, it can't be used to sign or encrypt any new items, but previously signed or encrypted items can be verified or decrypted. The key or certificate can be reactivated at a later date.

Status Checking

Suspension status checking is an extension of revocation status checking. However, the results indicate whether a certificate or key is currently valid or in suspension (such a status would be labeled *certification hold*).



Revocation status checking is discussed in sections “4.3 Certificates” and “4.3 Revocation.”

Recovery

Recovery is the process of pulling a key or certificate from escrow. Recovery can be used when a user loses their key or their key has been corrupted. This process can also be used to extract a key for the purpose of decrypting data even when the user still has valid possession of their key. The latter option may be necessary in a private corporate environment, but it's unacceptable in a public environment, such as the Internet.

Key recovery can only be performed by a key recovery agent. The key recovery agent is an administrative-level user who has the encryption key to the escrow database. They can decrypt and extract the necessary key from the escrow database and either give a copy to the user or use the key to decrypt all data. If the latter occurs (as is common in most cryptographic solution implementation), the end user must be issued a new key, which must be used in turn to re-encrypt all the data that should be secured.

M of N Control (Of M appropriate individuals, N must be present to authorize recovery)

A key recovery agent should be a trusted individual. If the environment doesn't warrant the trust of a single key recovery agent, a mechanism known as *M of N control* can be implemented. M of N control indicates that there are multiple key recovery agents (M) and that a specific minimum number of these key recovery agents (N) must be present and working in tandem in order to extract keys from the escrow database. The use of M of N control ensures accountability among the key recovery agents and prevents any one individual from having complete control over or access to a cryptographic solution.

Renewal

Renewal is the process by which a key or certificate is reissued with an extended lifetime date before the key or certificate expires. The renewal process doesn't require a complete repeat of

the request and identity proofing process; rather, the old key (which is about to expire) is used to sign the request for the new key. This allows the CA to quickly determine whether the end user's key or certificate can be immediately extended (or reissued with a new lifetime date) or rejected and revoked according to its existing lifetime dates. The decision of the CA often depends on the end user's compliance with the organization's certificate policy (the acceptable use policy for the key or certificate).

Destruction

After a key or certificate is no longer needed or it has expired or been revoked, it should be properly disposed of. This process is known as key destruction: the removal of the key or certificate from all software and hardware storage devices. For keys and certificates that are still valid, the CA should be informed about the destruction of the key or certificate. This action allows the CA to update its CRL and OCSP servers.

Reasons to use key destruction include going out of business, changing identity, or having obtained replacement keys or certificates.

Key Usage

Cryptographic keys and digital certificates can be used in a wide variety of applications. Cryptographic keys, both symmetric and asymmetric, are involved in numerous security and protection solutions. These include the following:

- Virtual private network (VPN) protocols such as IPsec
- Communication security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- The application of SSL to protect web traffic as in HTTP over SSL (HTTPS)
- Proprietary web communication security protocols such as Secure HTTP (SHTTP)
- Secure remote administration solutions, such as Secure Shell (SSH)
- E-mail security solutions, such as Pretty Good Privacy (PGP) and Secure MIME (S/MIME)

Multiple Key Pairs (Single, Dual)

In some situations, you may use multiple key pairs. One key set might be used for authentication and encryption and the other for digital signatures. This allows the first key pair to be escrowed and included on data backups of a centralized key-management scheme. The second key set is then protected from compromise, and the privacy of the owner's digital signature is protected, preventing misuse and forgery.

Exam Essentials

Key management basics Keys should be long enough to provide the necessary level of protection, should be stored and transmitted securely, should be random, and should use the full spectrum of the keyspace. In addition, they should be escrowed, properly destroyed at the end of their lifetime, used in correspondence with the sensitivity of the protected data, and have a shortened use lifespan if they're used repeatedly.

Centralized key management Centralized key management gives complete control of cryptographic keys to the organization and takes control away from the end users. In a centralized management solution, copies of all cryptographic keys are stored in escrow.

Decentralized key management In decentralized key management, end users generate their keys (whether symmetric or asymmetric) and submit keys only as needed to centralized authorities. The end user's private key is always kept private so they are the only entity in possession of it.

Key storage Cryptographic keys and digital certificates should be stored securely. If a private key (asymmetric) or a secret key (symmetric) is ever compromised, then the security of all data encrypted with the key is lost.

Software key storage A software solution offers flexible storage mechanisms and, often, customizable options. However, a software solution is vulnerable to electronic attacks (viruses or intrusions), may not properly control access (privilege-elevation attacks), and may be deleted or destroyed. Most software solutions rely on the security of the host OS, which may not be sufficient.

Hardware key storage Hardware solutions aren't as flexible. However, they're more reliable and more secure than software solutions. Hardware solutions may be expensive and are subject to physical theft. If a user isn't in physical possession of the hardware storage solution, they can't gain access to the secured or encrypted resources. Some common examples of hardware key storage solutions include smartcards and flash memory drives.

Private key protection In a symmetric system, all entities in possession of the shared secret key must protect the privacy and secrecy of that key. If the key is compromised anywhere or by anyone, the entire solution (all entities using the same key) is compromised (everything protected by that key).

Key escrow Key escrow is a storage process by which copies of private keys and/or secret keys are retained by a centralized management system. This system securely stores the encryption keys as a means of insurance or recovery in the event of a lost or corrupted key.

Key expiration Most cryptographic keys and all certificates have a built-in expiration date. Upon reaching that date, the key or certificate becomes invalid, and no system will accept it. Keys and certificates are assigned a lifetime with control settings known as *valid from* and *valid to* dates. Keys and certificates past their *valid to* dates should be discarded or destroyed.

Key revocation and status checking Keys and certificates can be revoked before they reach their lifetime expiration date. Status checking is the process of checking the lifetime dates against the current system date, checking the CRL, and/or querying an OCSP server.

Key suspension Suspension is an alternative to revocation. It can be used when a key or certificate will be temporarily removed from active use but the subject (or the CA) doesn't wish to outright invalidate the key or certificate. Suspension allows a key or certificate to be reactivated at a later date.

Key recovery Recovery is the process of pulling a key or certificate from escrow. The recovery process can be used when a user loses their key or their key has been corrupted. Only a key recovery agent can perform key recovery.

M of N control If the environment doesn't warrant the trust of a single key recovery agent, a mechanism known as M of N control can be implemented. M of N control indicates that there are multiple key recovery agents (M) and that a specific minimum number of these key recovery agents (N) must be present and working in tandem in order to extract keys from the escrow database.

Key renewal Renewal is the process by which a key or certificate is reissued with an extended lifetime date before it expires. The renewal process doesn't require a complete repeat of the request and identity proofing process; rather, the old key (which is about to expire) is used to sign the request for the new key.

Key destruction After a key or certificate is no longer needed or it has expired or been revoked, it should be properly disposed of. For keys and certificates that are still valid, the CA should be informed about the destruction of the key or certificate. This action allows the CA to update its CRL and OCSP servers.

Key usage Cryptographic keys and digital certificates can be used in a wide variety of applications. Cryptographic keys, both symmetric and asymmetric, are involved in numerous security and protection solutions. Uses include VPN, IPSec, SSL, TLS, HTTPS, SHTTP, SSH, PGP, and S/MIME.

Use of multiple key pairs In some situations, you may use multiple key pairs. One key set might be used for authentication and encryption and the other for digital signatures. This allows the first key pair to be escrowed and included on data backups of a centralized key management scheme. The second key set is then protected from compromise, and the privacy of the owner's digital signature is protected, preventing misuse and forgery.

Review Questions

1. Hashing is used to test, prove, or verify which security service?
 - A. Authentication
 - B. Confidentiality
 - C. Integrity
 - D. Nonrepudiation
2. Which of the following symmetric encryption algorithms offers the strength of 168-bit keys?
 - A. Data Encryption Standard
 - B. Triple DES
 - C. Advanced Encryption Standard
 - D. IDEA
3. Diffie-Hellman is what type of cryptographic system?
 - A. Asymmetric
 - B. Symmetric
 - C. Hashing
 - D. Certificate authority
4. The security service that protects the secrecy of data, information, or resources is known as what?
 - A. Integrity
 - B. Authentication
 - C. Nonrepudiation
 - D. Confidentiality
5. Digital signatures can be created using all but which of the following?
 - A. Asymmetric cryptography
 - B. Hashing
 - C. Key escrow
 - D. Symmetric cryptography
6. Certificates have what single purpose?
 - A. Proving identity
 - B. Proving quality
 - C. Providing encryption security
 - D. Exchanging encryption keys

7. When a subject or end user requests a certificate, they must provide which of the following items? (Choose all that apply.)
 - A. Proof of identity
 - B. Hardware storage device
 - C. Public key
 - D. Private key
8. From a private corporate perspective, which of the following is most secure?
 - A. Decentralized key management
 - B. Centralized key management
 - C. Individual key management
 - D. Distributed key management
9. The mechanism used by a key-management system to provide fault tolerance to private keys is called what?
 - A. Revocation
 - B. Enrollment
 - C. Suspension
 - D. Escrow
10. When should a key or certificate be renewed?
 - A. Every year
 - B. Every quarter
 - C. Just before it expires
 - D. Just after it expires

Answers to Review Questions

1. C. Hashing is used to test whether the integrity of data has been violated. Asymmetric cryptography provides authentication, integrity, and nonrepudiation. Symmetric cryptography provides confidentiality.
2. B. Triple DES offers the strength of 168-bit keys. DES offers the strength of 56-bit keys. AES offers the strength of 128, 192, or 256-bit keys. IDEA offers the strength of 128-bit keys.
3. A. Diffie-Hellman is an asymmetric cryptographic system. DES and AES are examples of symmetric cryptography. MD5 and SHA-1 are examples of hashing. Certificate authorities issue certificates based on an implemented PKI solution.
4. D. The security service that protects the secrecy of data, information, or resources is known as confidentiality. Integrity protects the reliability and correctness of data. Authentication verifies the identity of the sender or receiver of a message. Nonrepudiation prevents the sender of a message or the perpetrator of an activity from being able to deny that they sent the message or performed the activity.
5. C. Key escrow isn't used in digital signatures, but it's a fault-tolerance feature of certificate and key management. Asymmetric and symmetric cryptography along with hashing are used in digital signatures.
6. A. Certificates have the single purpose of proving identity. They don't prove quality or provide encryption security, and they aren't used to exchange encryption keys.
7. A, C. Proof of identity and the subject's public key must be provided to the CA when requesting a certificate. The private key should never be revealed to anyone, not even the CA. A hardware storage device is used after a key or certificate has been issued, not as part of the requesting process.
8. B. Centralized key management is more secure, or at least more desirable, from a private corporate perspective. From a public or individual perspective, decentralized key management is more secure. Individual and distributed key management are nonstandard terms that could be used to refer to decentralized key management.
9. D. Escrow is the mechanism used by a key-management system to provide fault tolerance to private keys. Revocation is the invalidation of keys or certificates before their lifetime dates have expired. Enrollment is when a user requests a new certificate. Suspension is when a key or certificate is temporarily removed from active.
10. C. Keys and certificates should be renewed just before they expire. All the other choices are incorrect.



Chapter

5

Operational/ Organizational Security

**THE FOLLOWING COMPTIA SECURITY+
EXAM OBJECTIVES ARE COVERED IN
THIS CHAPTER:**

- ✓ **5.1 Understand the application of the following concepts of physical security**
 - Access Control
 - Physical Barriers
 - Biometrics
 - Social Engineering
 - Environment
 - Wireless Cells
 - Location
 - Shielding
 - Fire Suppression
- ✓ **5.2 Understand the security implications of the following topics of disaster recovery**
 - Backups
 - Off Site Storage
 - Secure Recovery
 - Alternate Sites
 - Disaster Recovery Plan
- ✓ **5.3 Understand the security implications of the following topics of business continuity**
 - Utilities
 - High Availability/Fault Tolerance
 - Backups

✓ **5.4 Understand the concepts and uses of the following types of policies and procedures**

- Security Policy
 - Acceptable Use
 - Due Care
 - Privacy
 - Separation of Duties
 - Need to Know
 - Password Management
 - SLAs (Service Level Agreements)
 - Disposal/Destruction
 - HR (Human Resources) Policy
 - Termination (Adding and Revoking Passwords and Privileges, etc.)
 - Hiring (Adding and Revoking Passwords and Privileges, etc.)
 - Code of Ethics
- Incident Response Policy

✓ **5.5 Explain the following concepts of privilege management**

- User/Group/Role Management
- Single Sign-On
- Centralized vs. Decentralized
- Auditing (Privilege, Usage, Escalation)
- MAC/DAC/RBAC (Mandatory Access Control/Discretionary Access Control/Role-Based Access Control)

✓ **5.6 Understand the concepts of the following topics of forensics**

- Chain of Custody
- Preservation of Evidence
- Collection of Evidence

✓ **5.7 Understand and be able to explain the following concepts of risk identification**

- Asset Identification
- Risk Assessment
- Threat Identification
- Vulnerabilities

✓ **5.8 Understand the security relevance of the education and training of end users, executives, and human resources**

- Communication
- User Awareness
- Education
- On-line Resources

✓ **5.9 Understand and explain the following documentation concepts**

- Standards and Guidelines
- Systems Architecture
- Change Documentation
- Logs and Inventories
- Classification
 - Notification
- Retention/Storage
- Destruction



The Security+ exam will test your understanding of operational and organizational security issues. This domain includes a wide range of subjects including physical security, business continuity, security policy, risk management, forensics, security training, and security documentation. To pass the test and be effective in implementing security, you need to understand the basic concepts and terminology in this chapter.

