

Principles of Computer Security: CompTIA Security+™ and Beyond

Second Edition

**Wm. Arthur Conklin
Gregory White
Dwayne Williams
Roger Davis
Chuck Cothren**



New York Chicago San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi San Juan Seoul Singapore Sydney Toronto

CONTENTS AT A GLANCE

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

Introduction and Security Trends I

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 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, 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		
<i>Symmetric Encryption Summary.</i>	97		
Asymmetric Encryption.	98	Chapter 7	
RSA.	98	Standards and Protocols 152	
<i>Diffie-Hellman.</i>	99	PKTXandPKCS.	154
<i>ElGamal.</i>	100	<i>PKIX Standards.</i>	155
ECC.	100	PKCS.	156
<i>Asymmetric Encryption Summary.</i>	101	<i>Why You Need to Know the PKIX</i>	
Steganography.	101	<i>and PKCS Standards.</i>	158
Cryptography Algorithm Use.	103	X.509.	160
<i>Confidentiality.</i>	104	SSL/TLS.	161
<i>Integrity.</i>	104	ISAKMP.	162
<i>Nonrepudiation.</i>	104	CMP.	163
<i>Authentication.</i>	105	XKMS.	164
<i>Key Escrow.</i>	105	S/MIME.	166
<i>Digital Signatures.</i>	106	<i>IETF S/MIME History.</i>	166
<i>Digital Rights Management.</i>	107	<i>IETF S/MIME v3 Specifications.</i>	167
<i>Cryptographic Applications.</i>	108	PGP.	168
Chapter 5 Review.	110	<i>How PGP Works.</i>	168
		HTTPS.	169
Chapter 6		IPsec.	170
Public Key Infrastructure I 14		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
<i>Local Registration Authorities.</i>	120	WTLS.	171
Certificate Repositories.	120	PPTP.	172
Trust and Certificate Verification.	121	WEP.	172
Digital Certificates.	124	<i>WEP Security Issues.</i>	172
<i>Certificate Attributes.</i>	125	ISO/IEC 27002 (Formerly ISO 17799).	173
<i>Certificate Extensions.</i>	126	Chapter 7 Review.	174
<i>Certificate Lifecycles.</i>	127		
Centralized and Decentralized		Chapter 8	
Infrastructures.	132	Physical Security 178	
<i>Hardware Storage Devices.</i>	133	The Security Problem.	179
<i>Private Key Protection.</i>	134	Physical Security Safeguards.	183
<i>Key Recovery.</i>	135	<i>Walls and Guards.</i>	183
<i>Key Escrow.</i>	136	<i>Policies and Procedures.</i>	184
Public Certificate Authorities.	137	<i>Access Controls and Monitoring.</i>	188
In-House Certificate Authorities.	138	<i>En'vironmental Controls.</i>	191
<i>Choosing Between a Public CA</i>		<i>Fire Suppression.</i>	191
<i>and an In-House CA.</i>	138	<i>Authentication.</i>	195
<i>Outsourced Certificate Authorities.</i>	139	Chapter 8 Review.	200
<i>Tying Different PKIs Together.</i>	140		
<i>Trus) Models.</i>	140		

Chapter 9

Network Fundamentals 204

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

Chapter 10

Infrastructure Security 228

Devices	229
Workstations	229
Servers	231
Visualization	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

<i>Electronic Media</i>	254
<i>Network Attached Storage</i>	255
Chapter 10 Review	256

Chapter 11

Authentication and Remote Access 260

The Remote Access Process	261
<i>Identification</i>	262
<i>Authentication</i>	262
<i>Authorization</i>	267
<i>Access Control</i>	268
IEEE802.1X	270
<i>Wireless Protocols</i>	271
RADIUS	271
RAD/US <i>Authentication</i>	272
RADIUS <i>Authorization</i>	273
RADIUS <i>Accounting</i>	273
<i>Diameter</i>	274
TACACS+	274
TACACS+ <i>Authentication</i>	275
TACACS+ <i>Authorization</i>	276
TACACS+ <i>Accounting</i>	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
<i>Security Associations</i>	284
<i>IPsec Configurations</i>	285
<i>IPsec Security</i>	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
<i>802.11: Individual Standards</i>	304
<i>Attacking 802.11</i>	306
<i>New Security Protocols</i>	310
<i>Implementing 802.1X</i>	311
Chapter 12 Review	314

Chapter 13

„ Intrusion Detection Systems and Network Security 3 18

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

Chapter 14

Baselines 358

Overview of Baselines	359
Password Selection	359

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

Chapter 15

Types of Attacks and Malicious Software 388

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

Chapter 16

E-Mail and Instant Messaging 420

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

Chapter 17

Web Components 444

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

Chapter 18

Secure Software Development 474

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

Chapter 19

Disaster Recovery, Business Continuity, and Organizational Policies 492

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

Chapter 20

Risk Management 524

An Overview of Risk Management	525
<i>Example of Risk Management at the International Banking Level</i>	525
<i>Risk Management Vocabulary</i>	526
What Is Risk Management?.	527
Business Risks.	528
<i>Examples of Business Risks</i>	528
<i>Examples of Technology Risks</i>	529
Risk Management Models.	529
<i>General Risk Management Model</i>	529
<i>Software Engineering Institute Model</i>	532
<i>Model Application</i>	533
Qualitatively Assessing Risk	533
Quantitatively Assessing Risk	535
<i>Adding Objectivity to a Qualitative Assessment</i>	535
<i>A Common Objective Approach</i>	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 Ethics¹</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>& 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
^ ••j	sr.,
Chapter 25 Review.	636

Appendix A	
Objectives Map: CompTIA	
Security+ 640	

Appendix B
About the CD 648

<i>S^{ystem} 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

I Glossary	650
------------	-----

I Index	664
---------	-----