

Principles of Computer Security: CompTIA Security+™ and Beyond

(Exam SY0-301)

Third Edition

■ About the Authors

Dr. Wm. Arthur Conklin is an assistant professor in the College of Technology at the University of Houston. Dr. Conklin has terminal degrees from the Naval Postgraduate School in electrical engineering and The University of Texas at San Antonio in business administration. Dr. Conklin's research interests lie in the areas of software assurance and the application of systems theory to security issues associated with critical infrastructures. His dissertation was on the motivating factors for home users in adopting security on their own PCs. He has coauthored six books on information security and has written and presented numerous conference and academic journal papers. He has over ten years of teaching experience at the college level and has assisted in building two information security programs that have been recognized by the NSA and DHS as Centers of Academic Excellence in Information Assurance Education. A former U.S. Navy officer, he was also previously the Technical Director at the Center for Infrastructure Assurance and Security at The University of Texas at San Antonio.

Dr. Gregory White has been involved in computer and network security since 1986. He spent 19 years on active duty with the U.S. Air Force and is currently in the Air Force Reserves assigned to the Pentagon. He obtained his Ph.D. in computer science from Texas A&M University in 1995. His dissertation topic was in the area of computer network intrusion detection, and he continues to conduct research in this area today. He is currently the Director for the Center for Infrastructure Assurance and Security and is an associate professor of computer science at The University of Texas at San Antonio. Dr. White has written and presented numerous articles and conference papers on security. He is also the coauthor for five textbooks on computer and network security and has written chapters for two other security books. Dr. White continues to be active in security research. His current research initiatives include efforts in high-speed intrusion detection, community infrastructure protection, and visualization of community and organization security postures.

Dwayne Williams is Associate Director, Special Projects for the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio and has over 18 years of experience in information systems and network security. Mr. Williams's experience includes six years of commissioned military service as a Communications-Computer Information Systems Officer in the U.S. Air Force, specializing in network security, corporate information protection, intrusion detection systems, incident response, and VPN technology. Prior to joining the CIAS, he served as Director of Consulting for SecureLogix Corporation, where he directed and provided security assessment and integration services to Fortune 100, government, public utility, oil and gas, financial, and technology clients. Mr. Williams graduated in 1993 from Baylor University with a Bachelor of Arts in Computer Science. Mr. Williams is a Certified Information Systems Security Professional (CISSP) and coauthor of McGraw-Hill's *Voice and Data Security* and *CompTIA Security+ All-in-One Exam Guide*.

Roger L. Davis, CISSP, CISM, CISA, is Program Manager of ERP systems at the Church of Jesus Christ of Latter-day Saints, managing the Church's global financial system in over 140 countries. He has served as president of the Utah chapter of the Information Systems Security Association (ISSA) and various board positions for the Utah chapter of the Information Systems Audit and Control Association (ISACA). He is a retired Air Force lieutenant colonel with 30 years of military and information systems/security experience. Mr. Davis served on the faculty of Brigham Young University and the Air Force Institute of Technology. He coauthored McGraw-Hill's *CompTIA Security+ All-in-One Exam Guide* and *Voice and Data Security*. He holds a master's degree in computer science from George Washington University, a bachelor's degree in computer science from Brigham Young University, and performed post-graduate studies in electrical engineering and computer science at the University of Colorado.

Chuck Cothren, CISSP, is the president of Globex Security, Inc., and applies a wide array of network security experience to consulting and training. This includes performing controlled penetration testing, network security policies, network intrusion detection systems, firewall configuration and management, and wireless security assessments. He has analyzed security methodologies for voice over IP (VoIP) systems and supervisory control and data acquisition (SCADA) systems. Mr. Cothren was previously employed at the University of Texas Center for Infrastructure Assurance and Security. He is coauthor of *Voice and Data Security* and *CompTIA Security+ All-in-One Exam Guide*. Mr. Cothren holds a B.S. in Industrial Distribution from Texas A&M University.

About the Technical Editor

Bobby E. Rogers is a principal information security analyst with Dynetics, Inc., a national technology firm specializing in the certification and accreditation process for the U.S. government. He also serves as a penetration testing team lead for various government and commercial engagements. Bobby recently retired from the U.S. Air Force after almost 21 years, where he served as a computer networking and security specialist and designed and managed networks all over the world. His IT security experience includes several years working as an information assurance manager and a regular consultant to U.S. Air Force military units on various cybersecurity/computer abuse cases. He has held several positions of responsibility for network security in both the Department of Defense and private company networks. His duties have included perimeter security, client-side security, security policy development, security training, and computer crime investigations. As a trainer, he has taught a wide variety of IT-related subjects in both makeshift classrooms in desert tents and formal training centers. Bobby is also an accomplished author, having written numerous IT articles in various publications and training materials for the U.S. Air Force. He has also authored numerous security training videos.

He has a Bachelor of Science degree in computer information systems from Excelsior College and two Associates in Applied Science degrees from the Community College of the Air Force. Bobby's professional IT certifications include A+, Security+, ACP, CCNA, CCAI, CIW, CIWSA, MCP+I, MCSA (Windows 2000 & 2003), MCSE (Windows NT4, 2000 & 2003), MCSE: Security (Windows 2000 & 2003), CISSP, CIFI, CEH, CHFI, and CPTS, and he is also a certified trainer.

Principles of Computer Security: CompTIA Security+™ and Beyond

(Exam SY0-301)

Third 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

Cataloging-in-Publication Data is on file with the Library of Congress

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative, please e-mail us at bulksales@mcgraw-hill.com.

Principles of Computer Security: CompTIA Security+™ and Beyond, Third Edition (Exam SY0-301)

Copyright © 2012 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

All trademarks or copyrights mentioned herein are the possession of their respective owners and McGraw-Hill makes no claim of ownership by the mention of products that contain these marks.

