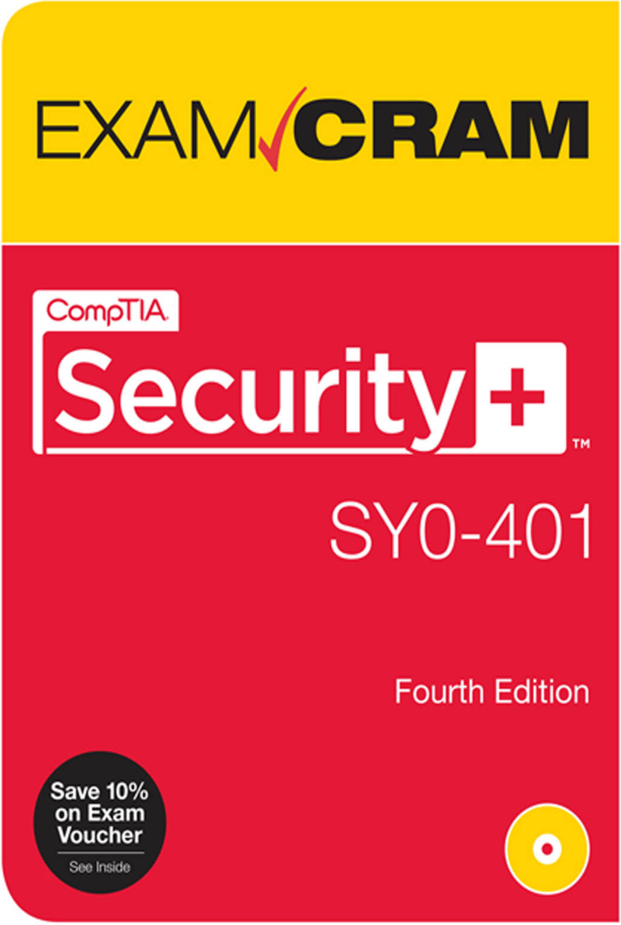

EXAM CRAM

CompTIA

Security+™

SY0-401

Fourth Edition

Save 10% on Exam Voucher
See Inside

PEARSON IT
CERTIFICATION

DIANE BARRETT
MARTIN WEISS
KIRK HAUSMAN

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

EXAM CRAM

CompTIA® Security+™

SY0-401

Fourth Edition

Diane Barrett,
Kalani K. Hausman,
Martin Weiss

800 East 96th Street, Indianapolis, Indiana 46240 USA

CompTIA® Security+™ SY0-401 Exam Cram, Fourth Edition

Copyright © 2015 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5334-2
ISBN-10: 0-7897-5334-0

Library of Congress Control Number: 2015930248

Printed in the United States of America

First Printing: February 2015

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Editor-in-Chief
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Keith Cline

Indexer
Erika Millen

Proofreader
Megan Wade-Taxter

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Media Producer
Lisa Matthews

Cover Designer
Alan Clements

Compositor
Studio Galou

Contents at a Glance

Introduction xxii

Part I: Network Security

CHAPTER 1 Secure Network Design 1
CHAPTER 2 Network Implementation 49

Part II: Compliance and Operational Security

CHAPTER 3 Risk Management 83
CHAPTER 4 Response and Recovery 143

Part III: Threats and Vulnerabilities

CHAPTER 5 Attacks 203
CHAPTER 6 Deterrents 261

Part IV: Application, Data, and Host Security

CHAPTER 7 Application Security 291
CHAPTER 8 Host Security 311
CHAPTER 9 Data Security

Part V: Access Control and Identity Management

CHAPTER 10 Authentication, Authorization, and Access Control 391
CHAPTER 11 Account Management 421

Part VI: Cryptography

CHAPTER 12 Cryptography Tools and Techniques 439
CHAPTER 13 Public Key Infrastructure 473
Practice Exam 1 491
Index 533

On the CD:

Practice Exam 2
Glossary

Contents

Introduction xxii

Part I: Network Security

CHAPTER 1 Secure Network Design 1

Implement Security Configuration Parameters on Network Devices and Other Technologies 2

- Firewalls 3
- Routers 4
- Switches 5
- Load Balancers 6
- Proxies 6
- Web Security Gateways 7
- VPN Concentrators 8
- NIDS and NIPS 8
- Protocol Analyzers 11
- Spam Filter 12
- UTM Security Appliances 12
- Web Application Firewall Versus Network Firewall 14
- Application-Aware Devices 15
- Cram Quiz 17
- Cram Quiz Answers 17

Given a Scenario, Use Secure Network Administration Principles 19

- Rule-Based Management 20
- Firewall Rules 20
- VLAN Management 21
- Secure Router Configuration 22
- Access Control Lists 23
- Port Security 23
- 802.1X 24
- Flood Guards 24
- Loop Protection 25
- Implicit Deny 25
- Network Separation 26
- Log Analysis 26
- Unified Threat Management 27

Cram Quiz 28
Cram Quiz Answers 28
Explain Network Design Elements and Components 30
DMZ 31
Subnetting. 32
VLAN 34
NAT 36
Remote Access 37
Telephony. 37
NAC 39
Virtualization. 40
Cloud Computing 41
Layered Security/Defense in Depth 44
Cram Quiz 45
Cram Quiz Answers 46
What Next? 47

CHAPTER 2 Network Implementation **49**

Given a Scenario, Implement Common Protocols and Services 50
Protocols. 51
Ports 65
OSI Relevance 67
Cram Quiz 68
Cram Quiz Answers 69
Given a Scenario, Troubleshoot Security Issues Related to Wireless Networking 70
WPA 71
WPA2 71
WEP 72
EAP 73
PEAP 73
LEAP 74
MAC Filter 74
Disable SSID Broadcast 75
TKIP 75
CCMP 76
Antenna Placement. 76

Power-Level Controls 77
Captive Portals 78
Antenna Types 78
Site Surveys 79
VPN (Over Open Wireless) 80
Cram Quiz 81
Cram Quiz Answers 81
What Next? 82

Part II: Compliance and Operational Security

CHAPTER 3 Risk Management 83

Explain the Importance of Risk-Related Concepts 84
Control Types 85
False Positives 85
False Negatives 86
Importance of Policies in Reducing Risk 86
Risk Calculation 90
Qualitative Versus Quantitative Measures 94
Vulnerabilities 94
Threat Vectors 95
Probability/Threat Likelihood 95
Risk-Avoidance, Transference, Acceptance, Mitigation, Deterrence 96
Risks Associated with Cloud Computing and Virtualization 96
Recovery Time Objective and Recovery Point Objective 97
Cram Quiz 99
Cram Quiz Answers 100
Summarize the Security Implications of Integrating Systems and Data with Third Parties 101
On-Boarding/Off-Boarding Business Partners 102
Social Media Networks and/or Applications 103
Interoperability Agreements 104
Privacy Considerations 105
Risk Awareness 106
Unauthorized Data Sharing 107
Data Ownership 108
Data Backups 108

Follow Security Policy and Procedures 109
Review Agreement Requirements to Verify Compliance and Performance Standards 110
Cram Quiz 111
Cram Quiz Answers 111
Given a Scenario, Implement Appropriate Risk Mitigation Strategies . . 113
Change Management 114
Incident Management 114
User Rights and Permissions Reviews 115
Perform Routine Audits 116
Enforce Policies and Procedures to Prevent Data Loss or Theft . . 117
Enforce Technology Controls 118
Cram Quiz 120
Cram Quiz Answers 120
Given a Scenario, Implement Basic Forensic Procedures 122
Order of Volatility 123
Capture System Image 124
Network Traffic and Logs 125
Capture Video 125
Record Time Offset 126
Take Hashes 127
Screenshots 127
Witnesses 128
Track Man-Hours and Expense 128
Chain of Custody 128
Big Data Analysis 130
Cram Quiz 132
Cram Quiz Answers 132
Summarize Common Incident Response Procedures 133
Preparation 134
Incident Identification. 135
Escalation and Notification 135
Mitigation Steps. 136
Lessons Learned 137
Reporting 137
Recovery/Reconstitution Procedures. 137
First Responder 138

Incident Isolation . . . 138
Data Breach . . . 139
Damage and Loss Control . . . 140
Cram Quiz . . . 141
Cram Quiz Answers . . . 141
What Next? . . . 142
CHAPTER 4 Response and Recovery . . . 143
Explain the Importance of Security-Related Awareness and Training . . 144
Security Policy Training and Procedures . . . 145
Role-Based Training . . . 147
Personally Identifiable Information . . . 147
Information Classification . . . 148
Public . . . 149
Data Labeling, Handling, and Disposal . . . 150
Compliance with Laws, Best Practices, and Standards . . . 150
User Habits . . . 151
New Threats and New Security Trends/Alerts . . . 152
Use of Social Networking and Peer-to-Peer Services . . . 153
Follow Up and Gather Training Metrics to Validate Compliance and Security Posture . . . 154
Cram Quiz . . . 155
Cram Quiz Answers . . . 156
Compare and Contrast Physical and Environmental Controls . . . 157
Environmental Controls . . . 157
Physical Security . . . 164
Control Types . . . 168
Cram Quiz . . . 171
Cram Quiz Answers . . . 172
Summarize Risk Management Best Practices . . . 173
Business Continuity Concepts . . . 174
Fault Tolerance . . . 180
Disaster Recovery Concepts . . . 185
Cram Quiz . . . 192
Cram Quiz Answers . . . 192
Given a Scenario, Select the Appropriate Control to Meet the Goals of Security . . . 194
Confidentiality . . . 194

Integrity . . . 196
Availability . . . 197
Safety . . . 198
Cram Quiz . . . 201
Cram Quiz Answers . . . 201
What Next? . . . 202

Part III: Threats and Vulnerabilities

CHAPTER 5 Attacks . . . 203
Explain Types of Malware . . . 204
Adware . . . 205
Viruses . . . 205
Worms . . . 207
Spyware . . . 207
Trojan Horses . . . 208
Rootkits . . . 209
Backdoors . . . 210
Logic Bombs . . . 210
Botnets . . . 211
Ransomware . . . 212
Polymorphic Malware . . . 213
Armored Virus . . . 213
Cram Quiz . . . 214
Cram Quiz Answers . . . 214
Summarize Various Types of Attacks . . . 215
Man-in-the-Middle . . . 216
Denial of Service . . . 216
Distributed DoS . . . 218
Replay . . . 220
DNS Poisoning . . . 220
ARP Poisoning . . . 221
Spoofing . . . 223
Spam . . . 224
Phishing and Related Attacks . . . 225
Privilege Escalation . . . 226
Malicious Insider Threat . . . 226
Transitive Access and Client-Side Attacks . . . 227

- Password Attacks . . . 227
- Typo Squatting/URL Hijacking . . . 230
- Watering Hole Attack . . . 231
- Cram Quiz . . . 232
- Cram Quiz Answers . . . 232

Summarize Social Engineering Attacks and the Associated Effectiveness with Each Attack . . . 234

- Social Engineering . . . 235
- Shoulder Surfing . . . 236
- Dumpster Diving . . . 237
- Tailgating . . . 238
- Impersonation . . . 238
- Hoaxes . . . 238
- Principles (Reasons for Effectiveness) . . . 239
- Cram Quiz . . . 241
- Cram Quiz Answers . . . 241

Explain Types of Wireless Attacks . . . 242

- Jamming/Interference . . . 243
- Rogue Access Points . . . 243
- War Driving . . . 244
- Bluejacking/Bluesnarfing . . . 244
- Packet Sniffing . . . 245
- WEP/WPA Attacks . . . 245
- WPS Attacks . . . 247
- Near-Field Communication . . . 247
- Cram Quiz . . . 249
- Cram Quiz Answers . . . 249

Explain Types of Application Attacks . . . 250

- Browser Threats . . . 251
- Code Injections . . . 252
- Directory Traversal . . . 253
- Header Manipulation . . . 253
- Zero-Day . . . 253
- Buffer Overflows . . . 254
- Integer Overflows . . . 255
- Cookies . . . 255
- Arbitrary/Remote Code Execution . . . 257

