

# CONTENTS AT A GLANCE

Chapter 1	■ <b>Introduction and Security Trends</b>	I
Chapter 2	■ <b>General Security Concepts</b>	20
Chapter 3	■ <b>Operational and Organizational Security</b>	50
Chapter 4	■ <b>The Role of People in Security</b>	66
Chapter 5	■ <b>Cryptography</b>	82
Chapter 6	■ <b>Public Key Infrastructure</b>	114
Chapter 7	■ <b>Standards and Protocols</b>	152
Chapter 8	■ <b>Physical Security</b>	178
Chapter 9	■ <b>Network Fundamentals</b>	204
Chapter 10	■ <b>Infrastructure Security</b>	228
Chapter 11	■ <b>Authentication and Remote Access</b>	260
Chapter 12	■ <b>Wireless Security</b>	294
Chapter 13	■ <b>Intrusion Detection Systems and Network Security</b>	318
Chapter 14	■ <b>Baselines</b>	358

Chapter 15 ■ **Types of Attacks and Malicious Software** 388

Chapter 16 ■ **E-Mail and Instant Messaging** 420

Chapter 17 ■ **Web Components** 444

Chapter 18 ■ **Secure Software Development** 474

Chapter 19 ■ **Disaster Recovery, Business Continuity, and  
Organizational Policies** 492

Chapter 20 ■ **Risk Management** 524

Chapter 21 ■ **Change Management** 544

Chapter 22 ■ **Privilege Management** 560

Chapter 23 ■ **Computer Forensics** 580

Chapter 24 ■ **Legal Issues and Ethics** 596

Chapter 25 ■ **Privacy** 618

Appendix A ■ **Objectives Map: CompTIA Security+** 640

Appendix B ■ **About the CD** 648

■ **Glossary** 650

■ **Index** 664

# CONTENTS

Preface. . . . .	xxi
Introduction . . . . .	xxiii
CompTIA Authorized Quality Curriculum. . . . .	xxvi
Instructor and Student Web Site . . . . .	xxvii

## Chapter 1

### ■ Introduction and Security Trends 1

The Security Problem . . . . .	1
<i>Security Incidents</i> . . . . .	1
<i>Threats to Security</i> . . . . .	7
<i>Security Trends</i> . . . . .	10
Avenues of Attack . . . . .	11
<i>The Steps in an Attack</i> . . . . .	12
<i>Minimizing Possible Avenues of Attack</i> . . . . .	13
<i>Types of Attacks</i> . . . . .	14
Chapter 1 Review . . . . .	15

## Chapter 2

### ■ General Security Concepts 20

Basic Security Terminology . . . . .	21
<i>Security Basics</i> . . . . .	21
<i>Access Control</i> . . . . .	31
<i>Authentication</i> . . . . .	31
<i>Authentication and Access</i>	
<i>Control Policies</i> . . . . .	32
Social Engineering . . . . .	33
Security Policies . . . . .	34
<i>Change Management Policy</i> . . . . .	35
<i>Classification of Information</i> . . . . .	36
<i>Acceptable Use Policy</i> . . . . .	36
<i>Due Care and Due Diligence</i> . . . . .	38
<i>Due Process</i> . . . . .	38
<i>Need to Know</i> . . . . .	39
<i>Disposal and Destruction Policy</i> . . . . .	39
<i>Service Level Agreements</i> . . . . .	40
<i>Human Resources Policies</i> . . . . .	40
Security Models . . . . .	42
<i>Confidentiality Models</i> . . . . .	42
<i>Integrity Models</i> . . . . .	43
Chapter 2 Review . . . . .	46

## Chapter 3

### ■ Operational and Organizational Security 50

Security Operations in Your Organization . . . . .	51
<i>Policies, Procedures, Standards,</i>	
<i>and Guidelines</i> . . . . .	51
<i>The Security Perimeter</i> . . . . .	52
Physical Security . . . . .	53
<i>Access Controls</i> . . . . .	54
<i>Physical Barriers</i> . . . . .	56
Environmental Issues . . . . .	56
<i>Fire Suppression</i> . . . . .	57
Wireless . . . . .	58
Electromagnetic Eavesdropping . . . . .	59
Location . . . . .	60
Chapter 3 Review . . . . .	62