5.1 Physical Security

The full name of this section from the Security+ objectives list is “Understand the application of the following concepts of physical security.” Physical security is an area that is often overlooked when designing security for an environment. However, without physical security, there is no security. As you prepare for the Security+ exam, don’t overlook the aspects and elements of physical security.



For more information on physical security, see Chapter 6 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

As a security professional, you need to reduce the overall opportunities for intrusions or physical security violations to occur. This can be accomplished using various mechanisms, including prevention, deterrence, and detection. In the following sections, the topics of managing security from the perspectives of access control, social engineering, and environment are discussed.

Access Control

In the realm of physical security, *access controls* are mechanisms designed to manage and control entrance into a location such as a building, a parking lot, a room, or even a specific box or server rack. Being able to control who can gain physical proximity to your environment (especially your computers and networking equipment) lets you provide true security for your data, assets, and other resources. Without physical access control, you have no security.

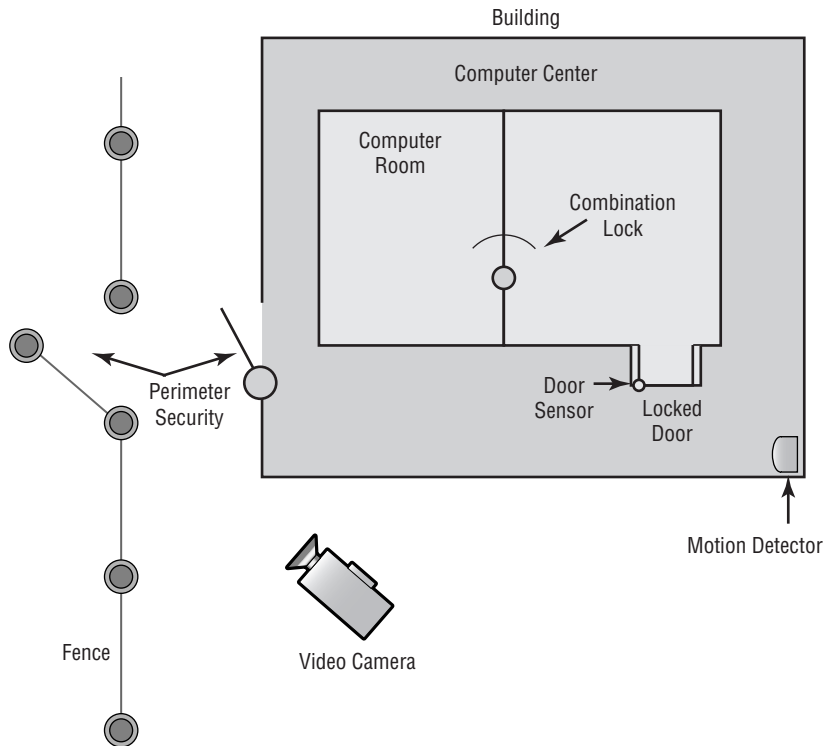
To ensure proper physical security, you should design the layout of your physical environment with security in mind. This means all equipment is placed in locations that can be secured, and access or entrance into those locations is controlled and monitored. Good physical security

access control also recognizes that some computers and network devices are more important or mission critical than others and therefore require greater physical security protection.

Mission-critical servers and devices should be placed in dedicated equipment rooms that are secured from all possible entrance and intrusion (see Figure 5.1). These rooms shouldn't have windows and should have floor-to-roof walls (rather than short walls that end at a drop ceiling). Equipment rooms should be locked at all times, and only authorized personal should ever be granted entrance. The rooms should be monitored, and all access should be logged and audited.

An important aspect of access control for a facility is the use of physical barriers.

FIGURE 5.1 An example of a multilayered physical security environment



Physical Barriers

Physical barriers are erected to control access to a location. Some of the most basic forms of physical barriers are walls and fences. Fences are used to designate the borders of a geographic area where entrance is restricted; a high fence, the presence of barbed wire, or electrified fencing all provide greater boundary protection. Walls provide protection as well, preventing entry except at designated points such as doors and windows. The stronger the wall, the more security it provides. And the greater the number of walls between the untrusted outside and the valuable assets located inside, the greater the level of physical security.

Although you need walls and fences to protect boundaries, there must be a means for authorized personnel to cross these barriers into the secured environment. Doors and gates can be locked and controlled in such a way that only authorized people can unlock and/or enter through them. Such control can take the form of a lock with a key that only authorized people possess. A security guard may check each person's credentials before granting entry. You can also use a biometrically controlled door (discussed in the following section).

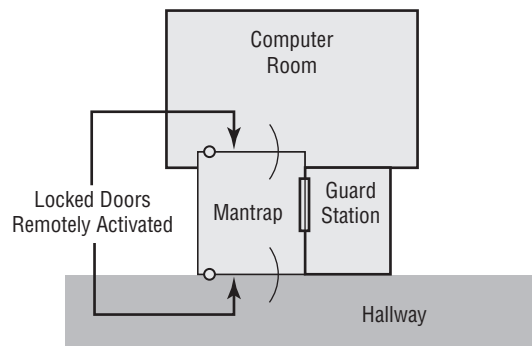
The presence of security guards at an entrance or around the perimeter of a security boundary serves as a deterrent to intruders and provides a form of physical barrier. Guard dogs can also protect against intrusion by detecting the presence of unauthorized visitors.

A mantrap is a form of high-security barrier entrance device (see Figure 5.2). It's a small room with two doors: one in the trusted environment and one opening to the outside. The mantrap works like this:

1. A person enters the mantrap.
2. Both doors are locked.
3. The person must properly authenticate to unlock the inner door again entry. If the authentication fails, security personnel are notified and the intruder is detained inside the mantrap.

Mantraps often contain scales and cameras in order to prevent *piggybacking*. Piggybacking occurs when one person authenticates, opens a door, and lets another person enter without that second person authenticating to the system.

FIGURE 5.2 A mantrap



Biometrics

Doors used to control entrance into secured areas can be protected by locks that are keyed to biometrics. A biometric lock requires that the person present a biometric factor, such as a fingerprint, hand scan, retinal scan, and so on, to the validation mechanism. Only after the biometric is verified is the door unlocked and the person allowed entry. When biometrics are used to control entrance into secured areas, they serve as a mechanism of identity proofing as well as authentication.



For additional discussion of biometrics, please see section “1.2 Identifying Authentication Methods” in Chapter 1, “General Security Concepts.”

Social Engineering

Social engineering is a form of attack that exploits human nature. Social engineering attacks take two primary forms: convincing someone to either perform an unauthorized operation or reveal confidential information. For example, the victim may be fooled into believing that a received e-mail is authoritative (such as an e-mail hoax), a person on the phone is someone to be respected and obeyed (such as someone claiming to be from tech support or a manager off-site), or a person with them is who they claim to be (such as an A/C repair technician).



For a complete discussion of social engineering, see section “1.6 Understanding Social Engineering” in Chapter 1.

Environment

When you’re designing a secure facility, it’s important to keep various environmental factors in mind. These include the following:

- Controlling the temperature and humidity
- Minimizing smoke and airborne dust and debris
- Minimizing vibrations
- Preventing food and drink from being consumed near sensitive equipment
- Avoiding strong magnetic fields
- Managing electromagnetic and radio frequency interference
- Conditioning the power supply
- Managing static electricity
- Providing proper fire detection and suppression

You need to focus on four of these issues, which are discussed next.

Wireless Cells

Wireless cells are the areas within a physical environment where a wireless device can connect to a wireless access point. Wireless cells can leak outside the secured environment and allow intruders easy access to the wireless network. You should adjust the strength of the wireless access point to maximize authorized user access and minimize intruder access. Doing so may require unique placement of wireless access points, shielding, and noise transmission.



For more information on wireless networking and site surveys, see section “2.6 Wireless” in Chapter 2, “Communication Security.”

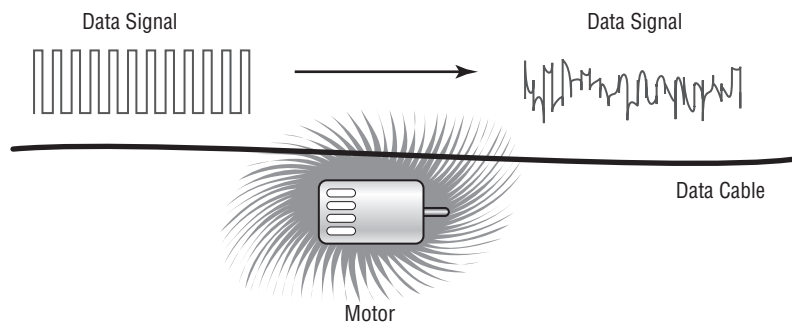
Location

Location refers to selecting the geographic placement of your facility. You should consider the implications of your facility’s location: for example, what is the local crime rate? What is the proximity to highways? How close are emergency services? Is the area in a flood zone, subject to earthquakes, or liable to experience excessive rain or snow? Knowing these characteristics will assist in the planning and design of the facility as well as the selection of the location.

Shielding

Shielding is used to restrict or control interference from electromagnetic or radio frequency disturbances (see Figure 5.3). This can include using shielded cabling, such as *shielded twisted pair* (STP), or cabling that is resistant to interference, such as fiber optic. It can include running networking cables and electrical power source cables through shielding conduit throughout the facility. Shielding can also refer to the use of metal walls, reflective wall coatings, or TEMPEST-level emanation shielding techniques (such as Faraday Cages).

FIGURE 5.3 Electromagnetic interference (EMI) pickup in a data cable



Fire Suppression

Fire is a common problem that must be addressed in the design of any facility. Electrical fires are common causes of building fires; they may result from overheated computer or networking equipment, or improperly managed electrical power cables and distribution nodes (power strips).

Early fire detection is important since the earlier the discovery, the less damage will be caused to the facility and equipment. Personnel safety is always of utmost importance. However, in a dedicated, secured, mission-critical server room (often called a *server cage*, *server vault*, or *data center*), the fire-suppression system can be gas-discharge based rather than water based. A

gas-discharge system removes oxygen from the air and may even suppresses the chemical reaction of combustion, often without damaging computer equipment; however, such systems are harmful to people.

Exam Essentials

Physical access control *Access control* refers to mechanisms designed to manage and control entrance into a location. Being able to control who can gain physical proximity to your environment (especially your computers and networking equipment) allows you to provide true security for your data, assets, and other resources. Without physical access control, you have no security.

Physical barriers Physical barriers are erected to control access into a location. Some of the most basic forms of physical barriers are walls and fences.

Boundary-crossing devices Doors and gates can be locked and controlled in such a way that only authorized personnel can unlock and enter through them. This control can take the form of a lock with a key that only authorized people possess. A security guard may check a person's credentials before granting entry. You can also use a biometrically controlled door.

Security guards The presence of security guards at an entrance or around the perimeter of a security boundary serves as a deterrent to intruders and provides a form of physical barrier. Guard dogs can also perform a basic function to protect against intrusion by detecting the presence of unauthorized visitors.

Mantraps A mantrap is a form of high-security barrier entrance device. It's a small room with two doors: one in the trusted environment and one opening to the outside. A person must properly authenticate to unlock the inner door and gain entry.

Biometrics used for physical security Locked doors that are used to control entrance into secured areas can be protected by locks that are keyed to biometrics.

Social engineering Social engineering is a form of attack that exploits human nature. Social engineering attacks can take two primary forms: convincing someone to either perform an unauthorized operation or reveal confidential information.

Environmental security issues When you're designing a secure facility, it's important to keep various environmental factors in mind. These factors include wireless cells, location, shielding, and fire suppression.

Wireless cells Wireless cells are the areas within a physical environment where a wireless device can connect to a wireless access point. Wireless cells can leak or reach outside the secured environment, allowing intruders easy access to the wireless network.

Location Location refers to the selection of the geographic placement of your facility. You should consider the implications of the location selected for your facility. Knowledge of location characteristics will assist in the planning and design of the facility as well as the selection of the actual location.

Shielding Shielding is used to restrict or control interference from electromagnetic or radio frequency disturbances. This can include using shielded cabling or cabling that is resistant to interference, or running cables through shielding conduit. Shielding can also refer to the use of metal walls, reflective wall coatings, or TEMPEST-level emanation shielding techniques (such as Faraday Cages).

Fire suppression Common causes of electrical fires are overheated computer or networking equipment and improperly managed electrical power cables and distribution nodes. A gas-discharge system removes oxygen from the air and suppresses the chemical reaction of combustion, often without damaging computer equipment; however, such systems are harmful to people.

5.2 Disaster Recovery

The full name of this section from the Security+ objectives list is “Understand the security implications of the following topics of disaster recovery.” Being able to restore operations after a significant disaster is an important part of a security policy and an overall security plan. The Security+ exam touches briefly on this issue.