Cram Quiz . . . 258
Cram Quiz Answers . . . 258
What Next? . . . 259
CHAPTER 6 **Deterrents** . . . **261**
Analyze a Scenario and Select the Appropriate Type of Mitigation and Deterrent Techniques . . . 262
Monitoring System Logs . . . 263
Hardening . . . 266
Network Security . . . 268
Security Posture . . . 269
Reporting . . . 270
Detection Controls Versus Prevention Controls . . . 271
Cram Quiz . . . 273
Cram Quiz Answers . . . 273
Given a Scenario, Use Appropriate Tools and Techniques to Discover Security Threats and Vulnerabilities . . . 274
Interpret Results of Security Assessment Tools . . . 275
Tools . . . 275
Risk Calculation . . . 279
Assessment Technique . . . 280
Cram Quiz . . . 282
Cram Quiz Answers . . . 282
Explain the Proper Use of Penetration Testing Versus Vulnerability Scanning . . . 283
Penetration Testing . . . 284
Vulnerability Scanning . . . 285
Testing . . . 287
Cram Quiz . . . 288
Cram Quiz Answers . . . 288
What Next? . . . 289

Part IV: Application, Data, and Host Security

CHAPTER 7 **Application Security** . . . **291**
Explain the Importance of Application Security Controls and Techniques . . . 292
Fuzzing . . . 293
Secure Coding Concepts . . . 294

Cross-Site Scripting Prevention 298
Cross-Site Request Forgery Prevention 299
Application Configuration Baseline (Proper Settings) 301
Application Hardening 302
Application Patch Management 305
NoSQL Databases Versus SQL Databases 306
Server-Side Versus Client-Side Validation 306
Cram Quiz 308
Cram Quiz Answers 309
What Next? 310

CHAPTER 8 Host Security **311**

Summarize Mobile Security Concepts and Technologies 312
Device Security 313
Application Security 321
BYOD Concerns 324
Cram Quiz 330
Cram Quiz Answers 331
Given a Scenario, Select the Appropriate Solution to Establish Host Security 332
Operating System Security and Settings 333
OS Hardening 335
Anti-malware 336
Patch Management 339
White Listing Versus Black Listing Applications 342
Trusted OS 342
Host-Based Firewalls 342
Host-Based Intrusion Detection 344
Hardware Security 344
Host Software Baselining 346
Virtualization 347
Cram Quiz 350
Cram Quiz Answers 351
What Next? 352

CHAPTER 9 Data Security **353**

Implement the Appropriate Controls to Ensure Data Security 354
Cloud Storage 355

SAN . . . 357
Handling Big Data . . . 358
Data Encryption . . . 359
Hardware-Based Encryption Devices . . . 366
Data In-Transit, Data At-Rest, Data In-Use . . . 372
Permissions/ACL . . . 375
Data Policies . . . 376
Cram Quiz . . . 379
Cram Quiz Answers . . . 380
Compare and Contrast Alternative Methods to Mitigate Security Risks in Static Environments . . . 381
Environments . . . 382
Methods . . . 385
Cram Quiz . . . 389
Cram Quiz Answers . . . 389
What Next? . . . 390

Part V: Access Control and Identity Management

CHAPTER 10 Authentication, Authorization, and Access Control . . . 391
Compare and Contrast the Function and Purpose of Authentication Services . . . 393
RADIUS . . . 394
TACACS+ . . . 394
Kerberos . . . 395
LDAP . . . 397
XTACACS . . . 398
SAML . . . 398
Secure LDAP . . . 398
Cram Quiz . . . 399
Cram Quiz Answers . . . 399
Given a Scenario, Select the Appropriate Authentication, Authorization, or Access Control . . . 401
Identification Versus Authentication Versus Authorization . . . 402
Authorization . . . 402
Authentication . . . 407
Authentication Factors . . . 413
Identification . . . 413

Federation 416
Transitive Trust/Authentication 417
Cram Quiz 418
Cram Quiz Answers 419
What Next? 419

CHAPTER 11 Account Management 421

Install and Configure Security Controls When Performing Account Management, Based on Best Practices 422
Mitigate Issues Associated with Users with Multiple Account/Roles and/or Shared Accounts 423
Account Policy Enforcement 424
Group-Based Privileges 431
User-Assigned Privileges 432
User Access Reviews 433
Continuous Monitoring 433
Cram Quiz 435
Cram Quiz Answers 436
What Next? 437

Part VI: Cryptography

CHAPTER 12 Cryptography Tools and Techniques 439

Given a Scenario, Utilize General Cryptography Concepts 441
Symmetric Versus Asymmetric 442
Elliptic Curve and Quantum Cryptography 444
In-Band Versus Out-of-Band Key Exchange 445
Session Keys 445
Transport Encryption 447
Nonrepudiation and Digital Signatures 447
Hashing 449
Key Escrow 450
Steganography 450
Use of Proven Technologies 451
Cram Quiz 452
Cram Quiz Answers 452
Given a Scenario, Use Appropriate Cryptographic Methods 454
Wireless Encryption Functions 455

Cryptographic Hash Functions 456
HMAC 458
Symmetric Encryption Algorithms 458
Asymmetric Encryption Algorithms 460
One-Time Pads 462
PGP 462
Use of Algorithms with Transport Encryption 463
Cipher Suites 466
Key Stretching 468
Cram Quiz 469
Cram Quiz Answers 470
What Next? 471

CHAPTER 13 Public Key Infrastructure 473

Given a Scenario, Use Appropriate PKI, Certificate Management, and Associated Components 474
Public Key Infrastructure Standards 475
PKI 478
Certificate Policies 481
Public and Private Key Usage 483
Revocation 486
Trust Models 487
Cram Quiz 489
Cram Quiz Answers 490
What Next? 490

PRACTICE EXAM 1 491

Exam Questions 492
Answers at a Glance 512
Answers with Explanations 513

INDEX 533

On the CD:

Practice Exam 2
Glossary

About the Authors

Diane Barrett is the president of NextGard Technology and a professor for Bloomsburg University. She has done contract forensic and security assessment work for several years and has authored several other security and forensic books. She is a program director for ADFSL's Conference on Digital Forensics, Security, and Law; the DFCP certification chair for the Digital Forensic Certification Board; and a volunteer for the NIST Cloud Computing Forensic Science Challenges working group. She holds many industry certifications, including CISSP, ISSMP, DFCP, and PCME, along with several from CompTIA, including Security+. Diane's education includes a Ph.D. in business administration with a specialization in information security and a master of science degree in information technology with a specialization in information security.

Kalani Kirk Hausman is an author, GRC professional, enterprise and security architect, ISO, and consultant with experience that includes medium- to large-scale globally deployed networks in governmental, higher education, healthcare, and corporate settings. Kalani's professional certifications include the CISSP, CGEIT, CRISC, CISA, CISM, GIAC-GHSC, PMP, ITIL, and CCP. He is active within the InfraGard; Information Systems Audit and Control Association (ISACA); ISSA; and High Technology Crime Investigation Association (HTCIA). Kalani is currently employed at Texas A&M University and as an adjunct professor of InfoSec at UMUC and APU/AMU. Kalani can be reached at kkhausman@hotmail.com or followed on Twitter at @kkhausman.

Martin M. Weiss has years of experience in information security, risk management, and compliance. Marty holds a bachelor of science degree in computer studies from the University of Maryland University College and an MBA from the Isenberg School of Management at the University of Massachusetts Amherst. He holds several certifications, including CISSP, CISA, and Security+. Marty has authored and co-authored more than a half dozen books on information technology. Occasionally, he molds minds as an adjunct professor with the University of Maryland University College. A Florida native, he now lives in New England somewhere between Boston and New York City.

Dedication

To my husband, Bill, for his patience and understanding.

—Diane Barrett

To Susan and our wonderful children, Jonathan and Cassandra, who remind me of the joy present in the world.

—Kalani K. Hausman

This is for you Annie! Welcome!

From the 3rd edition: Vp,lyos drvitoyu l;id rcs, vts, drvpmf rfoyopm eo;; ntsrl yir vpfr 2521202 0861704 3330307 3251403

Solution: CompTIA Security+ Exam Cram second edition will break the code (keyboard shift cipher) To my future daughter (page;line;word).

—Martin Weiss

Acknowledgments

Publishing a book takes the collaboration and teamwork of many individuals. Thanks to everyone involved in this process from Waterside Productions and Pearson Education (and thanks to those who purchase this book in their quest for certification). Betsy, thanks for keeping us all on track. To our editorial and technical reviewers, especially Chris, thank you for making sure that our work was sound and on target. Special thanks to my coauthors, Marty and Kirk.

—Diane Barrett

Thanks to my agent Carole McClendon, to Betsy Brown, Ellie Bru, and the excellent editorial staff at Pearson. Special thanks go to my coauthors Martin Weiss and Diane Barrett, whose knowledge and dedication produced this remarkable text.

—Kalani K. Hausman

Once again, thank you to the entire team that worked together to get this book updated and published. Special thanks to the work and for the support from Ellie, Betsy, Chris, Tonya, and of course Kirk and Diane. Thank you to you, the reader, for your trust and for looking to us to help you pursue your security knowledge and quest for certification. Finally, I'd like to acknowledge my incredible friends and family.

—Martin Weiss

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill.

Certification demonstrates that you have the knowledge and skill to solve technical or business problems in virtually any business environment. CompTIA certifications are highly-valued credentials that qualify you for jobs, increased compensation, and promotion.

LEARN → CERTIFY → WORK

IT is Everywhere	IT Knowledge and Skills Get Jobs	Job Retention	New Opportunities	High Pay-High Growth Jobs
IT is mission critical to almost all organizations and its importance is increasing.	Certifications verify your knowledge and skills that qualifies you for:	Competence is noticed and valued in organizations.	Certifications qualify you for new opportunities in your current job or when you want to change careers.	Hiring managers demand the strongest skill set.
• 79% of U.S. businesses report IT is either important or very important to the success of their company	• Jobs in the high growth IT career field • Increased compensation • Challenging assignments and promotions • 60% report that being certified is an employer or job requirement	• Increased knowledge of new or complex technologies • Enhanced productivity • More insightful problem solving • Better project management and communication skills • 47% report being certified helped improve their problem solving skills	• 31% report certification improved their career advancement opportunities	• There is a widening IT skills gap with over 300,000 jobs open • 88% report being certified enhanced their resume

Certification Helps Your Career

- **Security is one of the highest demand job categories**—growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.
- **Jobs for security administrators are expected to increase by 18%**—the skill set required for these types of jobs maps to the 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.
- **More than ¼ million**—individuals worldwide are CompTIA Security+ certified.
- **CompTIA Security+ is regularly used in organizations**—such as Hitachi Systems, Fuji Xerox, HP, Dell, and a variety of major U.S. government contractors.
- **Approved by the U.S. Department of Defense (DoD)**—as one of the required certification options in the DoD 8570.01-M directive, for Information Assurance Technical Level II and Management Level I job roles.

Steps to Getting Certified and Staying Certified

Review Exam Objectives	Review the Certification objectives to make sure you know what is covered in the exam.http://certification.comptia.org/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, review and answer the sample questions to get an idea what type of questions might be on the exam. http://certification.comptia.org/samplequestions.aspx
Purchase an Exam Voucher	Purchase exam vouchers on the CompTIA Marketplace. www.comptiastore.com
Take the Test!	Go to the Pearson VUE website and schedule a time to take your exam. http://www.pearsonvue.com/comptia/
Stay Certified! **Continuing Education**	Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/ce

How to obtain more information

- **Visit CompTIA online**—http://certification.comptia.org/home.aspx to learn more about getting CompTIA certified.
- **Contact CompTIA**—call 866-835-8020 and choose Option 2 or email questions@comptia.org.
- **Connect with us**—

To receive your 10% off
Exam Voucher, register
your product at:

www.pearsonitcertification.com/register

and follow the instructions.