## Chapter 4

### ■ The Role of People in Security 66

People—A Security Problem . . . . .	67
<i>Social Engineering</i> . . . . .	67
<i>Poor Security Practices</i> . . . . .	71
People as a Security Tool . . . . .	76
<i>Security Awareness</i> . . . . .	76
<i>Individual User Responsibilities</i> . . . . .	77
Chapter 4 Review . . . . .	78

## Chapter 5

### ■ Cryptography 82

Algorithms . . . . .	84
Hashing Functions . . . . .	87
<i>SHA</i> . . . . .	88
<i>Message Digest</i> . . . . .	90
<i>Hashing Summary</i> . . . . .	91
Symmetric Encryption . . . . .	91
<i>DES</i> . . . . .	92
<i>3DES</i> . . . . .	93
<i>AES</i> . . . . .	94
<i>CAST</i> . . . . .	95

RC	95	Certificate-Based Threats	145
Blowfish	97	Chapter 6 Review	147
IDEA	97		
Symmetric Encryption Summary	97		
Asymmetric Encryption	98	<b>Chapter 7</b>	
RSA	98	■ <b>Standards and Protocols 152</b>	
Diffie-Hellman	99	PKIX and PKCS	154
ElGamal	100	PKIX Standards	155
ECC	100	PKCS	156
Asymmetric Encryption Summary	101	Why You Need to Know the PKIX	
Steganography	101	and PKCS Standards	158
Cryptography Algorithm Use	103	X.509	160
Confidentiality	104	SSL/TLS	161
Integrity	104	ISAKMP	162
Nonrepudiation	104	CMP	163
Authentication	105	XKMS	164
Key Escrow	105	S/MIME	166
Digital Signatures	106	IETF S/MIME History	166
Digital Rights Management	107	IETF S/MIME v3 Specifications	167
Cryptographic Applications	108	PGP	168
Chapter 5 Review	110	How PGP Works	168
		HTTPS	169
<b>Chapter 6</b>		IPsec	170
■ <b>Public Key Infrastructure 114</b>		CEP	170
The Basics of Public Key Infrastructures	115	FIPS	170
Certificate Authorities	117	Common Criteria for Information Technology	
Registration Authorities	118	Security (Common Criteria or CC)	171
Local Registration Authorities	120	WTLS	171
Certificate Repositories	120	PPTP	172
Trust and Certificate Verification	121	WEP	172
Digital Certificates	124	WEP Security Issues	172
Certificate Attributes	125	ISO/IEC 27002 (Formerly ISO 17799)	173
Certificate Extensions	126	Chapter 7 Review	174
Certificate Lifecycles	127		
Centralized and Decentralized		<b>Chapter 8</b>	
Infrastructures	132	■ <b>Physical Security 178</b>	
Hardware Storage Devices	133	The Security Problem	179
Private Key Protection	134	Physical Security Safeguards	183
Key Recovery	135	Walls and Guards	183
Key Escrow	136	Policies and Procedures	184
Public Certificate Authorities	137	Access Controls and Monitoring	188
In-House Certificate Authorities	138	Environmental Controls	191
Choosing Between a Public CA		Fire Suppression	191
and an In-House CA	138	Authentication	195
Outsourced Certificate Authorities	139	Chapter 8 Review	200
Tying Different PKIs Together	140		
Trust Models	140		

## Chapter 9

### ■ Network Fundamentals 204

Network Architectures	205
Network Topology	206
Network Protocols	207
Packets	209
TCP vs. UDP	210
ICMP	211
Packet Delivery	213
Local Packet Delivery	213
Remote Packet Delivery	214
IP Addresses and Subnetting	215
Network Address Translation	217
Security Zones	218
VLANs	222
Tunneling	223
Chapter 9 Review	224

## Chapter 10

### ■ Infrastructure Security 228

Devices	229
Workstations	229
Servers	231
Virtualization	232
Network Interface Cards	232
Hubs	233
Bridges	233
Switches	234
Routers	235
Firewalls	236
Wireless	238
Modems	239
Telecom/PBX	240
VPN	241
Intrusion Detection Systems	241
Network Access Control	242
Network Monitoring/Diagnostic	242
Mobile Devices	244
Device Security, Common Concerns	244
Media	245
Coaxial Cable	245
UTP/STP	245
Fiber	247
Unguided Media	248
Security Concerns for Transmission Media	249
Physical Security Concerns	249
Removable Media	250
Magnetic Media	251
Optical Media	253