For more information on disaster recovery, see Chapter 9 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Disaster recovery planning is an essential element of an overall security management plan. Disaster recovery is an expansion of business continuity planning. Basically, when business continuity is interrupted, a disaster has occurred. Ultimately, both business continuity and disaster recovery planning rely on proper backup procedures.

Backups

The mantra of all security professionals should be: backup, backup, backup. Backups are the only means of insurance available to your data resources in the event of a loss, disruption, corruption, intrusion, destruction, infection, or disaster.

Backups must be tested in order to prove reliable and usable. Testing a backup means restoring data from the backup media to verify that restoration can be done. If you don't test your restoration process, there is no guarantee that your backup was successful.

There are three primary forms of backup:

Full A full backup copies all files to the backup media regardless of the archive bit setting. It clears or resets the archive bit.

Incremental An incremental backup copies only those files with a set or flagged archive bit. It clears or resets the archive bit.

Differential A differential backup copies only those files with a set or flagged archive bit. It doesn't alter the archive bit.

Off Site Storage

Backup media should be stored securely at an offsite location in order to prevent it from being damaged or destroyed by the same catastrophe that affects the business continuity of the primary site. It should be stored in a fire-protected safe, vault, or safety deposit box. Backup tapes should be moved offsite soon after a backup is complete, and the transportation of the backup tapes should be secured. The tapes should be protected at all times from physical damage, theft, alteration, and destruction.

Secure Recovery

Secure recovery ensures that mission-critical, sensitive, or secured servers can be restored after a disaster with minimal loss or security violations. Secure recovery ensures that affected systems reboot into a secured state and that all resources open and active at the time of the fault, failure, or security violation are restored and have their security restrictions reimposed properly. Any damaged files are restored from backup, and their proper security labels are reapplied.

Alternate Sites

Secure recovery can also be expanded to an entire organization under a disaster recovery plan. An organization-wide secure recovery procedure involves the use of an alternate site: a secondary location where the business can move to and continue performing mission-critical business operations.

There are three levels of alternate sites:

Hot A hot site is a real-time, moment-to-moment mirror image of the original site. It contains a complete network environment that is fully installed and configured with a copy of the business data. The moment the original site becomes inoperable due to a disaster, the hot site can be used to continue business operations without a moment of downtime.

Warm A warm site is a partially configured alternate site with most of the server and networking infrastructure installed. In the event of a disaster, some final software installation and configuration is needed, and data must be restored from a backup set. A warm site may require hours or a day to get it ready for real-time operation to support the business's mission-critical functions.

Cold A cold site is nothing more than an empty room. It contains no equipment, and no communication links are installed. It requires the complete creation of a network from scratch before it can support the business's critical functions. Often, a cold site requires weeks to configure.

Although a hot site is the most desired form of alternate site, it's the most expensive. A cold site is the least costly, but it makes recovery nearly impossible.

When you return from the alternate site, the disaster could be repeated. The primary site is a new environment, because the original network and computer systems were damaged beyond their ability to support the business; significant changes, repairs, and replacements have occurred to restore the environment. The restored primary site must be stress-tested before the mission-critical operations of the business are transferred back to it. So, the least critical functions should be moved back to the primary site first. Then, after the site shows resiliency, you can move more critical functions as the network proves its ability to support the organization once again.

Disaster Recovery Plan

A *disaster recovery plan* is the collection of detailed procedures used in the event that business functions are interrupted by a significant damaging event. Once the primary site is unable to support business functions, the disaster recovery plan is initiated. This plan outlines the procedures for getting the mission-critical functions of the business up and running at an alternate site while the primary site is restored to normal operations.

A disaster recovery plan is developed through critical process inventory and prioritization, a risk analysis and assessment process, and a detailed examination of dependencies of resources.

The overall disaster recovery plan should include plan maintenance and distribution of revisions. Over time, as the environment changes, the disaster recovery plan should be adjusted to comply with those changes. Once the plan has been altered to a specified change level (amount of change), it must be redistributed throughout the organization. Only the most current version of the plan should be in existence: All older copies of the plan should be destroyed.

Exam Essentials

Disaster recovery Disaster recovery is an expansion of business continuity. Basically, when business continuity is interrupted, a disaster has occurred. Ultimately, both business continuity and disaster recovery planning rely upon proper backup procedures.

Backups Backups are the only means of insurance available to your data resources in the event of a loss, disruption, corruption, intrusion, destruction, infection, or disaster. Backups must be tested in order for them to prove reliable and usable.

Common types of backups The three common types of backups are full, incremental, and differential.

Offsite storage Backup media should be stored securely at an offsite location to prevent them from being damaged or destroyed by the same catastrophe that affects the business continuity of the primary site. This location should be a fire-protected safe, vault, or safety deposit box.

Secure recovery Secure recovery ensures that servers can be restored with minimal loss or security violations. It ensures that affected systems reboot into a secured state and that all

resources open and active at the time of the fault, failure, or security violation are restored and have their security restrictions reimposed properly.

Alternate sites An alternate site is a secondary location where the business can move and continue performing mission-critical business operations. There are three levels of alternate sites: hot, warm, and cold.

Disaster recovery plan A disaster recovery plan is the collection of detailed procedures used in the event that business functions are interrupted by a significant damaging event. Once the primary site is unable to support business functions, the disaster recovery plan is initiated. This plan outlines the procedures for getting the mission-critical functions of the business up and running at an alternate site while the primary site is restored to normal operations.

5.3 Business Continuity

The full name of this section from the Security+ objectives list is “Understand the security implications of the following topics of business continuity.” Business continuity is the ability of an organization to continue to perform its mission-critical processes in spite of events that threaten its infrastructure.



For more information on business continuity, see Chapter 9 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Maintaining business continuity means maintaining the organization’s networking and IT infrastructure so that mission-critical functions continue to operate. This must be done in spite of reduced resources and damaged equipment. As long as business operations aren’t stopped, business continuity is used to sustain the organization. If business operations are stopped, disaster recovery takes over.

Business continuity planning consists of the following elements:

Risk Analysis and Assessment This element includes itemizing the risks to each mission-critical aspect of the organization.

Business Impact Analysis You must determine how much any individual realized risk will negatively affect the business’s continuity and also computes the maximum tolerable downtime.

Strategic Planning for Mitigation of Risks You need to determine what countermeasures, safeguards, or responses can be used to minimize the effect of risks.

Integration and Validation of the Plan This step includes putting the plan into practice in the daily work habits of users, integrating it into the security policy, and validating it through senior management approval and testing.

Training and Awareness The organization needs to properly train users on their responses and responsibilities in an emergency and maintain awareness between training periods.

Maintenance and Auditing of the Plan You must regularly update the plan as the environment changes and constantly monitor the environment, the plan itself, testing, and training of the plan for areas where it can be improved.

Utilities

Utilities such as electricity, water, waste water, communication lines, Internet links, trash, gas, and so on are often overlooked when considering security and preparing for emergencies in business continuity and disaster recovery planning. When you're evaluating the mission-critical processes of a business, don't forget that most of those processes depend on basic foundational elements such as electricity and Internet connectivity.

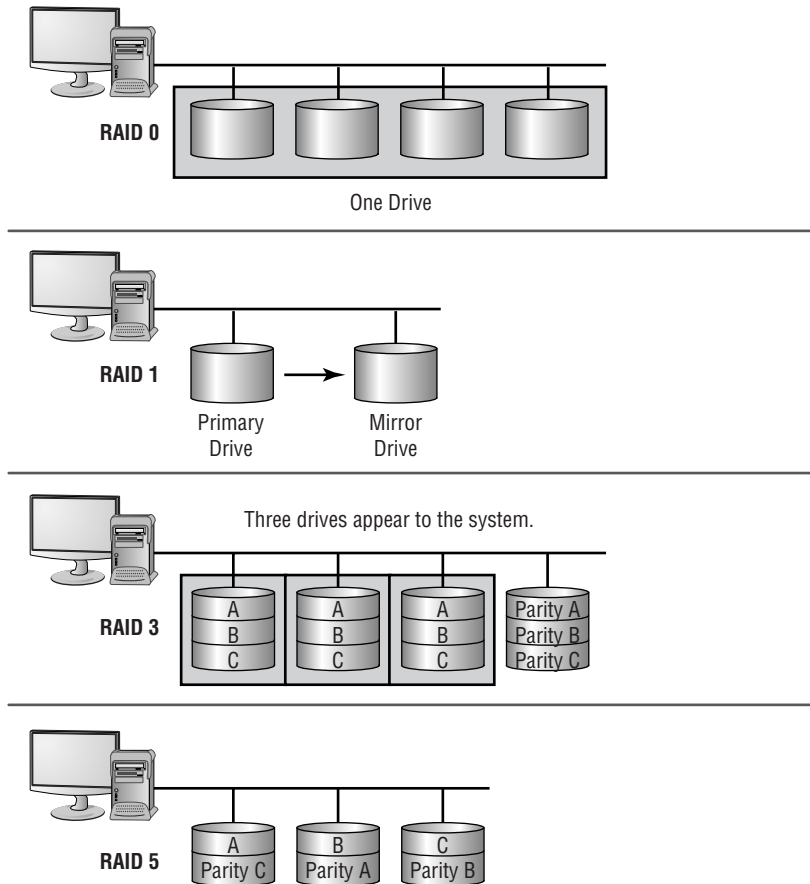
High Availability/Fault Tolerance

Availability is the assurance of sufficient bandwidth and timely access to resources. *High availability* means the availability of a system has been secured to offer very reliable assurance that the system will be online, active, and able to respond to requests in a timely manner, and that there will be sufficient bandwidth to accomplish requested tasks in the time required.

High availability is a form of fault tolerance—or, rather, a benefit of providing reliable fault tolerance. *Fault tolerance* is the ability of a network, system, or computer to withstand a certain level of failures, faults, or problems and continue to provide reliable service. Fault tolerance is also a means of avoiding single points of failure. A *single point of failure* is any system, software, or device that is mission critical to the entire environment: If that one element fails, then the entire environment fails. Your environments should be designed with redundancy so that there are no single points of failure. Such a redundant design is fault tolerant.

One example of a high-availability solution is a Redundant Array of Independent disks (RAID; see Figure 5.4). A RAID solution employs multiple hard drives in a single storage volume. RAID 1 provides mirroring: The data written to one drive is exactly duplicated to a second drive in real time. RAID 5 provides striping with parity: three or more drives are used in unison, and one drive's worth of space is consumed with parity information. The parity information is stored across all drives. If any one drive of a RAID 5 volume fails, the parity information is used to rebuild the contents of the lost drive on the fly. A new drive can replace the failed drive, and the RAID 5 system will rebuild the contents of the lost drive onto the replacement drive.

Another example of a high-availability solution is server clustering (see Figure 5.5). *Server clustering* is a technology that connects several duplicate systems together so they act cooperatively. If one system in a cluster fails, the other systems take over its workload. From a user's perspective, the cluster is a single entity with a single resource access name.

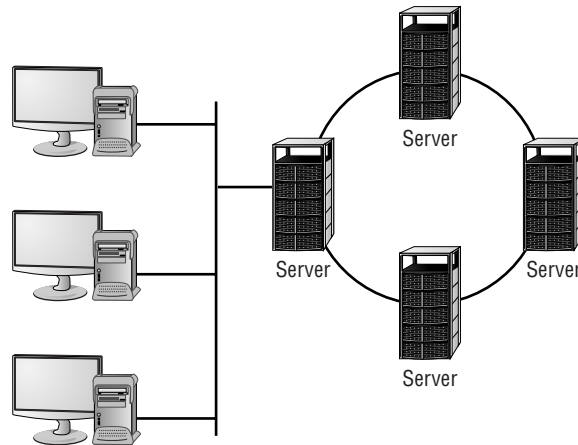
FIGURE 5.4 Examples of RAID implementations

Backups

Backups are an essential part of business continuity because they provide insurance against damage or loss of data files.



Backups are discussed in detail in section "5.2 Disaster Recovery."

FIGURE 5.5 Server clustering

Exam Essentials

Business continuity Maintaining business continuity means maintaining an organization's networking and IT infrastructure so that mission-critical functions continue to operate. This must be done in spite of reduced resources and damaged equipment.

Elements of business continuity planning The elements of business continuity planning include risk analysis and assessment, business impact analysis, strategic planning for mitigation of risks, integration and validation of the plan, training and awareness, and maintenance and auditing of the plan.

Utilities When you're evaluating the mission-critical processes of a business, don't forget that most of those processes depend on utilities, such as electricity and Internet connectivity.

High availability High availability means that the availability of a system has been secured to offer very reliable assurance that the system will be online, active, and able to respond to requests in a timely manner, and that there will be sufficient bandwidth to accomplish requested tasks in the time required. RAID is a high-availability solution.

Fault tolerance Fault tolerance is the ability of a network, system, or computer to withstand a certain level of failures, faults, or problems and continue to provide reliable service. Fault tolerance is also a form of avoiding single points of failure. A single point of failure is any system, software, or device that is mission critical to the entire environment.

5.4 Security Policy Issues

The full name of this section from the Security+ objectives list is “Understand the concepts and uses of the following types of policies and procedures.” A security policy is the foundational element of any successful security endeavor. In this section I discuss numerous examples of security policy. These forms of security documentation are designed to guide personnel in working within the desired security boundaries of an organization.