Introduction

Welcome to *CompTIA Security+ SY0-401 Exam Cram*, Fourth Edition. This book aims to help you get ready to take and pass the CompTIA Security+ exam, number SY0-401.

Chapters 1–13 are designed to remind you of everything you need to know to pass the SY0-401 certification exam. The two practice exams at the end of this book should give you a reasonably accurate assessment of your knowledge, and, yes, we've provided the answers and their explanations for these practice exams. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass CompTIA certification exams. Exam Cram books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

We strongly recommend that you spend some time installing, configuring, and working with the latest operating systems to patch and maintain them for the best and most current security possible because the Security+ exam focuses on such activities and the knowledge and skills they can provide for you. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but, without doubt, hands-on experience is the best teacher of all!

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take the Security+ exam is $293 USD for individuals ($226 for CompTIA members). CompTIA corporate members receive discounts on nonmember pricing. For more information about these discounts, a local CompTIA sales representative can provide answers to any questions you might have. If you don't pass, you can take the exam again for the same cost as the first attempt, for each attempt until you pass. In the United States and Canada, tests are administered by Prometric or VUE.

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. To be admitted into the testing room, you must supply two forms of identification, one of which must be a photo ID.

About This Book

We've structured the topics in this book to build on one another. Therefore, some topics in later chapters make the most sense after you've read earlier chapters. That's why we suggest that you read this book from front to back for your initial test preparation. If you need to brush up on a topic or if you have to bone up for a second try, you can use the index, table of contents, or Table I-1 to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference to some of the most important aspects of the Security+ certification.

Chapter Format and Conventions

Every Exam Cram chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- **Opening objectives list:** This defines the official CompTIA Security+ exam objectives covered in the chapter.
- **Cram Saver questions:** Each major section begins with a Cram Saver to help you determine your current level of knowledge of the topics in that section.
- **Topical coverage:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions geared to build your knowledge so that you can pass the exam.
- **Exam Alerts:** These are interspersed throughout the book. They include important information on test topics. Watch out for them!

ExamAlert

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more certification test questions.

- **Cram Quiz questions:** At the end of each topic is a quiz. The quizzes, and their explanations, are meant to gauge your knowledge of the subjects. If the answers to the questions don't come readily to you, consider reviewing the section.

Additional Elements

Beyond the chapters there are a few more elements:

- **Practice exams:** There are two practice exams. They are printed in the book and included with the Pearson IT Certification Practice Test Engine on the CD.
- **Cram Sheet:** The tear-out Cram Sheet is located right in the beginning of the book. This is designed to jam some of the most important facts you need to know for the exam into one small sheet, allowing for easy memorization.
- **Glossary:** Definitions of key CompTIA Security+ exam terms.

Exam Objectives

Table I-1 lists the skills measured by the SY0-401 exam and the chapter in which the objective is discussed. Some objectives are covered in other chapters, too.

TABLE I.1 **CompTIA SY0-401 Exam Objectives**

Exam Objective	Chapter
Domain 1: Network Security	
Implement security configuration parameters on network devices and other technologies	1
Given a scenario, use secure network administration principles	1
Explain network design elements and components	1

Exam Objective	Chapter
Given a scenario, implement common protocols and services	2
Given a scenario, troubleshoot security issues related to wireless networking	2
Domain 2: Compliance and Operational Security	
Explain the importance of risk related concepts	3
Summarize the security implications of integrating systems and data with third parties	3
Given a scenario, implement appropriate risk mitigation strategies	3
Given a scenario, implement basic forensic procedures	3
Summarize common incident response procedures	3
Explain the importance of security related awareness and training	4
Compare and contrast physical security and environmental controls	4
Summarize risk management best practices	4
Given a scenario, select the appropriate control to meet the goals of security	4
Domain 3: Threats and Vulnerabilities	
Explain types of malware	5
Summarize various types of attacks	5
Summarize social engineering attacks and the associated effectiveness with each attack	5
Explain types of wireless attacks	5
Explain types of application attacks	5
Analyze a scenario and select the appropriate type of mitigation and deterrent techniques	6
Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities	6
Explain the proper use of penetration testing versus vulnerability scanning	6
Domain 4: Application, Data, and Host Security	
Explain the importance of application security controls and techniques	7
Summarize mobile security concepts and technologies	8
Given a scenario, select the appropriate solution to establish host security	8
Implement the appropriate controls to ensure data security	9
Compare and contrast alternative methods to mitigate security risks in static environments	9
Domain 5: Access Control and Identity Management	
Compare and contrast the function and purpose of authentication services	10
Given a scenario, select the appropriate authentication, authorization or access control	10
Install and configure security controls when performing account management, based on best practices	11

Exam Objective	Chapter
Domain 6: Cryptography	
Given a scenario, utilize general cryptography concepts	12
Given a scenario, use appropriate cryptographic methods	12
Given a scenario, use appropriate PKI, certificate management and associated components	13

Pearson IT Certification Practice Test Engine and Questions on the CD

The CD in the back of the book includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and then activating the exam. The CD in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the CD.

Note

The cardboard CD case in the back of this book includes the CD and a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software from the CD

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows Virtual Machine, but it was built specifically for the PC platform. The minimum system requirements are the following:

- Windows XP (SP3), Windows Vista (SP2), or Windows 7
- Microsoft .NET Framework 4.0 Client
- Microsoft SQL Server Compact 4.0
- Pentium class 1GHz processor (or equivalent)

- 512MB RAM
- 650MB disc space plus 50MB for each downloaded practice exam

The software installation process is routine compared to other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the CD sleeve.

The following steps outline the installation process:

1. Insert the CD into your PC.
2. The software that automatically runs is the Pearson software to access and use all CD-based features. From the main menu, click the option to **Install the Exam Engine**.
3. Respond to windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

After the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate** button.
3. At the next screen, enter the activation key from the paper inside the cardboard CD holder in the back of the book. Once entered, click the **Activate** button.
4. The activation process will download the practice exam. Click **Next**, and then click **Finish.**

After you've completed the activation process, the My Products tab should list your new exam. If you do not see the exam, make sure you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Updating your exams ensures you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab and click the **Update Application** button. This ensures you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process and the registration process only has to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Pearson IT Certification Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the CD sleeve in the back of that book; you don't even need the CD at this point. From there, all you have to do is start the exam engine (if it is not still up and running) and perform steps 2–4 from the previous list.

Premium Edition

In addition to the free practice exams provided with your purchase, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the CD sleeve that contains a one-time-use code as well as instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to http://www.pearsonitcertification.com/store/product.aspx?isbn=0132939592.

This page intentionally left blank

CHAPTER 2

Network Implementation

This chapter covers the following official CompTIA Security+ SY0-401 exam objectives:

- Given a scenario, implement common protocols and services
- Given a scenario, troubleshoot security issues related to wireless networking

(For more information on the official CompTIA Security+ SY0-401 exam topics, see the “About the CompTIA Security+ SY0-401 Exam” section in the Introduction.)

The network infrastructure is subject to myriad internal and external attacks through services, protocols, and open ports. It is imperative that you understand how to properly implement services and protocols, especially if the network has been in existence for some period of time and some services are no longer needed or have been forgotten. To stop many would-be attackers, you must understand how protocols are used on the network, what common ports are used by network protocols, and how to securely implement a wireless network.

This chapter discusses these concepts to help you understand how to use the proper network implementation of protocols and services as a tool to protect and mitigate threats against network infrastructure based on organizational needs. It also has a section specifically dedicated to wireless security implementation based on organization requirements.

Given a Scenario, Implement Common Protocols and Services

- Protocols
- Ports
- OSI relevance

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Explain how IPsec is used, including the OSI model layer it operates on.
2. Explain what ICMP is and how it is used in a networking environment.
3. What are the major differences between IPv4 and IPv6?
4. Explain the purpose of ports 137, 138, and 139.
5. Explain what services/protocols operate on port 22.

Answers

1. The Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications. The use of IPsec can secure transmissions between critical servers and clients. This helps prevent attacks from taking place. Unlike most security systems that function within the application layer of the Open Systems Interconnection (OSI) model, IPsec functions within the network layer.
2. Internet Control Message Protocol (ICMP) is a protocol meant to be used as an aid for other protocols and system administrators to test for connectivity and search for configuration errors in a network. Ping uses the ICMP echo function and is the lowest-level test of whether a remote host is alive. A small packet containing an ICMP echo message is sent through the network to a particular IP address. The computer that sent the packet then waits for a return packet. If the connections are good and the target computer is up, the echo message return packet will be received.
3. The differences between IPv4 and IPv6 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices.
4. These are NetBIOS ports that are required for certain Windows network functions such as file sharing. But these ports also provide information about your computer that can be exploited by attackers. They also contain vulnerabilities that are widely used to break into systems and exploit them in various ways.

5. Secure Shell (SSH), Secure File Transfer Protocol (SFTP), and Secure Copy Protocol (SCP) are all protocols that operate on port 22. SSH is used to securely access a remote computer. SFTP is used for FTP access and encrypts both commands and data. SCP is used to securely transfer files to a remote host.

Protocols

Internet Protocol Security

The *Internet Protocol Security* (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications. The use of IPsec can secure transmissions between critical servers and clients. This helps prevent network-based attacks from taking place. Unlike most security systems that function within the application layer of the OSI model, IPsec functions within the network layer. IPsec provides authentication services and encapsulation of data through support of the Internet Key Exchange (IKE) protocol.

The asymmetric key standard defining IPsec provides two primary security services:

- **Authentication Header (AH):** This provides authentication of the data's sender, along with integrity and nonrepudiation. RFC 2402 states that AH provides authentication for as much of the IP header as possible, as well as for upper-level protocol data. However, some IP header fields might change in transit, and when the packet arrives at the receiver, the value of these fields might not be predictable by the sender. The values of such fields cannot be protected by AH. So, the protection provided to the IP header by AH is somewhat piecemeal.
- **Encapsulating Security Payload (ESP):** This supports authentication of the data's sender and encryption of the data being transferred along with confidentiality and integrity protection. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an antireplay service (a form of partial sequence integrity), and limited traffic-flow confidentiality. The set of services provided depends on options selected at the time of security association establishment and on the placement of the implementation. Confidentiality may be selected independently of all other services. However, the use of confidentiality without integrity/authentication (either in ESP or separately in AH) might subject traffic to certain forms of active attacks that could undermine the confidentiality service.

Protocols 51 and 50 are the AH and ESP components of the IPsec protocol. IPsec inserts ESP or AH (or both) as protocol headers into an IP datagram that immediately follows an IP header.

The protocol field of the IP header will be 50 for ESP or 51 for AH. If IPsec is configured to do authentication rather than encryption, you must configure an IP filter to let protocol 51 traffic pass. If IPsec uses nested AH and ESP, you can configure an IP filter to let only protocol 51 (AH) traffic pass.

IPsec supports the IKE protocol, which is a key management standard used to allow specification of separate key protocols to be used during data encryption. IKE functions within the Internet Security Association and Key Management Protocol (ISAKMP), which defines the payloads used to exchange key and authentication data appended to each packet.

The common key exchange protocols and standard encryption algorithms—including asymmetric key solutions such as the Diffie-Hellman Key Agreement and Rivest-Shamir-Adleman (RSA) standards; symmetric key solutions such as the International Data Encryption Algorithm (IDEA) and Digital Encryption Standard (DES); Triple DES (3DES) and hashing algorithms, such as the message digest 5 (MD5) and Secure Hash Algorithm (SHA)—are covered in detail in Chapter 12, "Cryptography Tools and Techniques."