Electronic Media	254
Network Attached Storage	255
Chapter 10 Review	256

## Chapter 11

### ■ Authentication and Remote Access 260

The Remote Access Process	261
Identification	262
Authentication	262
Authorization	267
Access Control	268
IEEE 802.1X	270
Wireless Protocols	271
RADIUS	271
RADIUS Authentication	272
RADIUS Authorization	273
RADIUS Accounting	273
Diameter	274
TACACS+	274
TACACS+ Authentication	275
TACACS+ Authorization	276
TACACS+ Accounting	276
Authentication Protocols	277
L2TP and PPTP	277
PPP	277
PPTP	278
EAP	279
CHAP	279
NTLM	280
PAP	280
L2TP	280
Telnet	281
SSH	281
VPNs	283
IPsec	284
Security Associations	284
IPsec Configurations	285
IPsec Security	286
Vulnerabilities of Remote Access Methods	288
Connection Summary	289
Chapter 11 Review	290

## Chapter 12

### ■ Wireless Security 294

Introduction to Wireless Networking	295
Mobile Phones	296
WAP	298
3G Mobile Networks	300

Bluetooth . . . . .	300
802.11 . . . . .	302
802.11: Individual Standards . . . . .	304
Attacking 802.11 . . . . .	306
New Security Protocols . . . . .	310
Implementing 802.1X . . . . .	311
Chapter 12 Review . . . . .	314

## Chapter 13

### ■ Intrusion Detection Systems and Network Security 318

History of Intrusion	
Detection Systems . . . . .	319
IDS Overview . . . . .	320
Network-Based IDSs . . . . .	322
Advantages of a NIDS . . . . .	326
Disadvantages of a NIDS . . . . .	326
Active vs. Passive NIDSs . . . . .	326
Signatures . . . . .	327
False Positives and False Negatives . . . . .	328
IDS Models . . . . .	329
Firewalls . . . . .	329
How Do Firewalls Work? . . . . .	331
Intrusion Prevention Systems . . . . .	333
Proxy Servers . . . . .	334
Internet Content Filters . . . . .	336
Protocol Analyzers . . . . .	336
Honeypots and Honeynets . . . . .	338
Host-Based IDSs . . . . .	340
Advantages of HIDSs . . . . .	343
Disadvantages of HIDSs . . . . .	344
Active vs. Passive HIDSs . . . . .	345
Resurgence and Advancement of HIDSs . . . . .	345
PC-Based Malware Protection . . . . .	346
Antivirus Products . . . . .	346
Personal Software Firewalls . . . . .	349
Pop-up Blockers . . . . .	350
Windows Defender . . . . .	351
Antispam . . . . .	353
Chapter 13 Review . . . . .	354

## Chapter 14

### ■ Baselines 358

Overview of Baselines . . . . .	359
Password Selection . . . . .	359

Operating System and Network	
Operating System Hardening . . . . .	360
Hardening Microsoft Operating Systems . . . . .	361
Hardening UNIX- or Linux-Based	
Operating Systems . . . . .	364
Updates (a.k.a. Hotfixes,	
Service Packs, and Patches) . . . . .	373
Network Hardening . . . . .	375
Software Updates . . . . .	376
Device Configuration . . . . .	376
Application Hardening . . . . .	377
Application Patches . . . . .	377
Patch Management . . . . .	378
Group Policies . . . . .	380
Security Templates . . . . .	382
Chapter 14 Review . . . . .	384

## Chapter 15

### ■ Types of Attacks and Malicious Software 388

Avenues of Attack . . . . .	389
The Steps in an Attack . . . . .	389
Minimizing Possible Avenues of Attack . . . . .	391
Attacking Computer Systems	
and Networks . . . . .	392
Denial-of-Service Attacks . . . . .	392
Backdoors and Trapdoors . . . . .	395
Null Sessions . . . . .	395
Sniffing . . . . .	396
Spoofing . . . . .	397
Man-in-the-Middle Attacks . . . . .	400
Replay Attacks . . . . .	400
TCP/IP Hijacking . . . . .	401
Drive-by Download Attacks . . . . .	401
Phishing and Pharming Attacks . . . . .	401
Attacks on Encryption . . . . .	402
Address System Attacks . . . . .	403
Password Guessing . . . . .	404
Software Exploitation . . . . .	405
Malicious Code . . . . .	406
Malware Defenses . . . . .	412
War-Dialing and War-Driving . . . . .	413
Social Engineering . . . . .	414
Auditing . . . . .	414
Chapter 15 Review . . . . .	416