For more information on security policy issues, see Chapter 9 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

A security policy is not just one document; it consists of numerous documents, from high-level visionary statements to detailed step-by-step procedures. You need to be familiar with the following details about security policies and related documentation.

Security Policy

A *security policy* is the collection of documents that describes the overall purpose and direction of security in an environment as well as the detailed procedural documents that indicate how various activities are to be performed in compliance with security. It's generally recognized that security policy comprises four types of documents: policies, standards (also known as base-lines), guidelines, and procedures.

Any changes or updates to the security policy or any individual security document must be made available to all affected personnel. A security policy often contains many sub-policies that address various aspects of security, business operations, or human resource issues. Many common sub-policies are discussed in the following sections.

Acceptable Use

An *acceptable use policy* defines what is and what is not an acceptable activity, practice, or use for company equipment and resources. Not having an acceptable use policy leads many users into the false assumption that any activity is permitted and that they enjoy privacy even on company equipment. However, there is no privacy on company equipment: Companies have the right and privilege of auditing, monitoring, and recording all activities that occur using their equipment and access services. An acceptable use policy outlines these monitoring tactics, dictates what users can and can't do, and clearly states that users don't have privacy.

Often, employees must read and sign an acceptable use policy as part of the hiring and training process. This signed policy serves as consent from the user to be watched by the auditing mechanisms employed by the company.

Due Care

Due care is the display of proper security attention in an organization. By designing and implementing an organization-wide security policy, a business shows due care. The organization must put forth the proper and expected level of effort to provide protection from security violations and injury to assets and personnel.

Privacy

Privacy is the level of confidentiality and isolation a user is given in a system. Most users falsely assume that they have privacy on company computers. Privacy assumes that the activities and communications performed are hidden from others or at least protected from being viewed by all but the intended recipients. However, no activity on company property is hidden from view by the auditing and monitoring components of the network.

Separation of Duties

Separation of duties occurs when the administrative or sensitive operations of a computer, system, or network are divided among several people. In this way, no single person has complete privileges over the entire environment. This separation provides protection against fraud and loss by preventing a single administrator from taking over and causing a disaster.

Need to Know

A *need-to-know* security policy grants and restricts access by compartmentalizing resources, objects, or data within a security domain. To gain access to compartmentalized items, the subjects (users) must obtain or prove the need to know—the necessity to have access to a resource based on assigned work tasks. Without need-to-know policies, such data is restricted from view even for users with sufficient security clearance. This form of access control is used in Mandatory Access Control (MAC) environments, similar to the principle of least privilege that's used in Discretionary Access Control (DAC) environments (discussed later in section 5.5).

Password Management

Password management is the system used to manage passwords across a large network environment. It typically includes the requirement that users create complex passwords. Complex passwords are long (six or more characters), use multiple character types (such as uppercase, lowercase, numerals, and symbols), and use no part of the person's e-mail address or user account name. Other password restrictions may be enforced as well, such as a maximum and minimum lifetime, no reuse of old passwords (often called a *password history*), and use of account lockout.

Account lockout automatically disables an account when someone attempts to log on but fails repeatedly because they type in an incorrect password. Account lockout is often configured to lock out an account after three to five failed logon attempts within a short time (such as 15 minutes). Accounts that are locked out may remain permanently disabled until an administrator intervenes or may return to functional status after a specified period of time.

In larger environments, password management also includes a feature for users to change their own passwords as needed or when required. This self-service password reset function eliminates the need for an administrator to be involved in the process of redefining passwords.

SLAs (Service Level Agreements)

A *service level agreement (SLA)* is a contract with a service company, contract worker, or consultant team that dictates the minimum levels of service or performance demanded by your organization. SLAs can include requirements for uptime, hosting services, response time, downtime reimbursement, failure resolution, and throughput requirements.

Disposal/Destruction

Security policy should dictate how printed material and used storage media are to be handled after their useful lifetime. Secure disposal and destruction of printed material often involves shredding and incineration. Secure disposal and destruction of storage media may require incineration, physical crushing, magnetic destruction, or the use of an acid bath. Once these items have been properly destroyed, they no longer pose a threat to the environment. If a would-be intruder or attacker obtained these items after disposal and destruction, they would be unable to glean any useful information from them. In effect, proper disposal and destruction is a countermeasure to dumpster diving and scavenging.

HR (Human Resources) Policy

HR policies deal with aspects of security that focus directly on personnel. These include termination, hiring, and a code of ethics.

TERMINATION (ADDING AND REVOKING PASSWORDS AND PRIVILEGES, ETC.)

A termination policy defines the procedures to follow when an employee is fired. When an employee is terminated, their access to the network should be revoked immediately to prevent retaliatory acts and provide security for the company. An employee should return all access tokens, ID badges, and keys to the company as well as any company property such as notebooks, PDAs, cell phones, and so on. Once an employee is terminated, they shouldn't be allowed to reenter the work area or access the network—their access should be completely disabled. Otherwise, by distributing their access credentials, the ex-employee may be able to use any remaining level of access privilege to wage retaliatory acts or provide a means for intruders to infiltrate the organization.

HIRING (ADDING AND REVOKING PASSWORDS AND PRIVILEGES, ETC.)

A hiring policy defines the procedures to follow to hire new employees. When you're hiring new employees, it's important to perform background checks, including verifying education, previous work experience, and certifications. Depending on your organization's level of sensitivity, this policy may also require an intense security-focused background check. Once you've obtained reasonable assurance as to a new employee's trustworthiness, you can begin to grant that person access privileges to the physical and IT environment. As workers prove their reliability and are able to sustain compliance with security policies, their access may be increased as their assigned work tasks expand.

CODE OF ETHICS

Not all issues encountered through security incidents or IT operational procedures have a distinct response or procedure. In those situations where no clear policy exists, a solid understanding of a company-wide code of ethics is needed to guide workers through their decision-making

processes. Your company needs to establish priority parameters for difficult situations. For example, which is more important: meeting a deadline, following procedures, complying with policy, or remaining within budget? These and many other issues are complex and may involve ethical dilemmas. A company code of ethics provides decision-making guidelines for these situations.

Incident Response Policy

An *incident response policy* is the procedure to follow when a security breach or security violation has occurred. One of the most important goals of an incident response policy is *containment*: the protection and preservation of evidence. This may require taking systems offline, duplicating hard drives using imaging software, making photographs of monitor displays, documenting strange conditions or activities, disconnecting a server from the network, and so on.

For end users, the incident response policy is simple and direct: They should step away from their computer system and contact the incident response team.

Throughout the implementation of an incident response procedure, you should document every action taken by end users and the incident response team. This documentation will serve as an audit trail to retrace the actions taken and the events that occur during the incident. Learning from the incident's documentation includes taking precautions to prevent the reoccurrence of the incident, updating the security policy and related procedural documents, and assessing the overall impact of asset loss, damage, and risk imposed on the environment by the incident.

Exam Essentials

Security policy A security policy is the collection of documents that describes the overall purpose and direction of security in an environment as well as the detailed procedural documents that indicate how various activities are to be performed in compliance with security.

Acceptable use An acceptable use policy defines what is and what is not an acceptable activity, practice, or use for company equipment and resources.

Due care Due care is the display of proper security attention in an organization. By designing and implementing an organization-wide security policy, you show due care.

Privacy Privacy is the level of confidentiality and isolation that a user is given in a system. Most users falsely assume that they have privacy on company computers.

Separation of duties Separation of duties occurs when all the administrative or sensitive operations of a computer, system, or network are divided among several people. It provides protection against fraud and loss by preventing a single administrator from taking over and causing a disaster.

Need to know A need-to-know security policy grants and restricts access by compartmentalizing resources, objects, or data within a security domain. To gain access to those compartmentalized items, the subjects (users) must obtain or prove the need to know: the necessity to have access to a resource based on assigned work tasks.

Password management Password management is the system used to manage passwords across a large network environment. It typically includes a requirement for users to create complex passwords.

SLAs A service-level agreement (SLA) is a contract with a service company, contract worker, or consultant team that dictates the minimum levels of service or performance demanded by your organization.

Disposal and destruction Disposal and destruction refer to the security policy that dictates how printed material and used storage media are to be handled after their useful lifetime. Once these items have been properly destroyed, they no longer pose a threat to the environment.

Termination policies A termination policy defines the procedures to follow when an employee is fired. When an employee is terminated, their access to the network should be revoked immediately.

Hiring policies A hiring policy defines the procedures to follow to hire new employees. When you're hiring new employees, it's important to perform background checks. This includes verifying education, previous work experience, and certifications.

Code of ethics Not all issues encountered through security incidents or IT operational procedures have a distinct response or procedure. In those situations where no clear policy exists, a solid understanding of a company-wide code of ethics is needed to guide workers through their decision-making processes. Your company needs to establish priority parameters for difficult situations.

Incident response policy An incident response policy is the procedure to follow when a security breach or security violation has occurred. One of the most important goals of an incident response policy is containment: the protection and preservation of evidence.

5.5 Privilege Management

The full name of this section from the Security+ objectives list is “Explain the following concepts of privilege management.” Privilege management refers to controlling and managing users and their privileges and activities within a secured environment.



For more information on privilege management, see Chapter 9 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Managing user privileges is a key element in maintaining security. About 80 percent of the security violations that companies experience originate from within their secured facility. This means an organization is more at risk from its own users than from external intruders and hackers.

Thus, privilege management is necessary to sustain a secure and productive network. Issues of privilege management are discussed in the following sections.

User/Group/Role Management

Privilege management can be addressed using one of three primary schemes: user, group, or role. These schemes correspond directly to the access control methodologies of *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), and *Role-Based Access Control* (RBAC).



For more information on these roles, see section “1.1 Identifying Access Control Models.”

Single Sign-On

Single sign-on means that once a user (or other subject) is authenticated into the realm, they need not reauthenticate to access resources on any realm entity. This allows users to access all the resources, data, applications, and servers they need to perform their work tasks with a single authentication procedure. Single sign-on eliminates the need for users to manage multiple user-names and passwords, since only a single set of logon credentials is required.

Kerberos is an example of a single sign-on solution.



Kerberos is discussed in Chapter 1.

Centralized vs. Decentralized

There are two over-arching approaches to privilege management: centralized and decentralized. In centralized privilege management, a single server (or set of servers) is responsible for managing, controlling, and implementing all security controls, access rights, and privileges. A domain network and a RADIUS authentication server are great examples of centralized privilege management solutions. In decentralized privilege management, each individual system is responsible for managing, controlling, and implementing security controls, access rights, and privileges. A workgroup network is a perfect example of a decentralized privilege management solution.

Auditing (Privilege, Usage, Escalation)

A *privilege* is an ability or activity that a user account is granted permission to perform. User accounts are often assigned privileges based on their work tasks and their normal activities. The *principle of least privilege* is a security rule of thumb that states that users should be granted only the level of access needed for them to accomplish their assigned work tasks, and no more. Furthermore, those privileges should be assigned for the shortest time period possible.

Exploitation of privileges is known as *privilege abuse* or *privilege escalation*. Privilege escalation occurs when a user account is able to obtain unauthorized access to higher levels of privileges, such as a normal user account that can perform administrative functions. Privilege escalation can occur through the use of a hacker tool or an incorrectly configured environment. It can also occur when lazy administrators fail to remove older privileges as a user is granted new privileges based on new job descriptions. An accumulation of privileges can be considered a form of privilege escalation.

Auditing should be used to monitor and track not just the assignment of privilege and the unauthorized escalation of privilege but also privilege usage. Knowing what users are doing and how often they do it may assist administrators in assigning and managing privileges.



Auditing is discussed in detail in Chapter 1, in section “1.7 Understanding Auditing.”

MAC/DAC/RBAC (Mandatory Access Control/Discretionary Access Control/Role Based Access Control)

One aspect of privilege management is the use of the correct access control system appropriate to your environment and security needs. The three common access control systems are MAC, DAC, and RBAC.



MAC, DAC, and RBAC are discussed in Chapter 1, in section “1.1 Identifying Access Control Models.”

Exam Essentials

User, group, and role management Privilege management can be addressed using one of three primary schemes: user, group, or role. These schemes correspond directly to the access control methodologies of DAC, MAC, and RBAC.

Single sign-on Single sign-on means that once a user (or other subject) is authenticated into a realm, they need not reauthenticate to access resources on any realm entity.

Centralized privilege management In centralized privilege management, a single server (or set of servers) is responsible for managing, controlling, and implementing all security controls, access rights, and privileges. A domain network and a RADIUS authentication server are great examples of centralized privilege management solutions.

Decentralized privilege management In decentralized privilege management, each individual system is responsible for managing, controlling, and implementing security controls, access rights, and privileges. A workgroup network is an example of a decentralized privilege management solution.

Privileges A privilege is an ability or activity that a user account is granted permission to perform. User accounts are often assigned privileges based upon their work tasks and their normal usage.

Principle of least privilege The principle of least privilege is a security rule of thumb that states that users should be granted only the level of access needed for them to accomplish assigned work tasks, and no more. Furthermore, those privileges should be assigned for the shortest time period possible.

Privilege escalation Privilege escalation occurs when a user account is able to obtain unauthorized access to higher levels of privileges, such as a normal user account that can perform administrative functions.