1 2 3 4 5 6 7 8 9 0 QDB QDB 1 0 9 8 7 6 5 4 3 2

ISBN: Book p/n 978-0-07-178616-4 and CD p/n 978-0-07-178617-1 of set 978-0-07-178619-5

MHID: Book p/n 0-07-178616-3 and CD p/n 0-07-178617-1 of set 0-07-178619-8

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill, or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

McGraw-Hill is an independent entity from CompTIA®. This publication and CD may be used in assisting students to prepare for the CompTIA Security+ exam. Neither CompTIA nor McGraw-Hill warrants that use of this publication and CD will ensure passing any exam. CompTIA and CompTIA Security+ are trademarks or registered trademarks of CompTIA in the United States and/or other countries. All other trademarks are trademarks of their respective owners.

SANS Institute IT Code of Ethics reproduced with permission, © SANS Institute.

Sponsoring Editor
TIMOTHY GREEN

Editorial Supervisor
JANET WALDEN

Project Editor
LEEANN PICKRELL

Acquisitions Coordinator
STEPHANIE EVANS

Technical Editor
BOBBY E. ROGERS

Copy Editor
LEEANN PICKRELL

Proofreader
PAUL TYLER

Indexer
REBECCA PLUNKETT

Production Supervisor
JEAN BODEAUX

Composition
CENVEO PUBLISHER SERVICES

Illustration
CENVEO PUBLISHER SERVICES

Art Director, Cover
JEFF WEEKS

- *This book is dedicated to the many security professionals who daily work to ensure the safety of our nation's critical infrastructures. We want to recognize the thousands of dedicated individuals who strive to protect our national assets but who seldom receive praise and often are only noticed when an incident occurs. To you, we say thank you for a job well done!*

■ Acknowledgments

We, the authors of *Principles of Computer Security: CompTIA Security+™ and Beyond, Third Edition*, have many individuals who we need to acknowledge—individuals without whom this effort would not have been successful. This third edition would not have been possible without Tim Green, who navigated a myriad of problems and made life easier for the author team. He brought together an all-star production team that made this book more than just a new edition, but a complete learning system.

The list needs to start with those folks at McGraw-Hill who worked tirelessly with the project's multiple authors and contributors and lead us successfully through the minefield that is a book schedule and who took our rough chapters and drawings and turned them into a final, professional product we can be proud of. We thank all the good people from the Acquisitions team, Tim Green and Stephanie Evans; from the Editorial Services team, Janet Walden and LeeAnn Pickrell; from the Illustration and Production teams, Jean Bodeaux and Amarjeet Kumar and the composition team at Cenveo Publisher Services. We also thank the technical editor, Bobby Rogers; the copy editors, Bill McManus and LeeAnn Pickrell; the proofreader, Paul Tyler; and the indexer, Rebecca Plunkett; for all their attention to detail that made this a finer work after they finished with it.

We also need to acknowledge our current employers who, to our great delight, have seen fit to pay us to work in a career field that we all find exciting and rewarding. There is never a dull moment in security, because it is constantly changing.

We would like to thank Art Conklin for herding the cats on this one.

Finally, we would each like to individually thank those people who—on a personal basis—have provided the core support for us individually. Without these special people in our lives, none of us could have put this work together.

Successful cat herders have many behind them helping them succeed. I owe thanks to many friends, their friendship and support makes efforts such as this possible. And to Susan, my lovely wife and friend, thank you for your sacrifices that enable me to do the things I do.

—Art Conklin, Ph.D.

I would like to thank my wife, Charlan, for the tremendous support she has always given me. It doesn't matter how many times I have sworn that I'll never get involved with another book project only to return within months to yet another one; through it all, she has remained supportive.

I would also like to publicly thank the United States Air Force, which provided me numerous opportunities since 1986 to learn more about security than I ever knew existed.

To whoever it was who decided to send me as a young captain—fresh from completing my master's degree in artificial intelligence—to my first assignment in computer security: thank you, it has been a great adventure!

—Gregory B. White, Ph.D.

For Macon.

—*Chuck Cothren*

Geena, thanks for being my best friend and my greatest support. Anything I am is because of you. Love to my kids and grandkids!

—*Roger L. Davis*

To my wife and best friend Leah for your love, energy, and support—thank you for always being there. Here's to many more years together.

—*Dwayne Williams*

ABOUT THIS BOOK

■ Important Technology Skills

Information technology (IT) offers many career paths and information security is one of the fastest-growing tracks for IT professionals. This book provides coverage of the materials you need to begin your exploration of information security.

In addition to covering all of the CompTIA Security+ exam objectives, additional material is included to help you build a solid introductory knowledge of information security.

Key Terms, identified in red, point out important vocabulary and definitions that you need to know.

Tech Tip sidebars provide inside information from experienced information security professionals.

Cross Check questions develop reasoning skills: ask, compare, contrast, and explain.

system), that requires authorization can use its own authorization method once a user has occurred. This makes for efficient and consistent applications.

Access Control

Access control refers to all security features used to prevent unauthorized access to a computer system or network—or even a network. In this sense, it may be confused with authentication, which is the ability of a subject (such as an individual or a computer system) to interact with an object (such as a file or hardware device). Once the individual has verified their identity, access controls regulate what the individual can actually do on the system. Just because a person is granted entry to the system, that does not mean that they should have access to all data the system contains.

To further illustrate, consider another example. When you go to your bank to make a withdrawal, the teller at the window will verify that you are indeed who you claim to be. This is usually done by asking you to provide some form of identification with your picture on it, such as your driver's license. You may also have to provide information such as your bank account number. Once the teller verifies your identity, you will have proved that you are a valid (authorized) customer of this bank. This does not, however, mean that you have the ability to view all information that the bank protects—such as your neighbor's account. The teller controls what information, and funds, you may have access to and grants you access only to that which you are authorized. In this example, your identification and bank account number serve as your method of authentication and the teller serves as the access control mechanism.