## Chapter 16

### ■ E-Mail and Instant Messaging 420

Security of E-Mail . . . . .	421
Malicious Code . . . . .	423
Hoax E-Mails . . . . .	427
Unsolicited Commercial E-Mail (Spam) . . . . .	428
Mail Encryption . . . . .	431
S/MIME . . . . .	432
PGP . . . . .	433
Instant Messaging . . . . .	435
Chapter 16 Review . . . . .	440

## Chapter 17

### ■ Web Components 444

Current Web Components and Concerns . . . . .	445
Web Protocols . . . . .	445
Encryption (SSL and TLS) . . . . .	446
The Web (HTTP and HTTPS) . . . . .	452
Directory Services (DAP and LDAP) . . . . .	453
File Transfer (FTP and SFTP) . . . . .	454
Vulnerabilities . . . . .	455
Code-Based Vulnerabilities . . . . .	455
Buffer Overflows . . . . .	456
Java and JavaScript . . . . .	457
ActiveX . . . . .	459
Securing the Browser . . . . .	460
CGI . . . . .	461
Server-Side Scripts . . . . .	461
Cookies . . . . .	462
Signed Applets . . . . .	464
Browser Plug-ins . . . . .	465
Application-Based Weaknesses . . . . .	467
Open Vulnerability and Assessment Language (OVAL) . . . . .	468
Web 2.0 and Security . . . . .	468
Chapter 17 Review . . . . .	470

## Chapter 18

### ■ Secure Software Development 474

The Software Engineering Process . . . . .	475
Process Models . . . . .	475
Secure Development Lifecycle . . . . .	476
Threat Modeling Steps . . . . .	478
Chapter 18 Review . . . . .	488

## Chapter 19

### ■ Disaster Recovery, Business Continuity, and Organizational Policies 492

Disaster Recovery . . . . .	493
Disaster Recovery Plans/Process . . . . .	493
Backups . . . . .	495
Utilities . . . . .	502
Secure Recovery . . . . .	502
Cloud Computing . . . . .	503
High Availability and Fault Tolerance . . . . .	503
Computer Incident Response Teams . . . . .	505
Test, Exercise, and Rehearse . . . . .	505
Policies and Procedures . . . . .	506
Security Policies . . . . .	507
Privacy . . . . .	513
Service Level Agreements . . . . .	513
Human Resources Policies . . . . .	513
Code of Ethics . . . . .	515
Incident Response Policies and Procedures . . . . .	516
Chapter 19 Review . . . . .	520

## Chapter 20

### ■ Risk Management 524

An Overview of Risk Management . . . . .	525
Example of Risk Management at the International Banking Level . . . . .	525
Risk Management Vocabulary . . . . .	526
What Is Risk Management? . . . . .	527
Business Risks . . . . .	528
Examples of Business Risks . . . . .	528
Examples of Technology Risks . . . . .	529
Risk Management Models . . . . .	529
General Risk Management Model . . . . .	529
Software Engineering Institute Model . . . . .	532
Model Application . . . . .	533
Qualitatively Assessing Risk . . . . .	533
Quantitatively Assessing Risk . . . . .	535
Adding Objectivity to a Qualitative Assessment . . . . .	535
A Common Objective Approach . . . . .	536
Qualitative vs. Quantitative Risk Assessment . . . . .	537
Tools . . . . .	538
Chapter 20 Review . . . . .	539

## Chapter 21

### ■ Change Management 544

Why Change Management?	545
The Key Concept: Separation of Duties	547
Elements of Change Management	548
Implementing Change Management	550
<i>The Purpose of a Change Control Board</i>	551
<i>Code Integrity</i>	553
The Capability Maturity Model Integration	553
Chapter 21 Review	555

## Chapter 22

### ■ Privilege Management 560

User, Group, and Role Management	561
<i>User</i>	561
<i>Group</i>	563
<i>Role</i>	564
Password Policies	564
<i>Domain Password Policy</i>	565
Single Sign-On	567
<i>Time of Day Restrictions</i>	568
<i>Tokens</i>	568
<i>Account and Password Expiration</i>	569
Security Controls and Permissions	570
<i>Access Control Lists</i>	571
Handling Access Control	
(MAC, DAC, and RBAC)	573
<i>Mandatory Access Control (MAC)</i>	573
<i>Discretionary Access Control (DAC)</i>	574
<i>Role-Based Access Control (RBAC)</i>	575
<i>Rule-Based Access Control (RBAC)</i>	575
Chapter 22 Review	576