5.6 Forensics

The full name of this section from the Security+ objectives list is “Understand the concepts of the following topics of forensics.” *Forensics* is the collection, protection, and analysis of evidence from a crime in order to present the facts of the incident in court.



For more information on forensics, see Chapter 10 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

One of the most critical aspects of forensics is the initial gathering and protection of evidence. In order for evidence to be presentable in court, you must be able to show that the chain of custody wasn't broken, that the evidence was properly preserved, and that the evidence was collected properly.

Chain of Custody

The *chain of custody* is a document that indicates various details about evidence across its life cycle. It begins with the time and place of discovery, who discovered the evidence, who secured it, who collected it, who transported it, who protected it while in storage, and who analyzed it. The chain of custody must be created and maintained from the moment evidence is discovered through the presentation of the evidence in court.

Preservation of Evidence

Evidence should be protected from alteration, damage, and corruption from the moment of its discovery through the rest of its lifetime, which may be concluded once it's presented in court. Evidence preservation includes properly managing the chain-of-custody document, collecting

the evidence into transportable containers, clearly labeling those containers, and then providing a secure environment for the evidence. A secure environment prevents damage and theft, but it also maintains the proper temperature and humidity while avoiding dust, smoke, debris, magnetic fields, and vibrations.

Collection of Evidence

Collection of evidence is the procedure of securing evidence by collecting it. This process is often called *bag and tag*. Basically, evidence is gathered, placed in a container, and labeled, and its chain-of-custody document is filled out. It's the responsibility of the crime scene technician to collect evidence.

Exam Essentials

Chain of custody The chain of custody is a document that indicates various details about evidence across its life cycle. It begins with the time and place of discovery, who discovered the evidence, who secured it, who collected it, who transported it, who protected it while in storage, and who analyzed it.

Evidence preservation Evidence should be protected from alteration, damage, and corruption from the moment of its discovery through the rest of its lifetime, which may be concluded once it's presented in court.

Collection of evidence Collection of evidence is the procedure of securing evidence by collecting it. This process is often called *bag and tag*. Basically, evidence is gathered, placed in a container, and labeled, and its chain of custody document is filled out. It's the responsibility of the crime scene technician to collect evidence.

5.7 Risk Identification

The full name of this section from the Security+ objectives list is "Understand and be able to explain the following concepts of risk identification." Risk identification is an essential part of an organization's security endeavor. Without performing a risk assessment and analysis, you won't know what problems your security policy needs to address.



For more information on risk identification, see Chapter 1 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Computer systems and networks can never be completely secure. However, that fact shouldn't prevent you from securing your environment as much as possible. Using asset identification,

risk assessment, threat identification, and vulnerability management focuses your security endeavors on those areas that pose the greatest threat to your assets.

Asset Identification

You don't know what to protect if you don't know what you have. A thorough asset inventory must be performed to identify mission-critical systems as well as everyday items (like paperclips and sticky notes) that your organization needs to perform its services and produce its products. Once you have a master inventory, you can prioritize your assets. You can then perform risk assessment for the most important items first; as you provide additional protection for them, you move on to less important items.

Risk Assessment

The goal of risk assessment, risk management, and risk analysis is to minimize the impact of risks on an organization. This is done through *mitigation* (applying safeguards or countermeasures), *assignment* (outsourcing or obtaining insurance), or *acceptance* (accepting the potential losses). This process identifies potential threats, evaluates the potential impact of those threats, and weighs the cost in terms of protection mechanisms needed and the potential loss or interruption of business continuity.

Four common formulas are associated with risk assessment and risk analysis:

Exposure Factor (EF) This is the percentage of asset value loss that would occur if a risk was realized (for example, if an attack took place).

Single Loss Expectancy (SLE) This is the potential dollar-value loss from a single risk realization incident. It's calculated by multiplying the EF by the asset value.

Annualized Rate of Occurrence (ARO) This number is the statistical probability that a specific risk may be realized a certain number of times in a year. It's obtained from a risk assessment company or an insurance company.

Annual Loss Expectancy (ALE) This is the potential dollar value loss per year per risk. It's calculated by multiplying the SLE by the ARO.

Threat Identification

A *threat* is any person or tool that can take advantage of a vulnerability. Threat identification is a formal process of outlining the potential threats to a system.

Vulnerabilities

A *vulnerability* is a weakness, error, or hole in the security protection of a system, network, computer, software, and so on. When a vulnerability exists, threats may exist to exploit it. You can use countermeasures and safeguards to patch vulnerabilities. Once a vulnerability is patched, threats no longer impose a danger to your systems.

Exam Essentials

Asset identification A thorough asset inventory must be performed to identify mission-critical systems as well as everyday items (like paperclips and sticky notes) that your organization needs to perform its services and produce its products. Once you have a master inventory, you can prioritize your assets.

Risk assessment The goal of risk assessment is to minimize the impact of risks on an organization. This is done through mitigation, assignment, or acceptance. This process identifies potential threats, evaluates the potential impact of those threats, and weighs the cost in terms of protection mechanisms needed and the potential loss or interruption of business continuity.

Risk assessment formulas The different risk assessment formulas are exposure factor (EF), single loss expectancy (SLE), annualized rate of occurrence (ARO), and annual loss expectancy (ALE).

Threats A threat is any person or tool that can take advantage of a vulnerability. Threat identification is a formal process of outlining the potential threats to a system.

Vulnerabilities A vulnerability is a weakness, error, or hole in the security protection of a system, network, computer, software, and so on. When a vulnerability exists, threats may exist to exploit it. You can use countermeasures and safeguards to patch vulnerabilities.

5.8 Security Training

The full name of this section from the Security+ objectives list is “Understand the security relevance of the education and training of end users, executives and human resources.” Security is useless if users aren’t properly trained to perform their work tasks within the confines of the secured environment.



For more information on security training, see Chapter 10 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

Security training for employees is essential to the success of any security endeavor. It should be part of your security policy and business operations. This should include communication, awareness training, education, and support through online resources.

Communication

As a security professional in any organization, you must keep the lines of communication open. This means you should be up front about security requirements for all personnel. Clearly train users on how to perform their work tasks while maintaining security.

As a manager, be open to discuss security issues with users from every level and classification. Be ready to discuss good and bad aspects of security. And, be willing to assist users in learning to be efficient and productive while sustaining security. By keeping communication open and abundant, you can help prevent users from giving up on security and intentionally bypassing security procedures.

User Awareness

User awareness is an effort to make security a regular thought for all employees. It begins with security training and orientation when a new worker is hired. However, user awareness must continue throughout the life of the organization. It includes regular reminders, refresher seminars, e-mails with security updates, newsletters, intranet websites, posters with security facts or rules, and so on—whatever is necessary to keep users aware of the importance of security.

If an organization fails to maintain user awareness of security, it will experience a slow erosion of security that may ultimately allow a serious intrusion to occur. Unfortunately, user awareness of security is generally the most overlooked element of security management. In fact, the lack of security awareness is the primary reason that social-engineering attacks succeed. With proper information, users can be equipped to recognize social-engineering attacks and avoid being taken in by them.

Education

Education is broad security training, usually focused on teaching a user to perform their work tasks securely. Security education has the ultimate goal of certification. Certification is the act of passing one or more exams in order to earn certification credentials (i.e., impressive acronyms to add to your resume), which verify that you possess certain knowledge, skills, and expertise.

On-line Resources

Security documentation, especially work-task-specific instructions, should be posted to an intranet website for easy access. In this way, users can keep themselves current on changing security policies and procedures.

Exam Essentials

Communication As a security professional in any organization, you must keep the lines of communication open. This means you should be up front about security requirements for all personnel. Clearly train users on how to perform their work tasks while maintaining security.

User awareness User awareness is an effort to make security a common and regular thought for all employees. Unfortunately, user security awareness is generally the most overlooked

element of security management. In fact, the lack of security awareness is the primary reason that social-engineering attacks succeed.

Security education Education means broad security training, usually focused on teaching a user to perform their work tasks securely. Security education is broader and has the ultimate goal of certification.

5.9 Security Documentation

The full name of this section from the Security+ objectives list is “Understand and explain the following documentation concepts.” As a standard rule of thumb for security, you should document everything. Documentation is often seen as a keystone of security. Through exhaustive documentation there will always be a detailed record of configurations, actions, procedures, etc. which will assist in the event of an incident, disaster, or implementation of change.



For more information on documentation, see Chapter 10 of the *Security+ Study Guide, Second Edition*, by Sybex.

Critical Information

With complete, detailed, exhaustive documentation, every aspect of your environment and every event in your secured environment are known. Documentation can be reviewed and referenced as new incidents or conditions arise. With proper documentation, the security of an organization is easier to maintain.

Standards and Guidelines

Standards and *guidelines* are elements of a security policy. A standards document dictates the required minimum security baselines that must exist for all systems throughout an organization. Using standards allows an organization to maintain a foundational minimum level of security on which to build even more secure solutions, systems, or areas. Standards can also outline industry or regulatory restrictions (such as those issued by HIPPA, the SEC, health codes, the FAA, the FCC, and so on) that must be complied with in order to avoid breaking any laws.

Guidelines are general-purpose documents that discuss security features, needs, and intentions. You should follow a guideline when a detailed specific procedure doesn't exist.

Systems Architecture

The construction of a system should be detailed in documentation. By outlining and categorizing the architecture of all systems in an organization, you simplify the procedures for upgrading and repairing those systems. If you know all the details about a computer, then the time and effort involved in repairing, upgrading, or duplicating that system are minimized.

Change Documentation

Change is the antithesis of security. In fact, change often results in reduced security. Therefore, security environments often implement a system of change management to minimize the negative impact of change on security. *Change documentation* is one aspect of a change-management system: It's the process of writing out the details of changes to be made to a system, computer, software, network, and so on before they're implemented. Then, the change documentation is transformed into a procedural document that is followed to the letter to implement the desired changes. Once the changes are implemented, the system is tested to see whether security was negatively affected. If security has decreased, the change documentation can be used to guide the reversal of the changes to restore the system to a previous state where stronger security was enforced.

Logs and Inventories

Logs, also known as *audit trails*, are files that collect details about events occurring within a computer system. These events can be security related, function related, or activity related. Logs keep a historical record of system activity and usage. In order for a logging system to be effective, an administrator must regularly review the log files. When reviewing the log files, the administrator looks for abnormal or significant events that may indicate breaches of security or the occurrence of unwanted, unethical, or unacceptable activities. This process is known as *passive detection*.

An *inventory* is a list of assets owned by a company, including all hardware devices, software, office equipment, and office supplies. The inventory can be used to obtain insurance and may be used in risk management to help guide the asset identification process.

Classification

Classification is the process of labeling objects (assets, data, information, and so on) with sensitivity labels and subjects (users) with clearance labels.



This topic is discussed in more detail in Chapter 1, in section “1.1 Identifying Access Control Models.”

Notification

Notification is the formal process by which users are informed when changes are made to security policies, classifications, or procedures. Any time a change affects a user's work tasks or alters security, a notification document should be distributed to all affected parties.

Retention/Storage

Retention and *storage* refer to the company policy of recording and warehousing information about the environment through audit trails, logs, backups, and so on. The security policy should include a discussion of what information will be recorded, how it will be stored, and how long it will be retained. This indication of a company's retention and storage policies benefits end users as well as the company itself. In the event of a crime, information may be pulled from stored data and used as evidence; e-mail messages are a common example of such data.

Destruction

At the end of the useful lifetime of documentation, or when it's been replaced or updated, all old copies should be removed from all intranet sites and from all printed materials. Old and out-of-date documentation should be taken out of circulation and properly destroyed. For printed material, this usually means shredding and/or incineration.

Exam Essentials

Standards A standards document dictates the required minimum security baselines that must exist for all systems throughout an organization. Using standards allows an organization to maintain a foundational minimum level of security on which to build even more secure solutions, systems, or areas. Standards can also outline the industry or regulatory restrictions that must be complied with to avoid breaking any laws.

Guidelines Guidelines are general-purpose documents that discuss security features, needs, and intentions. A guideline should be used when a detailed specific procedure doesn't exist.

System architecture documentation The construction of a system should be detailed in documentation. By outlining and categorizing the architecture of all systems in an organization, you simplify the procedures for upgrading and repairing those systems. If you know all the details about a computer, then the time and effort involved in repairing, upgrading, or duplicating a system are minimized.

Change documentation Change documentation is the process of writing out the details of changes to be made to a system. Once the changes are implemented, the system is tested to see whether security was negatively affected. If security has decreased, the change documentation can be used to guide the reversal of the changes in order to restore the system to a previous state where stronger security was enforced.

Logs Logs (another term for audit trails) are files that collect details about events occurring within a computer system. Logs keep a historical record of system activity and system usage. In order for a logging or auditing system to be effective, an administrator must regularly review the log files.

Inventories An inventory is a list of assets owned by a company. It includes all hardware devices, software, office equipment, and office supplies.

Notification Notification is the formal process by which users are informed when changes are made to security policy, classifications, or procedures. Any time any change affects a user's work tasks or alters security, a notification document should be distributed to all affected parties.

Retention and storage policies Retention and storage refer to the company policy of recording and warehousing information about the environment.