In computer systems and networks, there are several ways that access controls can be implemented. An access control matrix provides the simplest framework for illustrating the process. An example of an access control matrix is provided in Table 11.1. In this matrix, the system is keeping track of two processes, two files, and one hardware device. Process 1 can read both File 1 and File 2 but can write only to File 1. Process 1 cannot access Process 2, but Process 2 can execute Process 1. Both processes have the ability to write to the printer.

While simple to understand, the access control matrix is seldom used in computer systems because it is extremely costly in terms of storage space and processing. Imagine the size of an access control matrix for a large network with hundreds of users and thousands of files. The actual mechanics

	Process 1	Process 2	File 1	File 2	Printer
Process 1	Read, write, execute		Read, write	Read	Write
Process 2	Execute	Read, write, execute	Read, write	Read, write	Write

Principles of Computer Security: CompTIA Security+ and Beyond

Engaging and Motivational — Using a conversational style and proven instructional approach, the authors explain technical subjects in a clear, interesting way using real-world examples.

The Basics of Public Key Infrastructures

A public key infrastructure (PKI) provides all the components necessary for different types of users and entities to be able to communicate securely and in a predictable manner. A PKI is made up of various applications, policies, services, programming interfaces, protocols, users, and utilities. These key cryptographic technologies allow communication to take place using keys for digital signatures, data encryption, and integrity.

Although many different applications and protocols can provide the same type of functionality, constructing and implementing a PKI boils down to establishing a level of trust. If, for example, John and Diane want to communicate securely, John can generate his own public/private key pair and send his public key to Diane, or he can place his public key in a directory that is available to everyone, either from him or from a public directory. If Diane receives John's public key, she can use it to encrypt her messages so that only John can read them. However, she would actually be communicating with Katie. What is needed is a way to verify an individual's identity, to ensure that a person's public key is bound to their identity and that the previous scenario (and others) cannot take place.

In PKI environments, entities called registration authorities (RAs) and certificate authorities (CAs) provide services similar to those of the Department of Motor Vehicles (DMV). John, who has just received a driver's license, has to prove his identity to the DMV by providing his passport, birth certificate, or other identification documentation. If the DMV is satisfied with the proof John provides (and John passes a driving test), the DMV will create a driver's license that can then be used by John to prove his identity. Whenever John needs to identify himself, he can show his driver's license.

If Diane receives John's public key, how does she know the key really came from John? Maybe another individual, Katie, is masquerading as John and has replaced John's public key with her own, as shown in Figure 6.1 (referred to as a man-in-the-middle attack). If this took place, Diane would believe that her messages could be read only by John and that the replies were actually from him. However, she would actually be communicating with Katie. What is needed is a way to verify an individual's identity, to ensure that a person's public key is bound to their identity and that the previous scenario (and others) cannot take place.

In PKI environments, entities called registration authorities (RAs) and certificate authorities (CAs) provide services similar to those of the Department of Motor Vehicles (DMV). John, who has just received a driver's license, has to prove his identity to the DMV by providing his passport, birth certificate, or other identification documentation. If the DMV is satisfied with the proof John provides (and John passes a driving test), the DMV will create a driver's license that can then be used by John to prove his identity. Whenever John needs to identify himself, he can show his driver's license.

Man-in-the-Middle Attack

1. Katie replaces John's public key with her key in the publicly accessible directory.
2. Diane extracts what she thinks is John's key but it is in fact Katie's key.
3. Katie can now read messages Diane encrypts and sends to John.
4. After Katie decrypts and reads Diane's message, she encrypts it with John's public key and sends it on to him so he will not be the wiser.

Figure 6.1 Without PKIs, individuals could spoof others' identities.

Chapter 6: Public Key Infrastructures

Makes Learning Fun! — Rich, colorful text and illustrations bring technical concepts to life.

Proven Learning Method Keeps You on Track

Designed for classroom use and written by instructors for use in their own classes, Principles of Computer Security: CompTIA Security+ and Beyond is structured to give you comprehensive knowledge of information security. The textbook's active learning methodology guides you beyond mere recall and—through thought-provoking activities, labs, and sidebars—helps you develop critical-thinking, diagnostic, and communication skills.

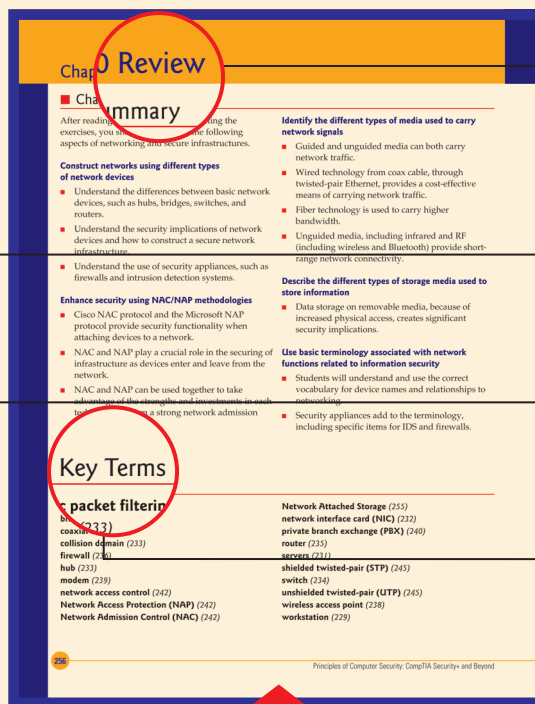
Effective Learning Tools

This feature-rich textbook is designed to make learning easy and enjoyable and to help you develop the skills and critical thinking abilities that will enable you to adapt to different job situations and to troubleshoot problems. Written by

instructors with decades of combined information security experience, this book conveys even the most complex issues in an accessible, easy-to-understand format.



Offers Practical Experience—Tutorials and lab assignments develop essential hands-on skills and put concepts in real-world contexts.



Robust Learning Tools—Summaries, key term lists, quizzes, essay questions, and lab projects help you practice skills

Chapter Review sections provide concept summaries, key terms lists, and lots of questions and projects.