Although IPsec by itself does not control access to the wireless local-area network (WAN), it can be used in conjunction with 802.1X to provide security for data being sent to client computers that are roaming between access points (AP) on the same network. For better security, segment the wireless network by placing a firewall between the WLAN and the remainder of the network. Because IPsec is a solution to securely authenticate and encrypt network IP packets, you can use IPsec to provide strong security between a Remote Authentication Dial-In User Service (RADIUS) server and a domain controller, or to secure traffic to a partner organization's RADIUS servers. RADIUS provides authentication and access control within an enterprise network and is explained in greater detail in Chapter 10, "Authentication, Authorization, and Access Control." Many of the VPN solutions use IPsec, and, like a virtual private network (VPN), IPsec is an excellent solution in many circumstances. However, it should not be a direct alternative for WLAN protection implemented at the network hardware layer.

Simple Network Management Protocol

Older protocols that are still in use might leave the network vulnerable. Protocols such as Simple Network Management Protocol (SNMP) and Domain Name Service (DNS) that were developed a long time ago and have been widely deployed can pose security risks, too. *SNMP* is an application layer protocol whose purpose is to collect statistics from TCP/IP devices. SNMP is used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPS). Many of the vulnerabilities associated with SNMP stem from using SNMPv1. Although these vulnerabilities were discovered in 2002, vulnerabilities are still being reported with current SNMP components. A recent Ubuntu Linux Security Advisory noted that vulnerabilities in Net-SNMP allow remote attackers to cause a denial of service.

The SNMP management infrastructure consists of three components:

- SNMP managed node
- SNMP agent
- SNMP network management station

The device loads the agent, which in turn collects the information and forwards it to the management station. Network management stations collect a massive amount of critical network information and are likely targets of intruders because SNMPv1 is not secure. The only security measure it has in place is its community name, which is similar to a password. By default, this is “public,” and many times is not changed, thus leaving the information wide open to intruders. SNMPv2 uses message digest 5 (MD5) for authentication. The transmissions can also be encrypted. SNMPv3 is the current standard, but some devices are likely to still be using SNMPv1 or SNMPv2.

SNMP can help malicious users learn a lot about your system, making password-guessing attacks a bit easier than brute-force attacks. SNMP is often overlooked when checking for vulnerabilities because it uses User Datagram Protocol (UDP) ports 161 and 162. Make sure that network management stations are secure physically and secure on the network. You might even consider using a separate management subnet and protecting it using a router with an access list. Unless this service is required, you should turn it off.

Secure Shell

As a more secure replacement for the common command-line terminal utility Telnet, the *Secure Shell* (SSH) utility establishes a session between the client and host computers using an authenticated and encrypted connection. SSH requires encryption of all data, including the login portion. SSH uses the asymmetric (public key) RSA cryptography method to provide both connection and authentication.

Data encryption is accomplished using one of the following algorithms:

- **Encryption Algorithm (IDEA):** The default encryption algorithm used by SSH, which uses a 128-bit symmetric key block cipher.
- **Blowfish:** A symmetric (private key) encryption algorithm using a variable 32- to 448-bit secret key.
- **Data Encryption Standard (DES):** A symmetric key encryption algorithm using a random key selected from a large number of shared keys. Most forms of this algorithm cannot be used in products meant for export from the United States.
- **Triple Data Encryption Standard (#DES):** A symmetric key encryption algorithm that dramatically improves upon the DES by using the DES algorithm three times with three distinct keys.

Using SSH helps guard against attacks such as eavesdropping, man-in-the-middle attacks, and spoofing. Attempts to spoof the identity of either side of a communication can be thwarted because each packet is encrypted using a key known only by the local and remote systems.

ExamAlert

Some versions of SSH, including the Secure Shell for Windows Server, provide a secure version of the File Transfer Protocol (SFTP) along with the other common SSH utilities.

Domain Name Service

Domain Name Service (DNS) was originally designed as an open protocol. DNS servers are organized in a hierarchy. At the top level of the hierarchy, root servers store the complete database of Internet domain names and their corresponding IP addresses. There are different types of DNS servers. The most common types are the following:

- **Authoritative servers:** Definitive for particular domains providing information about only those domains. An authoritative-only name server only returns answers to queries about domain names that have been specifically configured.
- **Caching servers:** Uses recursion to resolve a given name starting with the DNS root through to the authoritative name servers of the queried domain.

Internal DNS servers can be less susceptible to attacks than external DNS servers, but they still need to be secured. To stop outside intruders from accessing the internal network of your company, use separate DNS servers for internal and Internet name resolution. To provide Internet name resolution for internal hosts, you can have your internal DNS servers use a forwarder.

The following are some considerations for internal DNS servers:

- Eliminate any single point of failure by making sure that the structure is planned properly. Analyze where the clients of each DNS zone are located and how they will resolve names if the DNS server is unavailable.
- Prevent unauthorized access to your servers by implementing integrated zones with secure dynamic updates. Keep the list of DNS servers that are allowed to obtain a zone transfer small.
- Monitor the server events and DNS logs. Proper monitoring of logs and server events can help prevent unauthorized access as well as diagnose problems.

Transport Layer Security

Another asymmetric key encapsulation currently considered the successor to SSL is the Transport Layer Security (TLS) protocol, based on Netscape's Secure Sockets Layer 3.0 (SSL3) transport protocol, which provides encryption using stronger encryption methods, such as DES, or without encryption altogether if desired for authentication only. SSL and TLS transport are similar but not entirely interoperable. TLS also provides confidentiality and data integrity.

TLS has two layers of operation:

- **TLS Record Protocol:** This protocol allows the client and server to communicate using some form of encryption algorithm (or without encryption if desired).
- **TLS Handshake Protocol:** This protocol allows the client and server to authenticate one another and exchange encryption keys to be used during the session.

Secure Sockets Layer

Secure Sockets Layer (SSL) protocol communications occur between the HTTP (application) and TCP (transport) layers of Internet communications. SSL is used by millions of websites in the protection of their online transactions with their customers. SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. The SSL process uses certificates for authentication and encryption for message integrity and confidentiality. SSL establishes what is called a *stateful connection*. In a stateful connection, both ends set up and maintain information about the session itself during its life. This is different from a stateless connection, where there is no prior connection setup. The SSL stateful connection is negotiated by a handshaking procedure between client and server. During this handshake, the client and server exchange the specifications for the cipher that will be used for that session. SSL communicates using an asymmetric key with cipher strength of 40 or 128 bits.

SSL works by establishing a secure channel using public key infrastructure (PKI). This can eliminate a vast majority of attacks, such as session hijackings and information theft.

You can secure communications when performing administration on wireless access points (WAP) by leveraging protocols such as SSH or HTTP with SSL or TLS. A WAP can implement access control functions to allow or deny access to the network and provides the capability of encrypting wireless traffic. It also has the means to query an authentication and authorization service for authorization decisions and securely exchange encryption keys with the client to secure the network traffic.

As a general rule, SSL is not as flexible as IPsec from an application perspective but is more flexible for access from any location. One must determine the usage requirements for each class of user and determine the best approach.

Transmission Control Protocol/Internet Protocol

The core of TCP/IP consists of four main protocols: the Internet Protocol (IP), the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), and the Internet Control Message Protocol (ICMP). IP is responsible for providing essential routing functions for all traffic on a TCP/IP network. TCP provides connection-oriented communication. UDP provides connectionless communications. TCP connections are initiated and terminated with a three-way handshake process. ICMP provides administrative services to TCP/IP networks.

TCP/IP's implementation of the OSI model makes functionality simpler by mapping the same seven layers of the OSI model to a four-layer model instead. Unlike the OSI reference model, the TCP/IP model focuses more on delivering interconnectivity than on functional layers. It does this by acknowledging the importance of a structured hierarchical sequence of functions, yet leaves protocol designers flexibility for implementation. Table 2.1 compares the OSI and TCP/IP models.

TABLE 2.1 **OSI and TCP/IP Model Comparison**

OSI Reference Model	TCP/IP Reference Model
Application Presentation Session	Application
Transport	Transport
Network	Internet
Data link	Network access Physical

File Transfer Protocol Secure

FTP passes the username and password in a plain-text form, allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access to the server. *FTPS*, also known as *FTP Secure* and *FTP-SSL*, is an FTP extension that adds support for TLS and SSL. FTPS supports channel encryption as defined in RFC 2228.

With FTPS, data transfers take place in a way designed to allow both parties to authenticate each other and to prevent eavesdropping, tampering, and forgery on the messages exchanged. FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. It also supports compatible ciphers, including AES, RC4, RC2, Triple DES and DES, as well as hash functions SHA1, MD5, MD4, and MD2.

You should use FTPS when you need to transfer sensitive or confidential data between a client and a server that is configured to use SSL for secure transactions.

Secure variations of FTP ensure that data cannot be intercepted during transfer and allow the use of more secure transfer of user access credentials during FTP login. However, the same certificate vulnerabilities discussed earlier in this chapter apply here, too.

Hypertext Transport Protocol over Secure Sockets Layer

Basic web connectivity using Hypertext Transport Protocol (HTTP) occurs over TCP port 80, providing no security against interception of transacted data sent in clear text. An alternative to this involves the use of SSL transport protocols operating on port 443, which creates an encrypted pipe through which HTTP traffic can be conducted securely. To differentiate a call to port 80 (http://servername/), HTTP over SSL calls on port 443 using HTTPS as the URL port designator (https://servername/).

HTTP Secure (HTTPS) was originally created by the Netscape Corporation and used a 40-bit RC4 stream encryption algorithm to establish a secured connection encapsulating data transferred between the client and web server, although it can also support the use of X.509 digital certificates to allow the user to authenticate the sender. Now, 256-bit encryption keys have become the accepted level of secure connectivity for online banking and electronic commerce transactions.

ExamAlert

An alternative to HTTPS is the Secure Hypertext Transport Protocol (S-HTTP), which was developed to support connectivity for banking transactions and other secure web communications. S-HTTP supports DES, 3DES, RC2, and RSA2 encryption, along with Challenge Handshake Authentication Protocol (CHAP) authentication but was not adopted by the early web browser developers (for example, Netscape and Microsoft) and so remains less common than the HTTPS standard.

Although HTTPS encrypts communication between the client and server, it does not guarantee that the merchant is trustworthy or that the merchant's server is secure. SSL/TLS is designed to positively identify the merchant's server and encrypt communication between the client and server.

Secure Copy Protocol

The *Secure Copy Protocol* (SCP) is a network protocol that supports file transfers. SCP is a combination of RCP and SSH. It uses the BSD RCP protocol tunneled through the SSH protocol to provide encryption and authentication. The RCP performs the file transfer, and the SSH protocol performs authentication and encryption. SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit. It thwarts the ability for packet sniffers to extract information from data packets.

An SCP download request is server driven, which imposes a security risk when connected to a malicious server. SCP has been mostly superseded by the more comprehensive SFTP, and some implementations of the SCP utility actually use SFTP instead.

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is a protocol meant to be used as an aid for other protocols and system administrators to test for connectivity and search for configuration errors in a network. Ping uses the ICMP echo function and is the lowest-level test of whether a remote host is alive. A small packet containing an ICMP echo message is sent through the network to a particular IP address. The computer that sent the packet then waits for a return packet. If the connections are good and the target computer is up, the echo message return packet will be received. It is one of the most useful network tools available because it tests the most basic function of an IP network. It also shows the Time To Live (TTL) value and the amount of time it takes for a packet to make the complete trip, also known as *round-trip time* (RTT), in milliseconds (ms). One caveat with using ICMP: It can be manipulated by malicious users, so some administrators block ICMP traffic. If that is the case, you will receive a request timeout even though the host is available.

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute outputs the list of traversed routers in simple text format, together with timing information. Traceroute is available on most operating systems. On Microsoft Windows operating systems, it is named tracert. Traceroute uses an ICMP echo request packet to find the path. It sends an echo reply with the TTL value set to 1. When the first router sees the packet with TTL 1, it decreases it by 1 to 0 and discards the packet. As a result, it sends an ICMP Time Exceeded message back to the source address. The source address of the ICMP error message is the first router address. Now the source knows the address of the first router. Generally, three packets are sent at each TTL, and the RTT is measured for each one. Most implementations of traceroute keep working until they have gone 30 hops, but this can be extended up to 254 routers.