## Chapter 23

### ■ Computer Forensics 580

Evidence	582
<i>Standards for Evidence</i>	582
<i>Types of Evidence</i>	582
<i>Three Rules Regarding Evidence</i>	583
Collecting Evidence	583
<i>Acquiring Evidence</i>	583
<i>Identifying Evidence</i>	585
<i>Protecting Evidence</i>	585
<i>Transporting Evidence</i>	586
<i>Storing Evidence</i>	586
<i>Conducting the Investigation</i>	586
Chain of Custody	587
Free Space vs. Slack Space	588
<i>Free Space</i>	588
<i>Slack Space</i>	588

Message Digest and Hash	588
Analysis	589
Chapter 23 Review	591

## Chapter 24

### ■ Legal Issues and Ethics 596

Cybercrime	597
<i>Common Internet Crime Schemes</i>	599
<i>Sources of Laws</i>	600
<i>Computer Trespass</i>	600
<i>Significant U.S. Laws</i>	601
<i>Payment Card Industry Data</i>	
<i>Security Standard (PCI DSS)</i>	604
<i>Import/Export Encryption Restrictions</i>	605
<i>Non-U.S. Laws</i>	607
<i>Digital Signature Laws</i>	607
<i>Digital Rights Management</i>	609
Ethics	611
<i>SANS Institute IT Code of Ethics<sup>1</sup></i>	612
Chapter 24 Review	614
<i>Essay Quiz</i>	617

## Chapter 25

### ■ Privacy 618

Personally Identifiable	
Information (PII)	619
<i>Sensitive PII</i>	620
<i>Notice, Choice, and Consent</i>	620
U.S. Privacy Laws	620
<i>Privacy Act of 1974</i>	621
<i>Freedom of Information Act (FOIA)</i>	621
<i>Family Education Records</i>	
<i>and Privacy Act (FERPA)</i>	622
<i>U.S. Computer Fraud and Abuse</i>	
<i>Act (CFAA)</i>	622
<i>U.S. Children's Online Privacy</i>	
<i>Protection Act (COPPA)</i>	623
<i>Video Privacy Protection Act (VPPA)</i>	623
<i>Health Insurance Portability</i>	
<i>&amp; Accountability Act (HIPAA)</i>	624
<i>Gramm-Leach-Bliley Act (GLBA)</i>	625
<i>California Senate Bill 1386 (SB 1386)</i>	625
<i>U.S. Banking Rules and Regulations</i>	625
<i>Payment Card Industry Data</i>	
<i>Security Standard (PCI DSS)</i>	626
<i>Fair Credit Reporting Act (FCRA)</i>	627
<i>Fair and Accurate Credit</i>	
<i>Transactions Act (FACTA)</i>	627
Non-Federal Privacy Concerns	
in the United States	628

International Privacy Laws . . . . .	629
<i>OECD Fair Information Practices</i> . . . . .	629
<i>European Laws</i> . . . . .	629
<i>Canadian Laws</i> . . . . .	631
<i>Asian Laws</i> . . . . .	631
Privacy-Enhancing Technologies . . . . .	632
Privacy Policies . . . . .	632
<i>Privacy Impact Assessment</i> . . . . .	633
Web Privacy Issues . . . . .	634
<i>Platform for Privacy Preferences</i>	
<i>Project (P3P)</i> . . . . .	634
<i>Cookies</i> . . . . .	634
Chapter 25 Review . . . . .	636

## Appendix A

### ■ Objectives Map: CompTIA Security+ 640

## Appendix B

### ■ About the CD 648

<i>System Requirements</i> . . . . .	648
LearnKey Online Training . . . . .	648
Installing and Running MasterExam . . . . .	648
<i>MasterExam</i> . . . . .	648
Electronic Book . . . . .	649
Help . . . . .	649
Removing Installation(s) . . . . .	649
Technical Support . . . . .	649
<i>LearnKey Technical Support</i> . . . . .	649

### ■ Glossary 650

### ■ Index 664