Try This! exercises apply core skills in a new setting.

Notes, Tips, Warnings, and Exam Tips create a road map for success.

Key Terms List presents the important terms identified in the chapter.

Each chapter includes:

- **Learning Objectives** that set measurable goals for chapter-by-chapter progress
- **Illustrations** that give you a clear picture of the concepts and technologies
- **Try This!, Cross Check, and Tech Tip** sidebars that encourage you to practice and apply concepts in real-world settings
- **Notes, Tips, and Warnings** that guide you, and **Exam Tips** that give you advice or provide information specifically related to preparing for the exam
- **Chapter Summaries and Key Terms Lists** that provide you with an easy way to review important concepts and vocabulary
- **Challenging End-of-Chapter Tests** that include vocabulary-building exercises, multiple-choice questions, essay questions, and on-the-job lab projects

CONTENTS AT A GLANCE

- Chapter 1 ■ **Introduction and Security Trends 1**
- 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 116**
- Chapter 7 ■ **Standards and Protocols 154**
- Chapter 8 ■ **Physical Security 180**
- Chapter 9 ■ **Network Fundamentals 208**
- Chapter 10 ■ **Infrastructure Security 232**
- Chapter 11 ■ **Authentication and Remote Access 264**
- Chapter 12 ■ **Wireless Security 298**
- Chapter 13 ■ **Intrusion Detection Systems and Network Security 322**
- Chapter 14 ■ **Baselines 364**

Chapter 15	■	Types of Attacks and Malicious Software	396
Chapter 16	■	E-Mail and Instant Messaging	430
Chapter 17	■	Web Components	454
Chapter 18	■	Secure Software Development	484
Chapter 19	■	Disaster Recovery, Business Continuity, and Organizational Policies	502
Chapter 20	■	Risk Management	536
Chapter 21	■	Change Management	556
Chapter 22	■	Privilege Management	572
Chapter 23	■	Computer Forensics	594
Chapter 24	■	Legal Issues and Ethics	610
Chapter 25	■	Privacy	632
Appendix A	■	Objective Map	654
Appendix B	■	About the CD	666
	■	Glossary	668
	■	Index	684

CONTENTS

Preface	xxi
Introduction	xxiii
CompTIA Approved Quality Curriculum	xxvi
Instructor and Student Web Site	xxx

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 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>	43
<i>Integrity Models</i>	44
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>	72
People as a Security Tool	76
<i>Security Awareness</i>	76
<i>Individual User Responsibilities</i>	77
Chapter 4 Review	79

Chapter 5

■ Cryptography 82

Algorithms	84
Hashing Functions	87
<i>SHA</i>	89
<i>RIPEDM</i>	90
<i>Message Digest</i>	90
<i>Hashing Summary</i>	92
Symmetric Encryption	92
<i>DES</i>	93
<i>3DES</i>	94

Chapter 9

■ Network Fundamentals 208

Network Architectures	209
Network Topology	210
Network Protocols	211
<i>Packets</i>	213
<i>TCP vs. UDP</i>	214
<i>ICMP</i>	215
Packet Delivery	217
<i>Local Packet Delivery</i>	217
<i>Remote Packet Delivery</i>	218
<i>IP Addresses and Subnetting</i>	219
<i>Network Address Translation</i>	221
<i>Security Zones</i>	222
<i>VLANs</i>	226
Tunneling	227
Chapter 9 Review	228

Chapter 10

■ Infrastructure Security 232

Devices	233
<i>Workstations</i>	233
<i>Servers</i>	235
<i>Virtualization</i>	236
<i>Network Interface Cards</i>	236
<i>Hubs</i>	237
<i>Bridges</i>	237
<i>Switches</i>	238
<i>Loop Protection</i>	239
<i>Routers</i>	239
<i>Firewalls</i>	240
<i>Wireless</i>	242
<i>Modems</i>	243
<i>Telecom/PBX</i>	245
<i>VPN</i>	245
<i>Intrusion Detection Systems</i>	246
<i>Network Access Control</i>	246
<i>Network Monitoring/Diagnostic</i>	247
<i>Mobile Devices</i>	248
<i>Device Security, Common Concerns</i>	249
Media	249
<i>Coaxial Cable</i>	249
<i>UTP/STP</i>	250
<i>Fiber</i>	251
<i>Unguided Media</i>	252
Security Concerns for Transmission Media	254
Physical Security Concerns	254

Removable Media	255
<i>Magnetic Media</i>	255
<i>Optical Media</i>	258
<i>Electronic Media</i>	259
Cloud Computing	259
<i>Software as a Service</i>	260
<i>Platform as a Service</i>	260
<i>Infrastructure as a Service</i>	260
<i>Network Attached Storage</i>	260
Chapter 10 Review	261

Chapter 11

■ Authentication and Remote Access 264

The Remote Access Process	265
<i>Identification</i>	266
<i>Authentication</i>	266
<i>Authorization</i>	271
<i>Access Control</i>	272
IEEE 802.1X	274
<i>Wireless Protocols</i>	275
RADIUS	275
<i>RADIUS Authentication</i>	276
<i>RADIUS Authorization</i>	277
<i>RADIUS Accounting</i>	277
<i>Diameter</i>	278
TACACS+	278
<i>TACACS+ Authentication</i>	279
<i>TACACS+ Authorization</i>	280
<i>TACACS+ Accounting</i>	280
Authentication Protocols	281
<i>L2TP and PPTP</i>	281
<i>PPP</i>	281
<i>PPTP</i>	282
<i>EAP</i>	283
<i>CHAP</i>	283
<i>NTLM</i>	284
<i>PAP</i>	284
<i>L2TP</i>	284
<i>Telnet</i>	285
<i>SSH</i>	285
FTP/FTPS/SFTP	287
VPNs	287
IPsec	288
<i>Security Associations</i>	289
<i>IPsec Configurations</i>	289
<i>IPsec Security</i>	290
Vulnerabilities of Remote	
Access Methods	293
Connection Summary	294
Chapter 11 Review	295