Pathping is a Windows route-tracing tool that combines features of the ping and tracert commands with additional information. The command uses traceroute to identify which routers are on the path. When the traceroute is complete, pathping sends pings periodically to all the routers over a given time period and computes statistics based on the number of packets returned from each hop. By default, pathping pings each router 100 times, with a single ping every 0.25 seconds. Consequently, a default query requires 25 seconds per router hop. This is especially helpful in identifying routers that cause delays or other latency problems on a connection between two IP hosts.

IPv4

IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it ensure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper-layer transport protocol, such as TCP. IPv4 currently routes the majority of Internet traffic. IPv4 is widely used in both internal and external networks throughout the world.

IPv4 is susceptible to ping sweeps, port scans, and application and vulnerability scans. To mitigate sweeps and scans, filtering messages or traffic types is an acceptable solution because it is impossible to eliminate reconnaissance activity.

IPv6

Because of the increased demand of devices requiring IP addresses, IPv4 could not keep up with such an expansive demand. As a result, a new method was needed to address all the new devices requiring IP addresses. The Internet Engineering Task Force (IETF) published a new standard for IP addresses in RFC 2460. The new standard, *IPv6*, makes several changes to the older IPv4 standard. IPv6 increases the address size from IPv4 32 bits to 128 bits.

The differences between IPv6 and IPv4 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices. Table 2.2 provides a comparison of some of the differences between IPv4 and IPv6.

TABLE 2.2 **IPv4 and IPv6 Comparison**

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length.	Addresses are 128 bits (16 bytes) in length.
Header includes a checksum and options.	Header does not include a checksum, and all optional data is moved to IPv6 extension headers.
ARP uses broadcast request frames to resolve an IP address to a link-layer address.	Multicast Neighbor Solicitation messages are used to resolve IP addresses to link-layer addresses.
IPv4 header does not identify packet flow for quality of service (QoS).	IPv6 header identifies packet flow for QoS.

IPv4	IPv6
IPsec support is optional.	IPsec support is required.
IPv4 limits packets to 64 KB of payload.	IPv6 has optional support for jumbograms, which can be as large as 4 GB.
Must be configured either manually or through Dynamic Host Configuration Protocol (DHCP).	Does not require manual configuration or DHCP.

In addition to the difference in the address structure in IPv6, there are IPv6 versions of protocols and commands. The following are some of the more prevalent ones:

- **DHCPv6:** Provides stateful address configuration or stateless configuration settings to IPv6 hosts.
- **EIGRPv6:** Enhanced Interior Gateway Routing Protocol (EIGRP) is a routing protocol that was developed by Cisco. EIGRPv6 runs on IPv6 networks. It operates in the same manner as the IPv4 version, except that is routes IPv6 addresses.
- **ICMPv6:** Used by IPv6 nodes to report packet processing errors and diagnostics.
- **Pingv6:** Used in the same capacity as Ping except for IPv6 addresses. On Windows-based machines, is used, and on Linux/UNIX-based machines is used.

Internet Small Computer System Interface

Internet Small Computer System Interface (iSCSI) is an IP-based storage networking standard for linking data storage facilities. iSCSI is used for faster data transfers over intranets and handling remote storage access mainly in local-area networks (LAN) and WANs. It can be used in cloud environments as well, allowing remote resources to appear as local.

Businesses choose iSCSI because of ease of installation, cost, and utilization of current Ethernet networks. iSCSI clients or initiators send SCSI commands to SCSI targets on remote servers to communicate. iSCSI typically uses TCP port 860, with the target service using port 3260. iSCSI uses IPsec for protection. IPsec provides greater levels of security and integrity, as mentioned earlier in this section.

Fibre Channel

Fibre Channel (FC) is a gigabit network technology predominantly used to link data storage facilities or a storage-area network (SAN). FC is similar to iSCSI, but requires a Fibre Channel infrastructure. An FC infrastructure generally is more costly and complex to manage due to the separate network switching infrastructure. FC uses the Fibre Channel Protocol (FCP) to transport SCSI commands over the network consisting of ports and fabric. FC allows devices to attach through an interconnected switching system called a *fabric*. An FC port is not the same thing as computer port or network port. It is the node path performing data communications over the channel. The fiber may attach to a node port (N_Port) and to a port of the fabric (F_Port).The FC port manages a point-to-point connection between itself and the fabric.

FC network protection is primarily security through obscurity because direct access to the FC network is not available to most users, but this does not eliminate the need for security. Approved in 2004, the Fibre Channel Security Protocols standard (FC-SP) specifies how to protect against security breaches. This standard defines protocols for authentication, session keys, integrity and confidentiality, and policy implementation across an FC fabric. Basic FC security occurs through authentication and access control. To secure FC, authentication between FC devices and other devices with whom they communicate can be established using mutual authentication. Proper access control can be achieved through port locking, hard zoning, logical unit number (LUN) masking, and using secure management interfaces and protocols.

Fiber Channel over Ethernet

Fiber Channel over Ethernet (FCoE) is similar in concept to FC except that it allows Ethernet as a method of linking devices to storage. FC traffic runs over an Ethernet infrastructure by encapsulating FC over the Ethernet portions of the connectivity, allowing FC to run alongside IP traffic. FC traffic is used for the server applications, FC SAN, and FC storage. Because FCoE allows FC to be carried over Ethernet, the amount of equipment required in the data center can be reduced. FCoE uses a converged network adapter (CNA), lossless Ethernet links, and an FCoE switch.

Organizations often choose FCoE to maintain or evolve their existing FC network. SAN basic security flaws include weaknesses with authentication and authorization. FCoE can be secured in the manners suggested for FC but also includes control-plane protection and data-plane protection. Control-plane protection is access protection for the switches. Data-plane protection is security for traffic passing through the switches.

File Transfer Protocol

File Transfer Protocol (FTP) servers provide user access to upload or download files between client systems and a networked FTP server. FTP servers include many potential security issues, including anonymous file access and unencrypted authentication. Many FTP servers include the ability for anonymous access in their default installation configuration. Anonymous access is a popular method to provide general access to publicly available information. The problem with this form of access is that any user may download (and potentially upload) any file desired. This might result in a server's available file storage and network access bandwidth being rapidly consumed for purposes other than those intended by the server's administrator. If unauthorized file upload is allowed along with download, illegal file content could be placed on the server for download, without the knowledge of the system's administrator.

Even when user authentication is required, FTP passes the username and password in an unencrypted (plain-text) form, allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access. To mitigate FTP vulnerabilities, actions such as disabling anonymous access, hardening access control lists (ACL), enabling logging and disk quotas, setting access restrictions by IP, and enabling "blind" puts can be implemented. Using more secure variations of FTP ensures that data cannot be intercepted during transfer and allows the use of more secure transfer of user access credentials during FTP login.

Secure File Transfer Protocol

Secure File Transfer Protocol (SFTP), or Secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. It is functionally similar to FTP, but because it uses a different protocol, you cannot use a standard FTP client to talk to an SFTP server, nor can you connect to an FTP server with a client that supports only SFTP.

ExamAlert

A more secure version of FTP (SFTP) has been developed that includes SSL encapsulation. This version is referred to as FTP over SSH and uses the SSH TCP port 22. Do not confuse it with FTPS (FTP over SSL), which uses TCP ports 989 and 990. Either may be used within a modern enterprise network.

Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is a simple version of FTP used for transferring files between network devices. TFTP uses UDP port 69, has no login feature, and because it is implemented using UDP generally works only on LANs. TFTP works with either Bootstrap Protocol (BOOTP) or DHCP.

Because of the lack of security in TFTP, it is a good idea to place the TFTP server behind a firewall on an isolated LAN that only the essential equipment can reach.

Telnet

Telnet is a terminal emulation program used to access remote routers and UNIX systems. Telnet can be used as a tool to determine whether the port on a host computer is working properly. Telnet passes the username, password, and even transacted data in an unencrypted form (clear text), allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access to the server. Telnet-type clear-text connections create the ideal situation for TCP hijacking and man-in-the-middle attacks. Methods for mitigating Telnet vulnerabilities include using enhanced encryption or authentication security such as Kerberos, IPsec, SSH, SSL, or Cisco Secure Telnet.

Hypertext Transport Protocol

Hypertext Transfer Protocol (HTTP) allows users to connect to sources of information, services, products, and other functionality through the Internet. Business transactions, membership information, vendor/client communications, and even distributed business logic transactions can all occur though HTTP using basic Internet connectivity on TCP port 80.

An HTTP message contains a header and a body. The message header of an HTTP request has a request line and a collection of header fields. All HTTP messages must include the protocol version. Some HTTP messages can contain a content body, which is optional. The original HTTP specification has little support for the security mechanisms appropriate for today's Internet transactions. Methods for mitigating HTTP vulnerabilities include using enhanced encryption or authentication security HTTPS or SSL.

NetBIOS

Network Basic Input/Output System (NetBIOS) is an application programming interface (API) providing various networking services. NetBIOS provides name, datagram, and session services, allowing applications on different computers to communicate within a LAN. The session mode establishes a connection and provides error detection. The datagram mode is connectionless and supports LAN broadcast. NetBIOS is most commonly found in use with Microsoft Windows operating systems. Because it does not support routing, NetBIOS must be used with another transport mechanism such as TCP when it is implemented in an organization that has a WAN.

Ports

There are 65,535 TCP and UDP ports on which a computer can communicate. The port numbers are divided into three ranges:

- **Well-known ports:** The well-known ports are those from 0 through 1,023.
- **Registered ports:** The registered ports are those from 1,024 through 49,151.
- **Dynamic/private ports:** The dynamic/private ports are those from 49,152 through 65,535.

Often, many of these ports are not secured and, as a result, are used for exploitation. Table 2.3 lists some of the most commonly used ports and the services and protocols that use them. Many of these ports and services have vulnerabilities associated with them. It is important that you know what common ports are used by network protocols and how to securely implement services on these ports.

ExamAlert

Know the difference between the various ports that are used for network services and protocols.

TABLE 2.3 **Commonly Used Ports**

Port	Service/Protocol
15	Netstat
20	FTP-Data transfer
21	FTP-Control (command)
22	SSH/SFTP/SCP

Port	Service/Protocol
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP3
137, 138, 139	NetBIOS
143	IMAP
161/162	SNMP
443	HTTPS
445	SMB
989/990	FTPS
1,812	RADIUS
3389	RDP

Table 2.3 includes a list of protocols that may be currently in use on a network. These protocols, along with some older or antiquated protocols, may be configured open by default by the machine manufacturer or when an operating system is installed. Every operating system requires different services for it to operate properly. If ports are open for manufacturer-installed tools, the manufacturer should have the services listed in the documentation. Ports for older protocols such as Chargen (port 19) and Telnet (port 23) may still be accessible. For example, Finger, which uses port 79, was widely used during the early days of Internet, and today's sites no longer offer the service. However, you might still find some old implementations of Eudora mail that use the Finger protocol, or worse, the mail clients have long since been upgraded, but the port used 10 years ago was somehow left open. The quickest way to tell which ports are open and which services are running is to do a Netstat on the machine. You can also run local or online port scans.

The best way to protect the network infrastructure from attacks aimed at antiquated or unused ports and protocols is to remove any unnecessary protocols and create access control lists to allow traffic on necessary ports only. By doing so, you eliminate the possibility of unused and antiquated protocols being exploited and minimize the threat of an attack.

OSI Relevance

You should be very familiar with the OSI model as well as the common protocols and network hardware that function within each level. For example, you should know that hubs operate at the physical layer of the OSI model. Intelligent hubs, bridges, and network switches operate at the data link layer, and Layer 3 switches and routers operate at the network layer. The Network+ Exam Cram and Exam Prep books cover the OSI model in much more detail. If you will be working extensively with network protocols and hardware, you should also look at these texts.