Documentation destruction At the end of the useful lifetime of documentation, or when it's been replaced or updated, all old copies should be removed from all intranet sites and from all printed materials. Old and out-of-date documentation should be taken out of circulation and properly destroyed.

Review Questions

1. Which of the following can be considered a physical barrier?
 - A. Strong passwords
 - B. Firewalls
 - C. Security guard
 - D. AES
2. You run a full backup every Monday. You also run a differential backup every other day of the week. You experience a drive failure on Friday. Which of the following restoration procedures should you use to restore data to the replacement drive?
 - A. Restore the full backup and then each differential backup.
 - B. Restore the full backup and then the last differential backup.
 - C. Restore the differential backup.
 - D. Restore the full backup.
3. When is business continuity needed?
 - A. When new software is distributed
 - B. When business processes are interrupted
 - C. When a user steals company data
 - D. When business processes are threatened
4. When a user signs a(n) _____, it's a form of consent to the monitoring and auditing processes used by the organization.
 - A. Acceptable use policy
 - B. Privacy policy
 - C. Separation of duties policy
 - D. Code of ethics policy
5. In a MAC environment, when a user has clearance for assets but is still unable to access those assets, what other security feature is in force?
 - A. Principle of least privilege
 - B. Need to know
 - C. Privacy
 - D. Service level agreement

6. Which of the following is not a benefit of single sign-on?
 - A. Browsing multiple systems
 - B. Fewer usernames and passwords to memorize
 - C. More granular access control
 - D. Stronger passwords
7. Evidence is inadmissible in court if which of the following is violated or mismanaged?
 - A. Chain of custody
 - B. Service level agreement
 - C. Privacy policy
 - D. Change management
8. Which of the following risk assessment formulas represents the total potential loss a company may experience within a single year due to a specific risk to an asset?
 - A. EF
 - B. SLE
 - C. ARO
 - D. ALE
9. If user awareness is overlooked, what attack is more likely to succeed?
 - A. Man in the middle
 - B. Reverse hash matching
 - C. Physical intrusion
 - D. Social engineering
10. What is the primary purpose of system architecture documentation?
 - A. Insurance purchasing
 - B. Ease of upgrade and repair
 - C. Risk assessment
 - D. Awareness training

Answers to Review Questions

1. C. A security guard can be considered a physical barrier. Strong passwords, firewalls, and AES are all technology barriers.
2. B. The proper procedure is to restore the full backup and then the last differential backup. The other three options are incorrect or incomplete.
3. D. Business continuity is used when business processes are threatened. Security policy is used when new software is distributed. Disaster recovery is used when business processes are interrupted. Incident response is used when a user steals company data.
4. A. When a user signs an acceptable use policy, it's a form of consent to the monitoring and auditing processes used by the organization. A privacy policy usually explains that there is no privacy on company systems. A separation of duties policy indicates that administrative functions are divided among several people. The code of ethics policy describes decision-making processes to use when faced with ethical delimas.
5. B. *Need to know* is the MAC environment's granular access control method. The principle of least privilege is the DAC environment's concept of granular access control. Privacy and SLAs aren't forms of access control.
6. C. Single sign-on doesn't address access control and therefore doesn't provide granular or nongranular access control. Single sign-on provides the benefits of browsing multiple systems, fewer credentials to memorize, and the use of stronger passwords.
7. A. If the chain of custody is violated or mismanaged, evidence is inadmissible in court. SLAs, privacy policies, and change management aren't associated with evidence gathering or forensics.
8. D. The annual loss expectancy (ALE) represents the total potential loss a company may experience within a single year due to a specific risk to an asset. EF is the percentage of asset value loss that would occur if a risk was realized. SLE is the potential dollar value loss from a single risk realization incident. ARO is the statistical probability that a specific risk may be realized a certain number of times in a year.
9. D. Social engineering is more likely to occur if users aren't properly trained to detect and prevent it. The lack of user awareness training won't have as much impact on man-in-the-middle, reverse hash matching, or physical intrusion attacks.
10. B. The primary purpose of system architecture documentation is to simplify upgrades and repairs. It has secondary uses in insurance purchasing and risk assessment. It has no relation to awareness training.

Index

Note to the Reader: Throughout this index page numbers in bold indicate primary discussions or definitions of a topic. Italicized page numbers indicate illustrations.

Numbers

8.3 naming conventions, **63**
10Base2/Thinnet cable, **83**
10Base5/Thicknet cable, **83**
10BaseT cable, **85, 86**
100BaseT cable, **86**
802.11/11x wireless networks, **40**,
40–41, 65
1000BaseT cable, **86**

A

AAA servers, **43**
acceptable use policy, **163**
acceptance of risk, **172**
access control, *See also* remote access
 in cryptography, **128**
 in physical security, *See also*
 operational
 barriers, **151–152, 152**
 biometrics, **14–15, 152**
 defined, **150–151, 151**
 mantraps, **152, 152**
 security guards, **152**
to resources, *See also* Security+
 defined, **3**
 Discretionary Access Control, **5–6**
 exam essentials on, **6–7**
 Mandatory Access Control, **4–5**
 overview, **3–4, 168, 169**
 Role-Based Access Control, **6**
access hooks, **21**
account lockout, **164**
ACLs (access control lists), **5, 107**
active detection and response, **98**,
 99–100
ActiveX vulnerability, **57**
ad hoc mode, **66**
agents, **18**
AH (Authentication Header)
 protocol, **45**
ALE (Annual Loss Expectancy)
 formula, **172**
alternate sites, **157–158**
amplification networks, **19**
anomaly detection, **97, 98**
anonymous FTP, **62–63**
application hardening. *See* environment
application-level gateway firewalls, **76**
architecture documentation, **175**
ARO (Annualized Rate of Occurrence)
 formula, **172**
asset identification, **172**
asset inventories, **176**
assignment of risk, **172**
asymmetric encryption, **49–51, 50–51**,
 123, 126, 127
attack methods, *See also* IDSs;
 Security+; vulnerabilities
 back door, **21–22, 22**
 birthday, **26, 120**
 broadcast storm, **92**
 buffer overflow, **27, 57–58**
Denial of Service attacks
 bonk and boink, **21**
 countermeasures against, **21**
 defined, **18**
Distributed DOS, **19, 19**

- Distributed Reflective DOS, 19
 - fraggle, 19
 - land, 21
 - ping flood, 21
 - ping of death, 21
 - smurf, 19, 20
 - SYN flood, 20, 20
 - teardrop, 20, 20
 - eavesdropping, 56–57
 - exam essentials on, 28–29
 - on hashing, 120–121
 - malicious code
 - defined, 29
 - exam essentials on, 30
 - logic bombs, 30
 - Trojan horses, 30
 - viruses, 29
 - worms, 30
 - man-in-the-middle, 23, 23
 - mathematical, 25
 - overview, 18
 - packet sniffing, 56–57, 63, 78
 - password cracking, 12, 26–27, 120–121
 - replay, 24, 24
 - reverse hash matching, 26, 120
 - social engineering, 31–32, 52–53, 153
 - software exploitation, 27
 - spoofing, 22–23, 52
 - TCP/IP hijacking, 24, 25
 - war dialing, 79
 - attack surfaces, 15
 - attenuation, 83
 - auditing
 - audit trails/logs, 32, 33, 176
 - defined, 32–33
 - privileges, 169
 - using SNMP protocol, 81
 - authentication, *See also* Security+
 - in cryptography, 127
 - defined, 3
 - methods
 - biometrics, 14–15, 152
 - certificates, 10–11, 11
 - CHAP, 9–10, 10
 - defined, 7
 - exam essentials on, 15
 - Kerberos, 7–9, 9
 - multi-factor authentication, 13–14, 14
 - mutual authentication, 14
 - tokens, 13, 13
 - usernames/passwords, 12, 12
 - strong authentication, 14
 - tools
 - RADIUS, 42–43, 43
 - supported by L2TP/PPTP protocols, 44
 - TACACS, 43, 43
 - authentication servers, 110
 - authorization, 3, *See also* access control
 - availability, 160
-
- ## B
- back door attacks, 21–22, 22
 - backups, 156–157, 161
 - bag and tag process, 171
 - baseband signaling, 85, 85
 - biometrics, 14–15, 152
 - birthday attacks, 26, 120
 - blind FTP, 63
 - block cipher cryptography, 122
 - BNC connectors, 83, 83–84
 - boink/bonk attacks, 21
 - boot sector viruses, 29
 - bots, 18
 - bounce networks, 19
 - bridge trusts, 132, 133
 - broadband signaling, 85, 85

brute-force attacks, 27
 buffer overflow attacks, 27, 57–58
 business continuity, *See also* operational
 backups, 161
 defined, 159
 elements in planning, 159–160
 exam essentials, 162
 high availability/fault tolerance,
 160–161
 utilities, 160

C

callback feature, 79
 CD-R disks, 88
 centralized key management, 136–137,
 137, 138, 139
 centralized privilege management, 168
 certificates, *See also* cryptography
 certificate authorities, 10, 129, 130
 certificate policies, 131
 certificate practice statements, 131
 defined, 10–11, 11, 129
 destruction, 141
 expiration, 139
 obtaining, 10–11, 11, 130–131
 renewal, 140–141
 revocation, 131–132, 132, 139
 status checking, 139, 140
 storage, 138
 suspension, 140
 trust models, 132–134, 133
 trusted third parties, 10, 129
 X.509 certificates, 129, 130
 certification credentials, 174
 CGI (Common Gateway Interface), 58
 chain of custody, 170
 change documentation, 176
 CHAP (Challenge Handshake Authentica-
 tion Protocol), 9–10, 10
 circuit-level gateway firewalls, 76
 classification labeling, 4, 176
 clearance levels, 4–5
 clients, 81
 clustering servers, 160, 162
 coaxial cable, 83–85, 83
 code of ethics policy, 165–166
 cold sites, 157–158
 common routers, 76
 communication security, 39–70, *See also*
 Security+
 directory security, 60–61, 61
 e-mail security
 using digital signatures, 50–51, 51
 exam essentials on, 53–54
 using filters, 52
 hardening e-mail servers, 1
 08–109, 108
 hoax e-mail, 52–53
 MIME headers and, 51
 overview, 48, 49
 using PGP encryption, 50
 using S/MIME encryption,
 49–50, 50
 spam e-mail, 52
 spoofed e-mail, 52
 vulnerabilities, 51–53
 File Transfer Protocol
 anonymous FTP, 62–63
 blind FTP, 63
 defined, 62
 exam essentials on, 63–64
 file sharing, 63
 overview, 61–62
 Secure FTP, 62
 vulnerabilities, 63
 Internet security
 ActiveX and, 57

- buffer overflow attacks, 57–58
- cookies and, 58
- exam essentials on, 59–60
- HTTP protocol and, 54–55, 55, 56
- using HTTPS protocol, 56
- instant messaging and, 56–57
- JavaScript and, 57
- overview, 54–55, 55
- using S-HTTP protocol, 56
- signed applets and, 58
- SMTP relay and, 58–59
- using SSL encryption, 55–56
- using TLS encryption, 55, 56
- vulnerabilities, 56–59
- remote access security
 - in 802.11/11x wireless, 40–41, 40, 65
 - exam essentials on, 47–48
 - in IPSec protocols, 44–46, 45–46
 - in L2TP protocol, 44
 - overview, 39–40, 39
 - in PPTP protocol, 44
 - using RADIUS, 42–43, 43
 - using Secure Shell, 44
 - using TACACS, 43, 43
 - in virtual private networks, 41–42, 41
 - vulnerabilities, 46–47
- review question answers, 70
- review questions, 68–69
- wireless security
 - in 802.11/11x networks, 40–41, 40, 65
 - exam essentials on, 66–67
 - overview, 64
 - vulnerabilities, 66
 - using Wired Equivalent Privacy, 65
 - using WTLS in WAP protocol, 64–65, 65
- communication in security training, 174
- confidentiality, 4, 125, 125
- containment, 102, 166
- cookies, 58
- CPSs (certificate practice statements), 131
- CRLs (certificate revocation lists), 131–132, 132
- cross certification, 132, 133
- cryptography, 119–146, *See also* Security+
 - cryptographic algorithms
 - asymmetric encryption, 49–51, 50–51, 123, 126, 127
 - exam essentials, 124
 - hashing, 26, 119–121, 120
 - overview, 119
 - symmetric encryption, 46, 121–122, 126–127, 127
- encryption protocols
 - for e-mail, 49–51, 50–51
 - IPSec, 44–46, 45–46
 - Pretty Good Privacy, 50–51, 51
 - for remote access, 44–46, 45–46
 - S/MIME, 49–50, 50
 - Secure Sockets Layer, 55–56
 - Transport Layer Security, 55, 56
 - for web browsers/servers, 55–56
- key and certificate management
 - centralized key management, 136–137, 137, 138, 139
 - decentralized key management, 137–138, 137
 - destruction, 141
 - exam essentials, 141–143
 - expiration, 139
 - key disasters, 138
 - key management rules, 136
 - key usage, 141
 - M of N key control, 140
 - multiple key pairs, 141
 - overview, 136