Chapter 12

■ Wireless Security 298

Introduction to Wireless Networking	299
Mobile Phones	300
WAP	302
3G Mobile Networks	304
Bluetooth	304
802.11	307
802.11: Individual Standards	308
Attacking 802.11	311
New Security Protocols	315
Implementing 802.1X	316
Chapter 12 Review	318

Chapter 13

■ Intrusion Detection Systems and Network Security 322

History of Intrusion	
Detection Systems	323
IDS Overview	324
Network-Based IDSs	326
Advantages of a NIDS	330
Disadvantages of a NIDS	330
Active vs. Passive NIDSs	330
Signatures	331
False Positives and False Negatives	332
IDS Models	333
Firewalls	334
How Do Firewalls Work?	335
Intrusion Prevention Systems	337
Detection Controls vs. Prevention Controls	338
Web Application Firewalls vs. Network	
Firewalls	339
Proxy Servers	339
Internet Content Filters	341
Protocol Analyzers	341
Honeypots and Honeynets	343
Host-Based IDSs	345
Advantages of HIDSs	348
Disadvantages of HIDSs	349
Active vs. Passive HIDSs	350
Resurgence and Advancement of HIDSs	350
PC-Based Malware Protection	351
Antivirus Products	351
Personal Software Firewalls	353
Pop-up Blockers	355
Windows Defender	356
Antispam	357
All-in-One Security Appliances	358
Chapter 13 Review	359

Chapter 14

■ Baselines 364

Overview of Baselines	365
Password Selection	365
Operating System and Network Operating	
System Hardening	366
Hardening Microsoft Operating Systems	367
Hardening UNIX- or Linux-Based	
Operating Systems	370
Updates (a.k.a. Hotfixes,	
Service Packs, and Patches)	379
Network Hardening	381
Software Updates	382
Device Configuration	382
Securing Management Interfaces	383
VLAN Management	383
IPv4 vs. IPv6	384
Application Hardening	384
Application Configuration Baseline	384
Application Patches	384
Patch Management	385
Host Software Baseline	387
Group Policies	388
Security Templates	390
Chapter 14 Review	392

Chapter 15

■ Types of Attacks and Malicious Software 396

Avenues of Attack	397
The Steps in an Attack	397
Minimizing Possible Avenues of Attack	399
Attacking Computer Systems	
and Networks	400
Denial-of-Service Attacks	400
Backdoors and Trapdoors	403
Null Sessions	403
Sniffing	404
Spoofing	405
Man-in-the-Middle Attacks	408
Replay Attacks	409
TCP/IP Hijacking	409
Drive-by Download Attacks	409
Phishing and Pharming Attacks	410
Attacks on Encryption	410
Address System Attacks	411
Password Guessing	412
Software Exploitation	414
Client-side Attacks	414
Malicious Code	415

Malware Defenses	421
War-Dialing and War-Driving	422
Social Engineering	423
Auditing	423
Chapter 15 Review	425

Chapter 16

■ E-Mail and Instant Messaging 430

Security of E-Mail	431
Malicious Code	433
Hoax E-Mails	437
Unsolicited Commercial E-Mail (Spam)	438
Mail Encryption	441
S/MIME	442
PGP	443
Instant Messaging	445
Chapter 16 Review	450

Chapter 17

■ Web Components 454

Current Web Components and Concerns	455
Web Protocols	455
Encryption (SSL and TLS)	456
The Web (HTTP and HTTPS)	462
Directory Services (DAP and LDAP)	463
File Transfer (FTP and SFTP)	464
Vulnerabilities	465
Code-Based Vulnerabilities	465
Buffer Overflows	466
Java and JavaScript	467
ActiveX	469
Securing the Browser	470
CGI	471
Server-Side Scripts	471
Cookies	472
Signed Applets	474
Browser Plug-ins	475
Application-Based Weaknesses	477
Open Vulnerability and Assessment Language (OVAL)	478
Web 2.0 and Security	478
Chapter 17 Review	480

Chapter 18

■ Secure Software Development 484

The Software Engineering Process	485
Process Models	485
Secure Development Lifecycle	486
Threat Modeling Steps	488
Chapter 18 Review	498

Chapter 19

■ Disaster Recovery, Business Continuity, and Organizational Policies 502

Disaster Recovery	503
Disaster Recovery Plans/Process	503
Backups	505
Utilities	512
Secure Recovery	512
Cloud Computing	513
High Availability and Fault Tolerance	513
Failure and Recovery Timing	515
Computer Incident Response Teams	516
Test, Exercise, and Rehearse	517
Policies and Procedures	518
Security Policies	518
Privacy	524
Service Level Agreements	525
Human Resources Policies	525
Code of Ethics	527
Incident Response Policies and Procedures	527
Chapter 19 Review	532

Chapter 20

■ Risk Management 536

An Overview of Risk Management	537
Example of Risk Management at the International Banking Level	537
Risk Management Vocabulary	538
What Is Risk Management?	539
Business Risks	540
Examples of Business Risks	540
Examples of Technology Risks	541
Risk Management Models	541
General Risk Management Model	541
Software Engineering Institute Model	544
Model Application	545
Qualitatively Assessing Risk	545

Quantitatively Assessing Risk	547
<i>Adding Objectivity to</i>	
<i>a Qualitative Assessment</i>	547
<i>A Common Objective Approach</i>	548
Qualitative vs. Quantitative	
Risk Assessment	549
Tools	550
Chapter 20 Review	551

Chapter 21

■ Change Management 556

Why Change Management?	557
The Key Concept:	
Separation of Duties	559
Elements of Change Management	560
Implementing Change Management	562
<i>The Purpose of a Change Control Board</i>	563
<i>Code Integrity</i>	565
The Capability Maturity Model Integration	565
Chapter 21 Review	567