The layers of the OSI model are as follows:

7. Application layer
6. Presentation layer
5. Session layer
4. Transport layer
3. Network layer
2. Data link layer (subdivided into the Logical-Link Control [LLC] and Media Access Control [MAC] sublayers)
1. Physical layer

Most applications, like web browsers or email clients, incorporate functionality of the OSI layers 5, 6, and 7.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is the correct address size for IPv6 addresses?

   ○ **A.** 32 bit

   ○ **B.** 64 bit

   ○ **C.** 128 bit

   ○ **D.** 256 bit

2. Which of the following protocols runs on port 22 and protects the authenticity and confidentiality of file transfer data in transit?

   ○ **A.** DHCP

   ○ **B.** SSL

   ○ **C.** FTP

   ○ **D.** SCP

3. You are troubleshooting connectivity issues on the network. Which of the following would be most helpful in determining where the connectivity issues lie?

   ○ **A.** SNMP

   ○ **B.** ICMP

   ○ **C.** SSL

   ○ **D.** IPsec

4. You want to be sure that the NetBIOS ports that are required for certain Windows network functions have been secured. Which of the following ports would you check?

   ○ **A.** 25/110/143

   ○ **B.** 161/162

   ○ **C.** 137/138/139

   ○ **D.** 20/21

5. Your company is in the process of setting up a management system on your network, and you want to use SNMP. You have to allow this traffic through the router. Which UDP ports do you have to open? (Choose two correct answers.)

   ○ **A.** 161

   ○ **B.** 139

   ○ **C.** 138

   ○ **D.** 162

6. Which standard port is used to establish a web connection using the 40-bit RC4 encryption protocol?
   - ○ **A.** 21
   - ○ **B.** 80
   - ○ **C.** 443
   - ○ **D.** 8,250

Cram Quiz Answers

1. **C**. IPv6 increases the address size from IPv4 32 bits to 128 bits. Answers A, B, and D are incorrect because IPv6 addresses sizes are 128 bit.
2. **D**. SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit. Answer A is incorrect because DHCP is used to automatically assign IP addresses. Answer B is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. The standard port for SSL is port 443. Answer C is incorrect because in FTP the data is not protected.
3. **B**. Traceroute uses an ICMP echo request packet to find the path between two addresses. Answer A is incorrect because SNMP is an application layer protocol whose purpose is to collect statistics from TCP/IP devices. SNMP is used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPS). Answer C is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. Answer D is incorrect because IPsec authentication and encapsulation standard is widely used to establish secure VPN communications.
4. **C**. There are NetBIOS ports that are required for certain Windows network functions, such as file sharing, which are 137, 138, and 139. Answer A is incorrect because these ports are used for email. Answer B is incorrect because these ports are used for SNMP. Answer D is incorrect because these ports are used for FTP.
5. **A** and **D**. UDP ports 161 and 162 are used by SNMP. Answer B is incorrect because UDP port 139 is used by the NetBIOS session service. Answer C is incorrect because port 138 is used to allow NetBIOS traffic for name resolution.
6. **C**. A connection using HTTPS is made using the RC4 cipher and port 443. Answer A is incorrect because port 21 is used for FTP connections. Answer B is incorrect because port 80 is used for unsecure plain-text HTTP communications. Answer D is incorrect because port 8,250 is not designated to a particular TCP/IP protocol.

Given a Scenario, Troubleshoot Security Issues Related to Wireless Networking

- **WPA**
- **WPA2**
- **WEP**
- **EAP**
- **PEAP**
- **LEAP**
- **MAC filter**
- **Disable SSID broadcast**
- **TKIP**
- **CCMP**
- **Antenna placement**
- **Power-level controls**
- **Captive portals**
- **Antenna types**
- **Site surveys**
- **VPN (over open wireless)**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Explain the difference between PEAP and LEAP.
2. Explain how to improve the security of wireless networks with regard to SSIDs.
3. Explain what CCMP is.

Answers

1. PEAP provides several benefits within TLS, including an encrypted authentication channel, dynamic keying material from TLS, fast reconnect using cached session keys, and server authentication that protects against the setting up of unauthorized access points. LEAP is a proprietary EAP method because it requires the use of a Cisco AP. It features mutual authentication, secure session key derivation, and dynamic per-user, per-session WEP keys.

2. To improve the security of your network, change the SSID. Using the default SSID poses a security risk even if the AP is not broadcasting it. When changing default SSIDs, do not change the SSID to reflect your company's main names, divisions, products, or address. Turning off SSID broadcast does not effectively protect the network from attacks.
3. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local-area networks (WLAN). CCMP uses 128-bit keys with a 48-bit initialization vector (IV) that reduces vulnerability to replay attacks.

WPA

Wireless security comes in two major varieties: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Both include methods to encrypt wireless traffic between wireless clients and WAPs. WEP has been included in 802.11–based products for some time and includes a strategy for restricting network access and encrypting network traffic based upon a shared key. The Wi-Fi Protected Access (WPA and WPA2) standards were developed by the Wi-Fi Alliance to replace the WEP protocol. WPA was developed after security flaws were found in WEP. WPA protects networks by incorporating a set of enhanced security features. WPA-protected networks require users to enter a passkey to access a wireless network. There are two different modes of WPA: WPA-PSK (Personal Shared Key) mode and WPA-802.1X mode, which is more often referred to as WPA-RADIUS or WPA-Enterprise. For the PSK mode, a passphrase consisting of 8 to 63 ASCII characters is all that is required. The Enterprise mode requires the use of security certificates. WPA includes many of the functions of the 802.11i protocol but relies on Rivest Cipher 4 (RC4), which is considered vulnerable to keystream attacks.

WPA2

WPA2 is based on the IEEE 802.11i standard and provides government-grade security by implementing the AES encryption algorithm and 802.1X-based authentication. AES is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. WPA2 incorporates stricter security standards and is configurable in either the PSK or Enterprise mode. There are two versions of WPA2: WPA2-Personal and WPA2-Enterprise. WPA2-Personal protects unauthorized network access via a password. WPA2-Enterprise verifies network users through a server.

WPA2 is backward compatible with WPA and supports strong encryption and authentication for both infrastructure and ad hoc networks. In addition, it has support for the CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) encryption mechanism based on the Advanced Encryption Standard (AES) cipher as an alternative to the Temporal Key Integrity Protocol (TKIP). TKIP is an encryption protocol included as part of the IEEE 802.11i standard for WLANs. An AES-based encryption mechanism that is stronger than TKIP.

WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used on 802.11-based wireless networks to provide privacy of data sent between a wireless client and its AP. Originally, many wireless networks were based on the IEEE 802.11 standard, which had serious data transmission security shortcomings. When this standard was put into place, the 802.11 committee adopted an encryption protocol called *WEP*. To discuss WEP's shortcomings, we have to understand how it operates. WEP uses a stream cipher for encryption called *RC4*. RC4 uses a shared secret key to generate a long sequence of bytes from what is called a *generator*. This stream is then used to produce the encrypted ciphertext. Early 802.11b networks used 40-bit encryption because of government restrictions. Hackers can crack a 40-bit key in a few hours. It is much easier to break RC4 encryption if a second instance of encryption with a single key can be isolated. In other words, the weakness is that the same keys are used repeatedly. Specifications for the WEP standard are detailed within the 802.11b (Wi-Fi) specification. This specification details a method of data encryption and authentication that may be used to establish a more secured wireless connection.

ExamAlert

Developments in the field of cryptography revealed the WEP encryption method to be less secure than originally intended and vulnerable to cryptographic analysis of network traffic. More advanced protocols such as WPA2 and the 802.11i standard supersede WEP, but recommendations for a more secure wireless network may also include the use of IPsec and VPN connectivity to tunnel data communications through a secured connection.

Although using WEP is much better than no encryption at all, it's important to understand its limitations so that you have an accurate picture of the consequences and what you must do to properly protect your wireless environment.

EAP

The *802.1X standard* is a means of wireless authentication. The 802.1X authentication standard is an extension of point-to-point protocol (PPP) that relies on the Extensible Authentication Protocol (EAP) for its authentication needs. EAP is a challenge-response protocol that can be run over secured transport mechanisms. It is a flexible authentication technology and can be used with smart cards, one-time passwords, and public key encryption. It also allows for support of public certificates deployed using auto enrollment or smart cards. These security improvements enable access control to Ethernet networks in public places such as malls and airports. EAP-Transport Layer Security (EAP-TLS) uses certificate-based mutual authentication, negotiation of the encryption method, and encrypted key determination between the client and the authenticating server.

EAP messages are encapsulated into 802.1X packets and are marked as EAP over LAN (EAPOL). After the client sends a connection request to a wireless AP, the authenticator marks all initial communication with the client as unauthorized, and only EAPOL messages are accepted while in this mode. All other types of communication are blocked until credentials are verified with an authentication server. Upon receiving an EAPOL request from the client, the wireless AP requests login credentials and passes them on to an authentication server. Remote Authentication Dial-In User Service (RADIUS) is usually employed for authentication purposes; however, 802.1X does not make it mandatory.

PEAP

Protected EAP (PEAP) was co-developed by Cisco, Microsoft Corporation, and RSA Security, Inc. PEAP provides several additional benefits within TLS, including an encrypted authentication channel, dynamic keying material from TLS, fast reconnect using cached session keys, and server authentication that protects against the setting up of unauthorized access points. PEAP is a means of protecting another EAP method (such as MS-CHAPv2) within a secure channel. The use of PEAP is essential to prevent attacks on password-based EAP methods. As part of the PEAP negotiation, the client establishes a TLS session with the RADIUS server. Using a TLS session as part of PEAP serves a number of purposes:

- It allows the client to authenticate the RADIUS server; this means that the client only establishes the session with a server holding a certificate that is trusted by the client.

- It protects the MS-CHAPv2 authentication protocol against packet snooping.
- The negotiation of the TLS session generates a key that can be used by the client and RADIUS server to establish common master keys. These keys are used to derive the keys used to encrypt the WLAN traffic.

Secured within the PEAP channel, the client authenticates itself to the RADIUS server using the MS-CHAPv2 EAP protocol. During this exchange, the traffic within the TLS tunnel is visible only to the client and RADIUS server and is never exposed to the WAP.

LEAP

Lightweight Extensible Authentication Protocol (LEAP) combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys. LEAP was developed by Cisco for use on WLANs that use Cisco 802.11 wireless devices. LEAP is a proprietary EAP method because it requires the use of a Cisco AP. It features mutual authentication; secure session key derivation; and dynamic per-user, per-session WEP keys. However, because it uses unencrypted challenges and responses, LEAP is vulnerable to dictionary attacks. Still, when LEAP is combined with a rigorous user password policy, it can offer strong authentication security without the use of certificates. LEAP can only authenticate the user to the WLAN, not the computer. Without computer authentication, machine group policies will not execute correctly.

MAC Filter

Most wireless network routers and access points can filter devices based on their Media Access Control (MAC) address. The MAC address is a unique identifier for network adapters. *MAC filtering* is a security access control method whereby the MAC address is used to determine access to the network. When MAC address filtering is used, only the devices with MAC addresses configured in the wireless router or access point are allowed to connect. MAC filtering permits and denies network access through the use of blacklists and whitelists. A *blacklist* is a list of MAC addresses that are denied access. A *whitelist* is a list of MAC addresses that are allowed access. Blacklisting and whitelisting are discussed in further detail in Chapter 8, “Host Security.”

While giving a wireless network some additional protection, it is possible to spoof the MAC address. An attacker could potentially capture details about a MAC address from the network and pretend to be that device in order to connect. MAC filtering can be circumvented by scanning a valid MAC using a tool such as airodumping and then spoofing one's own MAC into a validated MAC address. After an attacker knows a MAC address that is out of the blacklist or within the whitelist, MAC filtering is almost useless.