- private key escrow, 138–139, 139
- private key protection, 138
- recovery from escrow, 140
- renewal, 140–141
- revocation, 131–132, 132, 139
- status checking, 139, 140
- storage, 138
- suspension, 140
- Public Key Infrastructure
 - certificate authorities, 10, 129, 130
 - certificate policies, 131
 - certificate practice statements, 131
 - certificate revocation, 131–132, 132
 - defined, 10–11, 11, 122, 129
 - exam essentials, 134–135
 - obtaining certificates, 10–11, 11, 130–131
 - trust models, 132–134, 133
 - trusted third parties, 129
 - X.509 certificates, 129, 130
- review question answers, 146
- review questions, 144–145
- security services
 - access control, 128
 - authentication, 127
 - confidentiality, 125, 125
 - digital signatures, 126–127, 127, 128
 - exam essentials, 128–129
 - integrity, 125–127, 127
 - nonrepudiation, 128
 - overview, 125
- standards and protocols, 135
- vulnerabilities
 - hashing, 26, 120–121
 - key recovery, 140
 - key storage, 137, 138
 - weak keys, 25

D

- DAC (Discretionary Access Control), 5–6, 7, 164, 168, 169
- data centers. *See* server rooms
- data repository servers, 110
- database servers, 111
- DDOS (Distributed Denial of Service), 19, 19, *See also* DOS
- decentralized key management, 137, 137–138
- decentralized privilege management, 168
- DHCP (Dynamic Host Configuration Protocol) servers, 110
- diagnostics. *See* auditing
- dictionary attacks, 27
- differential backups, 157
- digital signatures
 - using asymmetric encryption, 50–51, 51, 126
 - defined, 126
 - for nonrepudiation, 50, 128
 - signed applets, 58
 - using symmetric encryption, 126–127, 127
- directory security, 60–61, 61
- directory services, 61, 61, 110, 111
- disaster recovery, *See also* operational
 - alternate sites, 157–158
 - backups, 156–157
 - exam essentials, 158–159
 - offsite storage, 157
 - overview, 156
 - plans, 158
 - secure recovery, 157
- disclosure, 4
- diskettes, 88
- disposal/destruction policy, 165

DMZs (demilitarized zones), 62, 76,
90, 90

DNS (Domain Name Service)
servers, 109

documentation. *See* security
documentation

domain controllers, 110

DOS (Denial of Service) attacks,

See also attack

bonk and boink, 21

buffer overflows as, 57–58

countermeasures against, 21

defined, 18

Distributed DOS, 19, 19

Distributed Reflective DOS,

19–20, 20

on e-mail, 51

fraggle, 19

land, 21

ping flood, 21

ping of death, 21

smurf, 19, 20

SYN flood, 20, 20

teardrop, 20, 20

dual-homed firewalls, 76, 77

due care, 164

DVD-R disks, 88

E

802.11/11x wireless networks, 40,
40–41, 65

e-mail security, *See also* communication

using digital signatures, 50–51, 51

exam essentials on, 53–54

using filters, 52

hardening e-mail servers,

108–109, 108

overview, 48, 49

using PGP encryption, 50

using S/MIME encryption, 49–50, 50

vulnerabilities

corrupted MIME headers, 51

hoaxes, 52–53

open relays, 59

overview, 51

SMTP relays, 58–59

spam, 52

spoofed e-mail, 52

education on security, 174

EF (Exposure Factor) formula, 172

EMI (electromagnetic interference), 85,

86, 154, 154

employee termination policy, 165

encapsulation, 42

end-user computers, 81

environment hardening, *See also*

infrastructure

application hardening

data repository servers, 110

database servers, 111

defined, 16, 107

DHCP servers, 110

directory services, 110, 111

DNS servers, 109

e-mail servers, 108–109, 108

file servers, 109–110, 110

FTP servers, 109

NNTP servers, 109

print servers, 110

using updates, 107

web servers, 108

defined, 16

documenting, 103

exam essentials, 111–112

network hardening

using access control lists, 107

- configuration issues, 106–107
- defined, 106
- enabling/disabling services, 107
- using updates, 106
- OS/NOS hardening
 - defined, 103–104
 - file systems, 104–105
 - using updates, 105
- overview, 103
- security baselines and, 103
- escrow, key, 138–139, 139, 140
- ESP (Encapsulating Security Payload)
 - protocol, 45
- evidence. *See* forensics
- extranets, 90, 91

F

- false positives, 95
- FAT (File Allocation Table), 105
- fault tolerance, 160–161
- fiber optic cable, 87, 87
- file server hardening, 109–110, 110
- file system hardening, 104–105
- File Transfer Protocol. *See* FTP
- filters, *See also* firewalls
 - defined, 74
 - e-mail filters, 52
 - ingress filters, 78
- fire suppression, 154–155
- firewalls, 74–77, 75, 77, 95, 96
- firmware, 106
- flashcards, 88
- floppies, 88
- forensics, *See also* operational
 - chain of custody, 170
 - collection of evidence, 171
 - defined, 170

- evidence preservation, 170–171
- exam essentials, 171
- fraggle attacks, 19
- FTP (File Transfer Protocol), *See also*
 - communication
 - anonymous FTP, 62–63
 - blind FTP, 63
 - defined, 62
 - exam essentials, 63–64
 - file sharing, 63
 - FTP servers, 109
 - overview, 61–62
 - Secure FTP, 62
 - vulnerabilities, 63
- full backups, 156

G

- guidelines, 175

H

- hard drives, 88
- hardening. *See* environment
- hashing, *See also* cryptography
 - attacks on, 120–121
 - defined, 26, 119–120, 120
 - digital signatures and, 50–51, 51
- hierarchical trusts, 132, 133
- high availability, 160–161
- hiring policy, 165
- hoax e-mail, 52–53
- honey pots, 100–101, 101
- host-based IDSs, 97, 97
- hot sites, 157, 158
- hotfixes, 105
- HR (human resources) policy, 165–166

HTML (Hypertext Markup Language),
54–55, 55

HTTP (Hypertext Transfer Protocol),
54–55, 55, 56

HTTPS (HTTP over SSL) protocol, 56

I

IDSs (Intrusion Detection Systems),
See also infrastructure

active detection/response, 98, 99–100

anomaly detection, 97, 98

defined, 81, 95, 96

exam essentials, 102

false positives, 95

honey pots, 100–101, 101

host-based IDSs, 97, 97

incident response, 101–102

network-based IDSs, 96, 96

passive detection/response, 98

signature detection, 97, 98

IEEE 802.11/11x wireless networks,
40, 40–41, 65

IKE (Internet Key Exchange), 46

IM (instant messaging), 56–57

IMAP (Internet Message Access
Protocol), 48

incident response policy, 166

incremental backups, 157

infrastructure mode, 66

infrastructure security, 74–115,

See also Security+

environment hardening, *See also*
environment

application hardening, 107–111,
108, 110–111

documenting, 103

exam essentials, 111–112

network hardening, 106–107

OS/NOS hardening, 103–105

overview, 103

security baselines and, 103

using updates, 105, 106, 107

Intrusion Detection Systems

active detection/response,
98, 99–100

anomaly detection, 97, 98

containment, 102

defined, 81, 95, 96

exam essentials, 102

false positives, 95

honey pots, 100–101, 101

host-based IDSs, 97, 97

incident response, 101–102

network-based IDSs, 96, 96

passive detection/response, 98

signature detection, 97, 98

media security

CDs/DVDs, 88

coaxial cable, 83, 83–85

exam essentials, 88–89

fiber optic cable, 87, 87

flashcards, 88

floppies/diskettes, 88

hard drives, 88

overview, 82

removable media, 87–88

shielded cabling, 85–86, 85–86,
154, 154

smartcards, 88

tape drives, 87

unshielded cabling, 85–86, 85–86

review question answers, 115

review questions, 113–114

security devices, *See also* IDSs

exam essentials on, 82

firewalls, 74–77, 75, 77, 95, 96

Intrusion Detection Systems, 81,
95–102, 96–101

- mobile devices, 82
- modems, 79, 79
- for monitoring/diagnostics, 81
- Remote Access Server, 80
- routers, 77–78, 77–78
- servers, 81
- switches, 78, 78
- Telecom/PBX systems, 80, 80
- virtual private networks and, 81
- wireless security, 79
- workstations, 81
- security topologies
 - defined, 89
 - demilitarized zones, 90, 90
 - exam essentials on, 94–95
 - extranets, 90, 91
 - intranets, 90, 91
 - IP address translation and, 93–94, 93
 - RFC 1918 and, 93–94
 - security zones, 89–90, 89–91
 - tunneling and, 94
 - virtual LANs, 91–92, 92
- ingress filters, 78
- instant messaging (IM), 56–57
- integrity, data, 125–127, 127
- Internet Key Exchange (IKE), 46
- Internet Message Access Protocol (IMAP), 48
- Internet security, *See also*
 - communication
 - exam essentials on, 59–60
 - using HTTPS protocol, 56
 - overview, 54–55, 55
 - using S-HTTP protocol, 56
 - using SSL encryption, 55–56
 - using TLS encryption, 55, 56
 - vulnerabilities
 - ActiveX, 57
 - buffer overflows, 57–58

- Common Gateway Interface, 58
- cookies, 58
- HTTP protocol, 54–55, 55, 56
- instant messaging, 56–57
- JavaScript, 57
- signed applets, 58
- SMTP relay, 58–59
- intranets, 90, 91
- IP address translation, 93, 93–94
- IPSec (Internet Protocol Security)
 - protocols, 44–46, 45–46
- ISAKMP (Internet Security Association and Key Management Protocol), 46

J

- JavaScript vulnerability, 57

K

- KDC (Key Distribution Center), 8, 9
- Kerberos authentication, 7–9, 9
- keys. *See* cryptography; PKI

L

- L2TP (Layer 2 Tunneling Protocol), 44
- land attacks, 21
- LDAP (Lightweight Directory Access Protocol), 61, 61, 111
- logging. *See* auditing
- logic bombs, 30

M

- M of N (key) control, 140
- MAC (Mandatory Access Control), 4–5, 6, 164, 168, 169

MAC (message authentication code)

values, 119, 120

macro viruses, 29

maintenance hooks, 21

malicious code, *See also* attack;

Security+

defined, 29

exam essentials on, 30

logic bombs, 30

Trojan horses, 30

viruses, 29

worms, 30

man-in-the-middle attacks, 23, 23

mantraps, 152, 152

mathematical attacks, 25

MD (Message Digest) algorithms,

120, 121

media security, *See also* infrastructure

CDs/DVDs, 88

coaxial cable, 83, 83–85

exam essentials on, 88–89

fiber optic cable, 87, 87

flashcards, 88

floppies/diskettes, 88

hard drives, 88

overview, 82

removable media, 87–88

shielded cabling, 85–86, 85–86,

154, 154

smartcards, 88

tape drives, 87

unshielded cabling, 85–86, 85–86

MIME headers, corrupted, 51, *See also*

S/MIME

mitigation of risk, 172

mobile devices, 82

modems, 79, 79

monitoring. *See* auditing

multi-homed firewalls, 76, 90, 90

N

NAT (Network Address Translation),

93, 93–94

need to know, 5, 164

network hardening, 106–107

network-based IDSs, 96, 96

NNTP (Network News Transfer

Protocol) servers, 109

nonrepudiation, 50, 126, 128

NOS (network operating system)

hardening, 103–105

notification documents, 176

NTFS (New Technology File

System), 105

O

objects, 4–5, 8

OCSP (Online Certificate Status

Protocol), 132

100BaseT cable, 86

1000BaseT cable, 86

operational/organizational security,

150–180, *See also* Security+

business continuity

backups, 161

defined, 159

elements in planning, 159–160

exam essentials, 162

high availability/fault tolerance,

160–161

utilities, 160

disaster recovery

alternate sites, 157–158

backups, 156–157

exam essentials, 158–159

offsite storage, 157

overview, 156

- plans, 158
- secure recovery, 157
- forensics
 - chain of custody, 170
 - collection of evidence, 171
 - defined, 170
 - evidence preservation, 170–171
 - exam essentials, 171
- overview, 150
- physical security
 - access control, 150–153, 152
 - barriers, 151–152, 152
 - EMI/RFI shielding, 154, 154
 - environment factors, 153–155
 - exam essentials, 155–156
 - facility location, 154
 - fire suppression, 154–155
 - mantraps, 152, 152
 - overview, 150
 - security guards, 152
 - social engineering attacks, 153
 - wireless cells, 153
- privilege management
 - auditing, 169
 - centralized management, 168
 - decentralized management, 168
 - exam essentials, 169–170
 - MAC/DAC/RBAC access
 - control, 169
 - overview, 167–168
 - principle of least privilege, 168
 - privilege, defined, 168
 - privilege escalation, 169
 - single sign-on, 168
 - user/group/role management, 168
- review question answers, 180
- review questions, 178–179
- risk identification
 - asset identification, 172
 - exam essentials, 173
 - minimizing risk impact, 172
 - overview, 171–172
 - risk assessment formulas, 172
 - threat identification, 172
 - vulnerability management, 172
- security documentation
 - asset inventories, 176
 - change documentation, 176
 - classification labeling, 4, 176
 - destruction of, 177
 - environment hardening, 103
 - exam essentials, 177
 - guidelines, 175
 - incident responses, 166
 - logs/audit trails, 32–33, 176
 - notification documents, 176
 - overview, 175
 - retention/storage of, 176
 - standards, 175
 - systems architecture, 175
- security policy
 - acceptable use, 163
 - account lockout, 164
 - code of ethics, 165–166
 - defined, 163
 - disposal/destruction, 165
 - due care, 164
 - employee termination, 165
 - exam essentials, 166–167
 - hiring, 165
 - human resources, 165–166
 - incident response, 166
 - need to know, 164
 - password management, 164
 - separation of duties, 164
 - service level agreements, 165
 - user privacy, 164
- security training
 - communication, 174
 - education, 174