Chapter 22

■ Privilege Management 572

User, Group, and Role Management	573
<i>User</i>	573
<i>Group</i>	575
<i>Role</i>	576
Password Policies	576
<i>Domain Password Policy</i>	577
Single Sign-On	579
<i>Time of Day Restrictions</i>	580
<i>Tokens</i>	580
<i>Account and Password Expiration</i>	581
Security Controls and Permissions	582
<i>Access Control Lists</i>	584
Handling Access Control	
(MAC, DAC, and RBAC)	585
<i>Mandatory Access Control (MAC)</i>	585
<i>Discretionary Access Control (DAC)</i>	586
<i>Role-Based Access Control (RBAC)</i>	587
<i>Rule-Based Access Control (RBAC)</i>	587
<i>Account Expiration</i>	588
Preventing Data Loss or Theft	588
Chapter 22 Review	589

Chapter 23

■ Computer Forensics 594

Evidence	596
<i>Standards for Evidence</i>	596
<i>Types of Evidence</i>	596
<i>Three Rules Regarding Evidence</i>	597
Collecting Evidence	597
<i>Acquiring Evidence</i>	597
<i>Identifying Evidence</i>	599
<i>Protecting Evidence</i>	599
<i>Transporting Evidence</i>	600
<i>Storing Evidence</i>	600
<i>Conducting the Investigation</i>	600
Chain of Custody	601
Free Space vs. Slack Space	602
<i>Free Space</i>	602
<i>Slack Space</i>	602
Message Digest and Hash	602
Analysis	603
Chapter 23 Review	605

Chapter 24

■ Legal Issues and Ethics 610

Cybercrime	611
<i>Common Internet Crime Schemes</i>	613
<i>Sources of Laws</i>	614
<i>Computer Trespass</i>	614
<i>Significant U.S. Laws</i>	615
<i>Payment Card Industry Data</i>	
<i>Security Standard (PCI DSS)</i>	618
<i>Import/Export Encryption Restrictions</i>	619
<i>Non-U.S. Laws</i>	621
<i>Digital Signature Laws</i>	621
<i>Digital Rights Management</i>	623
Ethics	625
Chapter 24 Review	628

Chapter 25

■ Privacy 632

Personally Identifiable	
Information (PII)	633
<i>Sensitive PII</i>	634
<i>Notice, Choice, and Consent</i>	634
U.S. Privacy Laws	634
<i>Privacy Act of 1974</i>	635
<i>Freedom of Information Act (FOIA)</i>	635

<i>Family Education Records and Privacy Act (FERPA)</i>	636
<i>U.S. Computer Fraud and Abuse Act (CFAA)</i>	636
<i>U.S. Children’s Online Privacy Protection Act (COPPA)</i>	637
<i>Video Privacy Protection Act (VPPA)</i>	637
<i>Health Insurance Portability & Accountability Act (HIPAA)</i>	638
<i>Gramm-Leach-Bliley Act (GLBA)</i>	639
<i>California Senate Bill 1386 (SB 1386)</i>	639
<i>U.S. Banking Rules and Regulations</i>	639
<i>Payment Card Industry Data Security Standard (PCI DSS)</i>	640
<i>Fair Credit Reporting Act (FCRA)</i>	641
<i>Fair and Accurate Credit Transactions Act (FACTA)</i>	641
Non-Federal Privacy Concerns in the United States	642
International Privacy Laws	643
<i>OECD Fair Information Practices</i>	643
<i>European Laws</i>	643
<i>Canadian Laws</i>	645
<i>Asian Laws</i>	645
Privacy-Enhancing Technologies	646
Privacy Policies	646
<i>Privacy Impact Assessment</i>	647

Web Privacy Issues	648
<i>Platform for Privacy Preferences Project (P3P)</i>	648
<i>Cookies</i>	648
Chapter 25 Review	650

Appendix A

■ Objective Map 654

Appendix B

■ About the CD 666

System Requirements	666
LearnKey Online Training	666
Installing and Running MasterExam	666
<i>MasterExam</i>	666
Electronic Book	667
CompTIA Exam Objectives	667
Help	667
Removing Installation(s)	667
Technical Support	667
<i>LearnKey Technical Support</i>	667

■ Glossary 668

■ Index 684

PREFACE

Information and computer security has moved from the confines of academia to mainstream America in the last decade. The Code Red, Nimda, and Slammer attacks were heavily covered in the media and broadcast into the average American's home. Today, the Internet has turned 40, and with its maturing, the threats are increasing. Botnets and cyber-criminals are making news regularly. It has become increasingly obvious to everybody that something needs to be done to secure not only our nation's critical infrastructure but also the businesses we deal with on a daily basis. The question is, "Where do we begin?" What can the average information technology professional do to secure the systems that he or she is hired to maintain? One immediate answer is education and training. If we want to secure our computer systems and networks, we need to know how to do this and what security entails.

Complacency is not an option in today's hostile network environment. While we once considered the insider to be the major threat to corporate networks, and the "script kiddie" to be the standard external threat (often thought of as only a nuisance), the highly interconnected network world of today is a much different place. The U.S. government identified eight critical infrastructures a few years ago that were thought to be so critical to the nation's daily operation that if one were to be lost, it would have a catastrophic impact on the nation. To this original set of eight sectors, more have recently been added. A common thread throughout all of these, however, is technology—especially technology related to computers and communication. Thus, an individual, organization, or nation who wanted to cause damage to this nation could attack it not just with traditional weapons but with computers through the Internet. It is not surprising to hear that among the other information seized in raids on terrorist organizations, computers and Internet information are usually seized as well. While the insider can certainly still do tremendous damage to an organization, the external threat is again becoming the chief concern among many.

So, where do you, the IT professional seeking more knowledge on security, start your studies? The IT world is overflowing with certifications that can be obtained by those attempting to learn more about their chosen profession. The security sector is no different, and the CompTIA Security+ exam offers a basic level of certification for security. In the pages of this book you will find not only material that can help you prepare for taking the CompTIA Security+ exam but also the basic information that you will need in order to understand the issues involved in securing your computer systems and networks today. In no way is this book the final source for learning all about protecting your organization's systems, but it serves as a point from which to launch your security studies and career.