Disable SSID Broadcast

A *service set identifier* (SSID) is used to identify WAPs on a network. The SSID is transmitted so that wireless stations searching for a network connection can find it. By default, SSID broadcast is enabled. This means that it accepts any SSID. When you disable this feature, the SSID configured in the client must match the SSID of the AP; otherwise, the client does not connect to the AP. Having SSID broadcast enabled essentially makes your AP visible to any device searching for a wireless connection.

To improve the security of your network, change the SSIDs on your APs. Using the default SSID poses a security risk even if the AP is not broadcasting it. When changing default SSIDs, do not change the SSID to reflect your company's main names, divisions, products, or address. This just makes you an easy target for attacks such as war driving and war chalking. *War driving* is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or other mobile device. *War chalking* is the drawing of symbols in public places to advertise an open Wi-Fi network. Keep in mind that if an SSID name is enticing enough, it might attract hackers.

Turning off SSID broadcast does not effectively protect the network from attacks. Tools such as Kismet enable nonbroadcasting networks to be discovered almost as easily as broadcasting networks. From a security standpoint, it is much better to secure a wireless network using protocols that are designed specifically to address wireless network threats than to disable SSID broadcast.

ExamAlert

Turning off SSID broadcast does not effectively protect the network from attacks. It is much better to secure a wireless network using protocols that are designed specifically to address wireless network threats than to disable SSID broadcast.

TKIP

Temporal Key Integrity Protocol (TKIP) is the security protocol designed to replace WEP and is also known by its later iterations of *Wi-Fi Protected Access*

(WPA) or *WPA2*. Similar to WEP, TKIP uses the RC4 algorithm and does not require an upgrade to existing hardware, whereas more recent protocols, such as CCMP, which use the AES algorithm, do require an upgrade. TKIP was designed to provide more secure encryption than WEP by using the original WEP programming, but it wraps additional code at the beginning and end to encapsulate and modify it. To increase key strength, TKIP includes four additional algorithms: a cryptographic message integrity check, an IV sequencing mechanism, a per-packet key-mixing function, and a rekeying mechanism.

TKIP is useful for upgrading security on devices originally equipped with WEP, but does not address all security issues and might not be reliable enough for sensitive transmission. AES is a better choice and has become the accepted encryption standard for WLAN security.

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for WLANs. CCMP offers enhanced security compared with similar technologies such as TKIP. AES is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The AES cipher suite uses the Counter-Mode Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol (CCMP) as defined in RFC 3610. CCMP uses 128-bit keys with a 48-bit IV that reduces vulnerability to replay attacks. To provide for replay protection, a packet number (PN) field is used. CCMP produces a message integrity code (MIC) that provides data origin authentication and data integrity for the packet payload data. The PN is included in the CCMP header and incorporated into the encryption and MIC calculations. Counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

Antenna Placement

When designing wireless networks, antenna placement and power output should be configured for maximum coverage and minimum interference. Four basic types of antennas are commonly used in 802.11 wireless networking applications: parabolic grid, yagi, dipole, and vertical. APs with factory-default omni antennas cover an area that is roughly circular and are affected by RF obstacles such as walls. When using this type of antenna, it is common to place APs in central locations or divide an office into quadrants. Many APs use multiple-input, multiple-output (MIMO) antennas. This type of antenna takes advantage of multipath signal reflections. Ideally, locate the AP as close as possible to the antennas. The farther the signal has to travel across the cabling between the AP and the antenna, the more signal loss that occurs. Loss is an important factor when deploying a wireless network, especially at higher power levels. Loss occurs as a result of the signal traveling between the wireless base unit and the antenna.

APs that require external antennas need additional consideration. You need to configure the antennas properly, consider what role the AP serves (AP or bridge), and consider where the antennas are placed. When the antenna is mounted on the outside of the building or the interface between the wired network and the transceiver is placed in a corner, it puts the network signal in an area where it is easy to intercept. Antenna placement should not be used as a security mechanism.

Professional site surveys for wireless network installations and proper AP placement are sometimes used to ensure coverage area and security concerns. Up-front planning takes more time and effort but can pay off in the long run, especially for large WLANs.

ExamAlert

Physical placement and transmit power adjustments can make it harder for intruders to stay connected to your APs. But never count on physical placement alone to stop attackers.

Power-Level Controls

One of the principle requirements for wireless communication is that the transmitted wave must reach the receiver with ample power to allow the receiver to distinguish the wave from the background noise. An antenna that is too strong raises security concerns. Strong omnidirectional Wi-Fi signals are radiated to a greater distance into neighboring areas, where the signals can be readily detected and viewed. Minimizing transmission power reduces the chances your data will leak out. Companies such as Cisco and Nortel have implemented dynamic power controls in their products. The system dynamically adjusts the power output of individual access points to accommodate changing network conditions, helping ensure predictable wireless performance and availability.

ExamAlert

Reducing the energy consumption by wireless communication devices is an important issue in WLANs. Know the mechanisms that prevent interference and increase capacity.

Transmit power control is a mechanism used to prevent too much unwanted interference between different wireless networks. Adaptive transmit power control in 802.11 WLANs on a per-link basis helps increase network capacity and improves battery life of Wi-Fi-enabled mobile devices.

Captive Portals

The *captive portal* technique enables administrators to block Internet access for users until some action is taken. When a user attempts to access the Internet, the HTTP client is directed to a special web page that usually requires the user to read and accept an acceptable use policy (AUP). By using a captive portal, the web browser is used to provide authentication. Captive portals are widely used in businesses such as hotels and restaurants that offer free Wi-Fi hotspots to Internet users. A captive portal web page can be used to require authentication, require payment for usage, or display some type of policy or agreement. Although captive portals are mainly for Wi-Fi hotspots, you can also use them to control wired access.

Antenna Types

Wireless antenna types are either omnidirectional or directional. *Omnidirectional* antennas provide a 360-degree radial pattern to provide the widest possible signal coverage. An example of omnidirectional antennas are the antennas commonly found on APs. *Directional* antennas concentrate the wireless signal in a specific direction, limiting the coverage area. An example of a directional antenna is a yagi antenna.

The need or use determines the type of antenna required. When an organization wants to connect one building to another building, a directional antenna is used. If an organization is adding Wi-Fi internally to an office building or a warehouse, an omnidirectional antenna is used. If the desire is to install Wi-Fi in an outdoor campus environment, a combination of both antennas would be used.

Site Surveys

A *site survey* is necessary before implementing any WLAN solution, to optimize network layout within each unique location. This is particularly important in distributed wireless network configurations spanning multiple buildings or open natural areas, where imposing structures and tree growth may affect network access in key areas.

A site survey should include a review of the desired physical and logical structure of the network, selection of possible technologies, and several other factors, including the following:

- Federal, state, and local laws and regulations relating to the proposed network solution.
- Potential sources of radio frequency (RF) interference, including local broadcast systems as well as motors, fans, and other types of equipment that generate RF interference. This includes an analysis of potential channel overlap between WAP hardware.
- Available locations for WAP hardware installation and physical network integration connectivity.
- Any special requirements of users, applications, and network equipment that must function over the proposed wireless network solution.
- Whether a point-to-point (ad hoc or wireless bridge) or multipoint wireless solution is required. In most solutions, point-to-multipoint connectivity will be required to support multiple wireless clients from each WAP connected to the physical network.

ExamAlert

All wireless networks share several common security vulnerabilities related to their use of RF broadcasts, which may potentially be detected and compromised without the knowledge of the network administrator.

Data transported over this medium is available to anyone with the proper equipment, and so must be secured through encryption and encapsulation mechanisms no subject to public compromise.

VPN (Over Open Wireless)

VPNs are commonly used to securely connect employees to corporate networks when they are not in the office by using an Internet connection. More organizations are requiring hotspot visitors to VPN into the organizational network because they have no control over the security used in public Wi-Fi hotspots. The same principles that apply to wired VPNs can be applied to VPNs over open wireless networks. The use of a VPN over public Wi-Fi hotspots can increase privacy and provide data protection. VPNs over open wireless are not always immune to man-in-the-middle attacks. They can be susceptible to Wi-Fi-based attacks and VPN-based attacks.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. You want to implement non-vendor-specific strong authentication protocols for wireless communications. Which of the following would best meet your requirements? (Select two correct answers.)

○ **A.** EAP
○ **B.** PEAP
○ **C.** LEAP
○ **D.** WEP

2. Which of the following technologies would be selected when looking to reduce a vulnerability to replay attacks by using 128-bit keys with a 48-bit initialization vector (IV)?

○ **A.** ICMP
○ **B.** WEP
○ **C.** WPA
○ **D.** CCMP

3. Which of the following technologies would be used by a hotel for guest acceptance of an acceptable use policy?

○ **A.** Site survey
○ **B.** MAC filtering
○ **C.** VPN over wireless
○ **D.** Captive portal

Cram Quiz Answers

1. **A** and **B**. The IEEE specifies 802.1X and EAP as the standard for secure wireless networking, and PEAP is standards based. PEAP provides mutual authentication and uses a certificate for server authentication by the client, while users have the convenience of entering password-based credentials. Answer C is incorrect because LEAP is a Cisco proprietary protocol. Answer D is incorrect because WEP is the most basic form of encryption that can be used on 802.11-based wireless networks to provide privacy of data sent between a wireless client and its access point.

2. **D**. CCMP uses 128-bit keys with a 48-bit IV that reduces vulnerability to replay attacks. Answer A is incorrect because ICMP is a network troubleshooting protocol. Answer B is incorrect because WEP is the most basic form of encryption that can be used on 802.11-based wireless networks. Answer C is incorrect because WPA protects networks by incorporating a set of enhanced security features. WPA-protected networks require users to enter a passkey in order to access a wireless network.

3. **D**. A captive portal web page can be used to require authentication, require payment for usage, or display some type of policy or agreement. Answer A is incorrect because a site survey is used to optimize network layout within each unique wireless location. Answer B is incorrect because MAC filtering is a security access control method whereby the MAC address is used to determine access to the network. Answer C is incorrect because the use of a VPN over public Wi-Fi hotspots can increase privacy and provide data protection, but is not used to force acceptance of an acceptable use policy.

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all the Cram Quiz questions on the CD. You can also create a custom exam by objective with the practice exam software. Note any objective that you struggle with and go to the material that covers that objective in this chapter.