- exam essentials, 174–175
- on-line resources, 174
- overview, 173
- user awareness, 174
- Orange Book specifications, 5
- OS (operating system) hardening, 103–105

P

- packet filter firewalls, 76
- packet sequencing, 24
- packet sniffing attacks, 56–57, 63, 78
- PAP (Password Authentication Protocol), 9
- passive detection and response, 98
- passwords
 - cracking attacks, 12, 26–27, 120–121
 - defined, 12, 12
 - history, 164
 - management policy, 164
 - one-time passwords, 13
 - strong passwords, 12, 26
 - weak passwords, 12
- PAT (Port Address Translation), 94
- patches, 105
- PBX (Private Branch Exchange) systems, 80, 80
- penetration testing, 33
- PGP (Pretty Good Privacy), 50–51, 51
- physical security, *See also* operational
 - access controls
 - barriers, 151–152, 152
 - biometrics, 14–15, 152
 - mantraps, 152, 152
 - overview, 150–151
 - security guards, 152
 - environment factors
 - EMI/RFI shielding, 154, 154
 - facility location, 154
 - fire suppression, 154–155
 - overview, 153
 - wireless cells, 153
- exam essentials, 155–156
- overview, 150
- social engineering attacks, 153
- piggybacking, 152
- ping flood/ping of death attacks, 21
- PKI (Public Key Infrastructure), *See also* cryptography
 - certificate authorities, 129–131, 130
 - certificate policies, 131
 - certificate practice statements, 131
 - certificate revocation, 131–132, 132
 - defined, 10–11, 11, 122, 129
 - exam essentials, 134–135
 - trust models, 132–134, 133
 - trusted third parties, 10, 129
 - X.509 certificates, 129, 130
- policy. *See* security policy
- polymorphic viruses, 29
- POP (Post Office Protocol), 48
- PPTP (Point-to-Point Tunneling Protocol), 44
- principle of least privilege, 5, 6, 168
- print server hardening, 110
- printed data, disposal of, 165
- privacy policy, 164
- Private Branch Exchange (PBX) systems, 80, 80
- private IP addresses, 93–94
- private keys. *See* cryptography; symmetric encryption
- privilege management, *See also* operational
 - auditing, 169
 - centralized management, 168
 - decentralized management, 168

- exam essentials, 169–170
- MAC/DAC/RBAC access control, 169
- overview, 167–168
- principle of least privilege, 5, 6, 168
- privilege, defined, 168
- privilege escalation, 169
- single sign-on, 168
- user/group/role management, 168
- proxies, 76
- public keys. *See* asymmetric encryption; cryptography

R

- radio frequency disturbance, 154
- RADIUS (Remote Access Dial-In User Service), 42–43, 43
- RAID (Redundant Array of Independent Disks), 160, 161
- RAs (registration authorities), 131
- RAS (Remote Access Server), 43, 43, 80
- RBAC (Role-Based Access Control), 6, 7, 168, 169
- RBAC (Rule-Based Access Control), 6
- realms, 8
- recovering keys from escrow, 140
- recovery. *See* disaster recovery
- remote access security, *See also* communication
 - in 802.11/11x wireless, 40–41, 40, 65
 - exam essentials, 47–48
 - in IPSec protocols, 44–46, 45–46
 - in L2TP protocol, 44
 - overview, 39–40, 39
 - in PPTP protocol, 44
 - using RADIUS, 42–43, 43
 - using Secure Shell, 44
 - using TACACS, 43, 43

- in virtual private networks, 41–42, 41
- vulnerabilities, 46–47
- remote calling, 80
- removable media, 87–88
- replay attacks, 24, 24
- reverse hash matching, 26, 120
- revocation, certificate, 131–132, 132, 139
- RFC 1918, 93–94
- risk identification, *See also* operational; vulnerabilities
 - asset identification, 172
 - exam essentials, 173
 - minimizing risk impact, 172
 - overview, 171–172
 - risk assessment formulas, 172
 - threat identification, 172
 - vulnerability management, 172
- routers, 76, 77–78, 77–78

S

- S-HTTP (Secure-HTTP), 56
- S/FTP (Secure FTP), 62
- S/MIME (Secure Multipurpose Internet Mail Extensions), 49–50, 50
- secret (private) keys. *See* cryptography; symmetric encryption
- Security+ exam objectives, *See also* communication; cryptography; infrastructure; operational
 - access control models
 - defined, 3
 - Discretionary Access Control, 5–6
 - exam essentials on, 6–7
 - Mandatory Access Control, 4–5
 - overview, 3–4, 168, 169
 - Role-Based Access Control, 6

- attack methods, *See also* attack
 - back door, 21–22, 22
 - birthday, 26, 120
 - buffer overflow, 27, 57–58
 - Denial of Service, 18–21, 19–20
 - exam essentials on, 28–29
 - man-in-the-middle, 23, 23
 - mathematical, 25
 - overview, 18
 - password cracking, 12, 26–27, 120–121
 - replay, 24, 24
 - social engineering, 31–32, 52–53
 - software exploitation, 27
 - spoofing, 22–23, 52
 - TCP/IP hijacking, 24, 25
 - weak keys and, 25
- auditing, 32–33
- authentication methods, *See also* authentication; certificates
 - biometrics, 14–15, 152
 - certificates, 10–11, 11
 - CHAP, 9–10, 10
 - defined, 7
 - exam essentials on, 15
 - Kerberos, 7–9, 9
 - multi-factor authentication, 13–14, 14
 - mutual authentication, 14
 - tokens, 13, 13
 - usernames/passwords, 12, 12
- malicious code
 - defined, 29
 - exam essentials on, 30
 - logic bombs, 30
 - Trojan horses, 30
 - viruses, 29
 - worms, 30
- non-essential services, 15–17
- review question answers, 36
- review questions, 34–35
- security associations, 46
- security baselines, 103
- security devices, *See also* infrastructure
 - exam essentials on, 82
 - firewalls, 74–77, 75, 77, 95, 96
 - Intrusion Detection Systems, 81, 95–102, 96–101
 - mobile devices, 82
 - modems, 79, 79
 - for monitoring/diagnostics, 81
 - Remote Access Server, 80
 - routers, 77–78, 77–78
 - servers, 81
 - switches, 78, 78
 - Telecom/PBX systems, 80, 80
 - virtual private networks and, 81
 - wireless networks, 79
 - workstations, 81
- security documentation, *See also* operational
 - asset inventories, 176
 - change documentation, 176
 - classification labeling, 4, 176
 - destruction of, 177
 - environment hardening, 103
 - exam essentials, 177
 - guidelines, 175
 - incident responses, 166
 - logs or audit trails, 176
 - notification documents, 176
 - overview, 175
 - retention/storage of, 176
 - standards, 175
 - systems architecture, 175
- security domains, 4–5
- security guards, 152
- security policy, *See also* operational
 - acceptable use, 163
 - account lockout, 164

- certificates, 131
- code of ethics, 165–166
- defined, 163
- disposal/destruction, 165
- due care, 164
- employee termination, 165
- exam essentials, 166–167
- firewalls, 76
- hiring, 165
- human resources, 165–166
- incident response, 166
- need to know, 164
- password management, 164
- separation of duties, 164
- service level agreements, 165
- user privacy, 164
- security topologies, *See also*
 - infrastructure
 - defined, 89
 - demilitarized zones, 90, 90
 - exam essentials on, 94–95
 - extranets, 90, 91
 - intranets, 90, 91
 - IP address translation and, 93–94, 93
 - RFC 1918 and, 93–94
 - security zones, 89–90, 89–91
 - tunneling and, 94
 - virtual LANs, 91–92, 92
- security training, *See also* operational
 - communication, 174
 - education, 174
 - exam essentials, 174–175
 - on-line resources, 174
 - overview, 173
 - user awareness, 174
- sensitivity labels, 4–5
- separation of duties policy, 164
- server clustering, 160, 162
- server rooms, mission-critical, 151, 151, 154
- servers, 81
- service level agreements (SLAs), 165
- service packs, 105
- services, non-essential, 15–17
- shielding, 85–86, 85–86, 154, 154
- signature detection in IDSs, 97, 98
- signatures, digital. *See* digital
- single points of failure, 160
- single sign-on, 8, 168
- site surveys, 66
- SLE (Single Loss Expectancy)
 - formula, 172
- smartcards, 13, 13–14, 88
- SMTP relay, 58–59
- SMTP (Simple Mail Transport Protocol), 48, 49
- smurf attacks, 19, 20
- sniffing attacks, packet, 56–57, 63, 78
- SNMP (Simple Network Management Protocol), 81
- social engineering attacks, 31–32, 52–53, 153
- software exploitation attacks, 27
- spam, 52
- spoofing attacks, 22–23, 52
- SSH (Secure Shell), 44
- SSL (Secure Sockets Layer), 55–56
- standards, 175
- stateful inspection firewalls, 76
- storage
 - encryption keys, 138–139, 139, 140
 - media, disposal of, 165
 - media, storing offsite, 157
 - security documentation, 176
- STP (shielded twisted pair) cable, 85–86, 85–86, 154
- stream cipher cryptography, 122
- strong authentication, 14

strong passwords, 12, 26
 STs (Service Tickets), 8, 9
 subjects, 4–5, 8
 switches, 78, 78
 symmetric encryption, 46, 121–122,
 126–127, 127
 SYN flood attacks, 20, 20
 system hardening, 16
 system scanning, 33
 systems architecture documentation, 175

T

T-connectors, 84
 TACACS (Terminal Access Controller
 Access Control System), 43, 43
 tape drives, 87
 TCP SYN flood attacks, 20, 20
 TCP/IP hijacking attacks, 24, 25
 TCSEC (Trusted Computer System Eval-
 uation Criteria), 5
 teardrop attacks, 20
 Telecom/PBX systems, 80, 80
 Telnet, 44
 10Base2/Thinnet cable, 83
 10Base5/Thicknet cable, 83
 10BaseT cable, 85, 86
 terminals, 81
 termination, coax cable, 83, 85
 TGTs (Ticket Granting Tickets), 8, 9
 threats, 172, *See also* attack; risk;
 vulnerabilities
 timestamps, packet, 24
 TLS (Transport Layer Security), 55, 56
 tokens, 13, 13
 training. *See* security training
 transport mode in IPSec, 45, 46
 Trojan horses, 30

trust models, 132–134, 133
 trusted third parties, 10, 129
 tunneling protocols, 42, 94, *See also*
 IPSec; L2TP; PPTP

U

updating
 applications, 107
 networks, 106
 OSs/NOSs, 105
 user awareness of security, 174
 user privacy policy, 164
 username/password authentication,
 12, 12
 utilities, physical, 160
 UTP (unshielded twisted pair) cable,
 85–86, 85–86

V

valid from/valid to dates, 139
 vampire taps, 83, 84
 viruses, 29
 VLANs (virtual local area networks), 78,
 91–92, 92
 VPN protocols, 42, 94, *See also* IPSec;
 L2TP; PPTP
 VPNs (virtual private networks), 41,
 41–42, 81
 vulnerabilities, *See also* attack; risk;
 threats
 in cryptography
 hashing, 26, 120–121
 key recovery, 140
 key storage, 137, 138
 weak keys, 25
 defined, 172

- in e-mail security
 - hoaxes, 52–53
 - MIME headers, 51
 - open relays, 59
 - overview, 51
 - SMTP relays, 58–59
 - spam, 52
 - spoofed e-mail, 52
- in File Transfer Protocol, 63
- in Internet security
 - ActiveX, 57
 - buffer overflows, 57–58
 - Common Gateway Interface, 58
 - cookies, 58
 - HTTP protocol, 54–55, 55, 56
 - instant messaging, 56–57
 - JavaScript, 57
 - signed applets, 58
 - SMTP relay, 58–59
- in physical security
 - EMI disturbance, 85, 86, 154, 154
 - fire, 154
 - radio frequency disturbance, 154
 - social engineering, 153
 - wireless cells, 153
- privilege escalation, 169
- in remote access, 46–47
- in wireless networks, 66
- vulnerability scanning, 33

W

WAP (Wireless Application Protocol),
64–65, 65

- war dialing attacks, 79
- warm sites, 157
- weak keys, 25
- web server hardening, 108
- wireless security, *See also*
 - communication
 - in 802.11/11x networks, 40–41,
40, 65
 - exam essentials on, 66–67
 - overview, 64, 79
 - site surveys, 66
 - vulnerabilities, 66
 - using Wired Equivalent
Privacy, 65
 - wireless cells, 153
 - using WTLS in WAP protocol,
64–65, 65
- workstations, 81
- worms, 30
- WTLS (Wireless Transport Layer
Security), 64

X

x.500 standard, 61
X.509 certificates, 129, 130

Z

Zimmerman, Phillip R., 50
zombies, 18–19, 19
zone transfers, 109