One thing is certainly true about this field of study—it never gets boring. It constantly changes as technology itself advances. Something else you will find as you progress in your security studies is that no matter how much technology advances and no matter how many new security devices are developed, at its most basic level, the human is still the weak link in the security chain. If you are looking for an exciting area to delve into, then you have certainly chosen wisely. Security offers a challenging blend of technology and people issues. We, the authors of this book, wish you luck as you embark on an exciting and challenging career path.

Wm. Arthur Conklin, Ph.D.

Gregory B. White, Ph.D.

INTRODUCTION

Computer security is becoming increasingly important today as the number of security incidents steadily climbs. Many corporations are now spending significant portions of their budget on security hardware, software, services, and personnel. They are spending this money not because it increases sales or enhances the product they provide, but because of the possible consequences should they not take protective actions.

Why Focus on Security?

Security is not something that we want to have to pay for; it would be nice if we didn't have to worry about protecting our data from disclosure, modification, or destruction from unauthorized individuals, but that is not the environment we find ourselves in today. Instead, we have seen the cost of recovering from security incidents steadily rise along with the rise in the number of incidents themselves. Since September 11, 2001, this has taken on an even greater sense of urgency as we now face securing our systems not just from attack by disgruntled employees, juvenile hackers, organized crime, or competitors; we now also have to consider the possibility of attacks on our systems from terrorist organizations. If nothing else, the events of September 11, 2001, showed that anybody is a potential target. You do not have to be part of the government or a government contractor; being an American is sufficient reason to make you a target to some, and with the global nature of the Internet, collateral damage from cyber attacks on one organization could have a worldwide impact.

A Growing Need for Security Specialists

To protect our computer systems and networks, we will need a significant number of new security professionals trained in the many aspects of computer and network security. This is not an easy task as the systems connected to the Internet become increasingly complex, with software whose lines of code number in the millions. Understanding why this is such a difficult problem to solve is not hard if you consider how many errors might be present in a piece of software that is several million lines long. When you add the additional factor of how fast software is being developed—from necessity as the market is constantly moving—understanding how errors occur is easy.

Not every “bug” in the software will result in a security hole, but it doesn't take many to affect the Internet community drastically. We can't just blame the

vendors for this situation, because they are reacting to the demands of government and industry. Most vendors are fairly adept at developing patches for flaws found in their software, and patches are constantly issued to protect systems from bugs that may introduce security problems. This introduces a whole new problem for managers and administrators—patch management. How important this has become is easily illustrated by how many of the most recent security events have occurred as a result of a security bug for which a patch was available months prior to the security incident; members of the community had not correctly installed the patch, however, thus making the incident possible. One of the reasons this happens is that many of the individuals responsible for installing the patches are not trained to understand the security implications surrounding the hole or the ramifications of not installing the patch. Many of these individuals simply lack the necessary training.

Because of the need for an increasing number of security professionals who are trained to some minimum level of understanding, certifications such as the Security+ have been developed. Prospective employers want to know that the individual they are considering hiring knows what to do in terms of security. The prospective employee, in turn, wants to have a way to demonstrate his or her level of understanding, which can enhance the candidate's chances of being hired. The community as a whole simply wants more trained security professionals.

Preparing Yourself for the Security+ Exam

Principles of Computer Security: CompTIA Security+ and Beyond, Third Edition is designed to help prepare you to take the Security+ certification exam. When you pass it, you will demonstrate you have that basic understanding of security that employers are looking for. Passing this certification exam will not be an easy task, for you will need to learn many things to acquire that basic understanding of computer and network security.

How This Book Is Organized

The book is divided into chapters to correspond with the objectives of the exam itself. Some of the chapters are more technical than others—reflecting the nature of the security environment where you will be forced to deal with not only technical details but also other issues such as security policies and procedures as well as training and education. Although many individuals involved in computer and network security have advanced degrees in math, computer science, information systems, or computer or electrical engineering, you do not need this technical background to address security effectively in your organization. You do not need to develop your own cryptographic algorithm, for example; you simply need to be able to understand how cryptography is used, along with its strengths and weaknesses.

As you progress in your studies, you will learn that many security problems are caused by the human element. The best technology in the world still ends up being placed in an environment where humans have the opportunity to foul things up—and all too often do.

Onward and Upward

At this point, we hope that you are now excited about the topic of security, even if you weren't in the first place. We wish you luck in your endeavors and welcome you to the exciting field of computer and network security.



■ CompTIA Security+

- Designed for IT professionals focused on system security.
- Covers network infrastructure, cryptography, assessments, and audits.
- Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.



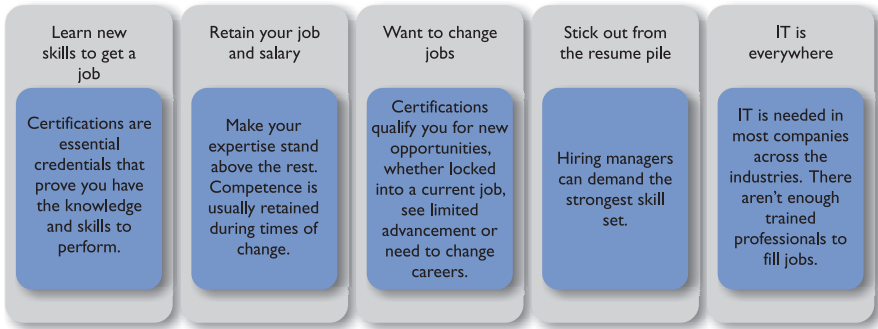
■ It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill. Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

Security is one of the highest-demand job categories—growing in importance as the frequency and severity of security threats continue to be a major concern for organizations around the world.

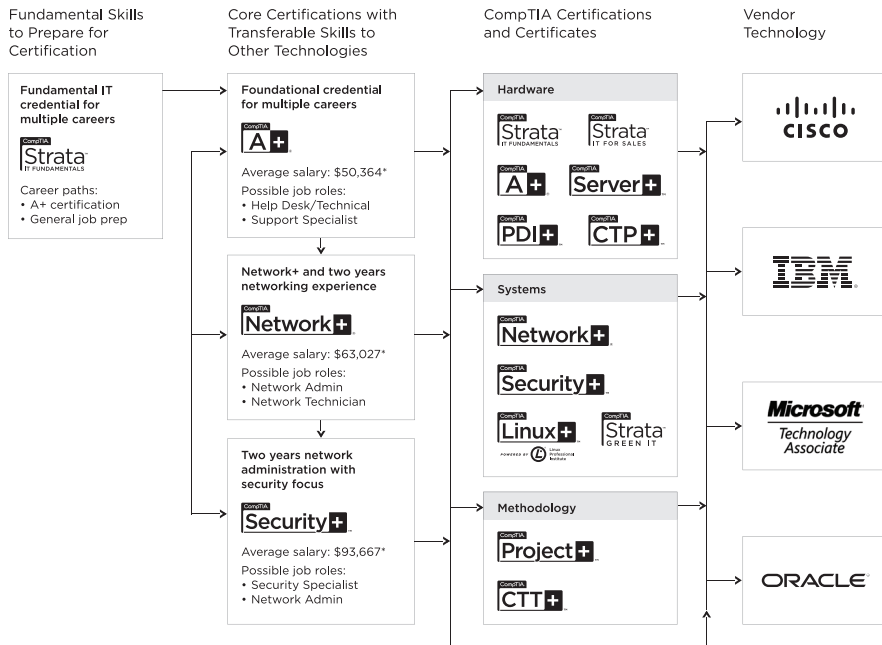
- Jobs for security administrators are expected to increase by 18 percent; the skill set required for these types of jobs map to CompTIA Security+ certification.
- Network security administrators can earn as much as \$106,000 per year.
- CompTIA Security+ is the first step in starting your career as a network security administrator or systems security administrator.
- CompTIA Security+ is regularly used in organizations such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career



CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and that allow you to pursue specific areas of concentration. Depending on the path you choose, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your career.



*Source: Computerworld Salary Survey 2010—U.S. salaries only

■ Steps to Getting Certified and Staying Certified

1. **Review exam objectives.** Review the certification objectives to make sure you know what is covered in the exam:
www.comptia.org/certifications/testprep/examobjectives.aspx
2. **Practice for the exam.** After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam:
www.comptia.org/certifications/testprep/practicetests.aspx
3. **Purchase an exam voucher.** Purchase exam vouchers on the CompTIA Marketplace, which is located at:
www.comptiastore.com
4. **Take the test!** Select a certification exam provider, and schedule a time to take your exam. You can find exam providers at the following link:
www.comptia.org/certifications/testprep/testingcenters.aspx
5. **Stay Certified! Meet the Continuing Education Requirement.** Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of your certification. There are a number of ways the certification can be renewed. For more information go to:
http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx

■ Join the Professional Community

The free online IT Pro Community provides valuable content to students and professionals.

Career IT job resources include

- Where to start in IT
- Career assessments
- Salary trends
- U.S. job board

Join the IT Pro Community and get access to:

- Forums on networking, security, computing, and cutting-edge technologies
- Access to blogs written by industry experts

- Current information on cutting-edge technologies
- Access to various industry resource links and articles related to IT and IT careers



OFFICIAL

MULTI-LAYERED LEARNING
TOOLS INCLUDED

■ Content Seal of Quality

This courseware bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100 percent of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

■ Why CompTIA?

- **Global recognition** CompTIA is recognized globally as the leading IT nonprofit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by hiring managers** Hiring managers value CompTIA certification because it is vendor- and technology-independent validation of your technical skills.
- **Recommended or required by government and businesses** Many government organizations and corporations (for example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more) either recommend or require technical staff to be CompTIA certified.
- **Three CompTIA certifications ranked in the top 10** In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

■ How to Obtain More Information

- **Visit CompTIA online** Go to www.comptia.org to learn more about getting CompTIA certified.
- **Contact CompTIA** Please call 866-835-8020, ext. 5 or e-mail questions@comptia.org.
- **Join the IT Pro Community** Go to <http://itpro.comptia.org> to join the IT community to get relevant career information.
- **Connect with CompTIA** Find us on Facebook, LinkedIn, Twitter, and YouTube.

■ CAQC Disclaimer

The logo of the CompTIA Approved Quality Curriculum (CAQC) program and the status of this or other training material as “Approved” under the CompTIA Approved Quality Curriculum program signifies that, in CompTIA’s opinion, such training material covers the content of CompTIA’s related certification exam.

The contents of this training material were created for the CompTIA Security+ exam covering CompTIA certification objectives that were current as of the date of publication.

CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such “Approved” or other training material in order to prepare for any CompTIA certification exam.

INSTRUCTOR AND STUDENT WEB SITE

For instructor and student resources, check out www.PrinciplesSecurity3e.com. Students will find chapter quizzes that will help them learn more about computer security, and teachers can access support materials (ask your sales representative for details).

■ Additional Resources for Teachers

The Principles of Computer Security: CompTIA Security+ and Beyond Online Learning Center (www.PrinciplesSecurity3e.com) provides many resources for instructors:

- Answer keys to the end-of-chapter activities in the textbook
- Answer keys to the lab manual activities
- Access to testbank files and software that allows you to generate a wide array of paper- or network-based tests, and that features automatic grading
- Hundreds of practice questions and a wide variety of question types and difficulty levels, enabling you to customize each test to maximize student progress
- Blackboard cartridges and other formats may also be available upon request; contact your sales representative
- Engaging PowerPoint slides on the lecture topics (including full-color artwork from the book)