Index

Symbols

- **3DES (Triple Data Encryption Standard), 54, 459**
- **802.1X standard, 24, 73**
- **/ (slash) separator, 33**

A

- **acceptable use policy, 88, 328**
- **acceptance of risk, 96**
- **access control, 195, 391-392, 412**
  - account management, 421
    - continuous monitoring, 433-434
    - credential management, 424
    - disablement, 426-427
    - expiration, 425-426
    - generic account prohibition, 429-430
    - group-based privileges, 431-432
    - group policy, 424-425
    - lockout, 427
    - multiple accounts, 423
    - password complexity, 425
    - password history, 427-428
    - password length, 428-429
    - password reuse, 428
    - recovery, 426
    - shared accounts, 423
    - user access reviews, 433
    - user-assigned privileges, 432
  - ACL (access control list), 23, 375
  - authentication
    - authentication factors, 413
    - CAC (common access card), 409
    - CHAP (Challenge-Handshake Authentication Protocol), 411
    - defined, 391, 407-408
    - HOTP (HMAC-based one-time password), 411
    - implicit deny, 412
    - Kerberos, 395-397
    - LDAP (Lightweight Directory Access Protocol), 397-398
    - multifactor authentication, 409-410
    - OTP (one-time password), 411
    - PAP (Password Authentication Protocol), 411
    - RADIUS (Remote Authentication Dial-In User Service), 394
    - SAML (Security Assertion Markup Language), 398
    - Secure LDAP, 398
    - smart cards, 409
    - SSO (single sign-on), 412
    - TACACS (Terminal Access Controller Access Control System), 394-395
    - tokens, 408
    - trusted OS, 412
    - XTACACS (Extended Terminal Access Controller Access Control System), 398
  - authorization
    - ACL (access control list), 403-404
    - defined, 391, 402
    - discretionary access, 404-405
    - least privilege, 403
    - MAC (mandatory access control), 404
    - role-based access control, 406
    - rule-based access control, 405-406
    - separation of duties, 403
    - time-of-day restrictions, 406-407
  - defined, 391, 421
  - identification, 413
    - biometrics, 414-415
    - defined, 407
    - federation, 416

    - personal identity verification (PIV) card, 416
    - transitive trust/authentication, 417
    - usernames, 416
  - implicit deny, 25-26
  - NAC (network access control), 39-40
  - RBAC (rule-based access control), 20
  - remote access, 37
- **access control list (ACL), 23, 166, 375, 403-404**
- **access logs, 265**
- **access requestor (AR), 39**
- **account management, 421**
  - continuous monitoring, 433-434
  - credential management, 424
  - disablement, 426-427
  - expiration, 425-426
  - generic account prohibition, 429-430
  - group-based privileges, 431-432
  - group policy, 424-425
  - lockout, 427
  - multiple accounts, 423
  - password complexity, 425
  - password history, 427-428
  - password length, 428-429
  - password reuse, 428
  - recovery, 426
  - shared accounts, 423
  - user access reviews, 433
  - user-assigned privileges, 432
- **AccuTracking, 318**
- **Acid Rain, 209**
- **ACL (access control list), 23, 375, 403-404**
- **active/passive configuration, 6**
- **active versus passive tools, 278**
- **add-ons, malicious, 252**
- **addresses**
  - APIPA (Automatic Private IP Addressing), 37
  - link-local addresses, 36
  - MAC (Media Access Control) address, 5, 74-75
  - ULA (unique local address), 36
- **administrative controls, 170**
- **Advanced Encryption Standard (AES), 455, 459**
- **adware, 205**
- **AES (Advanced Encryption Standard), 455, 459**
- **AH (Authentication Header), 51, 466**
- **AirMagnet, 244**
- **aisles, hot/cold, 163**
- **alarms, 168, 270**
- **ALE (annualized loss expectancy), 92**
- **alerts, 271**
- **algorithms, 440**
  - asymmetric encryption algorithms, 460-462
  - hash algorithms, 456-458
  - symmetric encryption algorithms, 458-460
- **Android systems, 383**
- **annual rate of occurrence (ARO), 92**
- **annualized loss expectancy (ALE), 92**
- **annualized rate of occurrence (ARO), 85**
- **anomaly-based IDSs, 10-11**
- **antennas, 76-78**
- **anti-malware, 336-339**
- **antispam software, 337-338**
- **antispyware software, 338**
- **antivirus software 325, 336-337**
- **APIPA (Automatic Private IP Addressing), 37**
- **application attacks**
  - arbitrary/remote code execution, 257
  - browser threats, 251-252
  - buffer overflows, 254
  - code injections, 252
  - cookies, 255-257
  - directory traversal, 253
  - header manipulation, 253
  - integer overflows, 255
  - zero-day attacks, 253-254

application-aware devices, 15-16
application configuration baseline, 301-302
application control, 318-319
application firewalls, 386
application fuzzing, 294
application hardening, 302-305
Application log, 263
application patch management, 305-306
application security, 291, 321
  application white listing, 323-324
  authentication, 322
  black listing, 342
  BYOD (bring your own device), 324
    acceptance-use policy, 328
    architecture/infrastructure considerations, 328
    corporate policies, 327
    data ownership, 325
    data privacy, 326
    forensics, 326
    legal concerns, 328
    onboard camera/video, 329
    onboarding/offboarding, 326-327
    patch and antivirus management, 325
    support ownership, 325
    user acceptance, 327
  credential management, 322
  encryption, 323
  fuzzing, 293-294
  geotagging, 323
  key management, 321-322
  risk management, 103-104
  secure coding concepts, 294-296
    application configuration baseline, 301-302
    application hardening, 302-305
    application patch management, 305-306
    client-side validation, 306-307
    cross-site request forgery prevention, 299-301
    error and exception handling, 296-297
    input validation, 297-298
    NoSQL versus SQL databases, 306
    server-side validation, 306-307
    XSS (cross-site scripting), 298-299
  transitive trusts and authentication, 324
  white listing, 342
AR (access requestor), 39
arbitrary code execution, 257
architecture considerations
  architecture review, 281
  BYOD (bring your own device), 328
armored viruses, 213
ARO (annual rate of occurrence), 85, 92
ARP poisoning, 221-223
assessment technique, 280-281
asset tracking, 319
asymmetric encryption, 443-444, 460-462
attack signatures, 272
attack surfaces, 280
attacks, 203
  application attacks
    arbitrary/remote code execution, 257
    browser threats, 251-252
    buffer overflows, 254
    code injections, 252
    cookies, 255-257
    directory traversal, 253
    header manipulation, 253
    integer overflows, 255
    zero-day attacks, 253-254
  ARP poisoning, 221-223
  client-side attacks, 227
  denial-of-service (DoS) attacks, 216-218
  distributed DoS (DDoS) attacks, 218-220

- DNS poisoning, 220-221
- malicious insider threat, 226-227
- malware
  - adware, 205
  - armored viruses, 213
  - backdoors, 210
  - botnets, 211-212
  - logic bombs, 210-211
  - polymorphic malware, 213
  - ransomware, 212-213
  - rootkits, 209-210
  - spyware, 207-208
  - Trojan horses, 208-209
  - viruses, 205-206
  - worms, 207
- man-in-the-middle attacks, 216
- password attacks, 227-230
- phishing, 225-226
- privilege escalation, 226
- replay attacks, 220
- social engineering attacks
  - dumpster diving, 237-238
  - explained, 235-236
  - hoaxes, 238-239
  - impersonation, 238
  - principles of influence, 239-240
  - shoulder surfing, 236-237
  - tailgating, 238
- spam, 224-225
- spoofing, 223-224
- transitive access, 227
- typo squatting/URL hijacking, 230-231
- watering hole attacks, 231
- wireless attacks
  - bluejacking, 244
  - bluesnarfing, 244
  - jamming/interference, 243
  - near-field communication (NFC), 247-248
  - packet sniffing, 245
  - rogue access points, 243-244
  - war driving, 244
  - WEP/WPA attacks, 245-246
  - WPS attacks, 247

attestation, 367

audits, 116-117, 265

authentication, 322. See also authorization
- authentication factors, 413
- authentication tags, 450
- CAC (common access card), 409
- CHAP (Challenge-Handshake Authentication Protocol), 411
- defined, 391, 407-408
- HOTP (HMAC-based one-time password), 411
- implicit deny, 412
- Kerberos, 395-397
- LDAP (Lightweight Directory Access Protocol), 397-398
- multifactor authentication, 409-410
- OTP (one-time password), 411
- PAP (Password Authentication Protocol), 411
- RADIUS (Remote Authentication Dial-In User Service), 394
- SAML (Security Assertion Markup Language), 398
- Secure LDAP, 398
- smart cards, 409
- SSO (single sign-on), 412
- TACACS (Terminal Access Controller Access Control System), 394-395
- tokens, 408
- transitive trusts, 324
- trusted OS, 412
- XTACACS (Extended Terminal Access Controller Access Control System), 398

Authentication Header (AH), 51, 466

authenticators, 458

authoritative servers, 54

authority, 239

authorization. See also authentication
- ACL (access control list), 403-404

- defined, 391, 402
- discretionary access, 404-405
- least privilege, 403
- MAC (mandatory access control), 404
- role-based access control, 406
- rule-based access control, 405-406
- separation of duties, 403
- time-of-day restrictions, 406-407

Automatic Private IP Addressing (APIPA), 37

automotive in-vehicle computing systems, 385

availability, 197-198, 348-349

avoidance of risk, 96

awareness of risk, 106-107

B

BAA (business associate agreement), 105

backdoor Trojans, 208

backdoors, 210

backup plans/policies, 108-109, 186-187

- backup execution/frequency, 188-189
- cold sites, 190
- hot sites, 190
- warm sites, 190

balancing load, 184

banner grabbing, 278-279

barricades, 167

baselines

- application configuration baseline, 301-302
- baseline reporting, 280
- configuration baselines, 270
- host software baselining, 346-347

bastion hosts, 7

BCP (business continuity planning), 175-176

Bcrypt, 468

behavior-based IDSs, 10

BES (BlackBerry Enterprise Server), 315, 365

BIA (business impact analysis), 90, 174-175

big data, 130-131, 358-359

biometrics, 167, 414-415

birthday paradox, 229

black box testing, 287

black listing, 74, 338, 342

BlackBerry Enterprise Server (BES), 315, 365

Blaster worm, 207

blind spoofing, 223

block ciphers, 444, 459

blood vessel biometrics, 415

Blowfish, 54, 459

bluejacking, 244

bluesnarfing, 244

Boink attack, 218

Bonk attack, 218

boot sector viruses, 205

botnets, 211-212

bots, 211

BPA (business partner agreement), 104

BPDU (bridge protocol data unit), 25

bridge CA models, 488

bridge protocol data units (BPDU), 25

bring your own device. See BYOD

browser threats, 251-252

brute-force attacks, 228-229

buffer overflow exploitation, 297

buffer overflows, 252-254

business associate agreement (BAA), 105

business continuity concepts, 174

- business continuity planning (BCP), 175-176
- business impact analysis (BIA), 174-175
- continuity of operations, 176
- critical systems and components, 175

- disaster recovery, 176-177
- high availability, 177-178
- IT contingency planning, 177
- redundancy, 178-179
- risk assessment, 176
- single points of failure, 175
- succession planning, 177
- tabletop exercises, 179-180

business continuity planning (BCP), 175-176

business impact analysis (BIA), 90, 174-175

business partners
- business partner agreement (BPA), 104
- on-boarding/off-boarding, 102-103

BYOD (bring your own device), 118, 324, 365
- acceptance-use policy, 328
- architecture/infrastructure considerations, 328
- corporate policies, 327
- data ownership, 325
- data privacy, 326
- forensics, 326
- legal concerns, 328
- onboard camera/video, 329
- onboarding/offboarding, 326-327
- patch and antivirus management, 325
- support ownership, 325
- user acceptance, 327

C

CA (certificate authority), 480

cables
- coaxial cables, 161
- locks, 345
- twisted-pair cabling, 162

CAC (common access card), 409

caching servers, 54

cameras (BYOD), 329

captive portals, 78

car in-vehicle computing systems, 385

cards
- CAC (common access card), 409
- PIV (personal identity verification) card, 409
- smart cards, 409

CCMP (Cipher Block Chaining Message Authentication Code Protocol), 246, 455

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 76

CCTV (closed-circuit television), 126, 166, 199

centralized key management, 484-485

centralized solutions, 337

certificates, 196
- CA (certificate authority), 480
- certificate policies, 481-483
- certificate revocation list (CRL), 487
- digital certificates, 478-480

Certified Secure Software Lifecycle Professional (CSSLP), 295

chain of custody, 128-130

Challenge Handshake Authentication Protocol (CHAP), 411, 458

change management, 114

CHAP (Challenge Handshake Authentication Protocol), 411, 458

Children’s Online Privacy Protection Act (COPPA), 87

CIDR (classless interdomain routing), 33

Cipher Block Chaining Message Authentication Code Protocol (CCMP), 246, 455

cipher suites, 439, 466-468

Class A fires, 160

Class B fires, 160

Class C fires, 160

Class D fires, 160

classification levels, 148-149

classless interdomain routing (CIDR), 33
clean desk policies, 151
clear box testing, 287
client-side attacks, 227
client-side validation, 306-307
closed-circuit television (CCTV), 166, 199
cloud computing, 41, 355-357
  community clouds, 43
  hybrid clouds, 43
  infrastructure-as-a-service (IaaS), 42
  platform-as-a-service (PaaS), 41
  private clouds, 42
  public clouds, 43
  risk management, 96-97
  software-as-a-service (SaaS), 41
clustering, 183
coaxial cables, 161
code injections, 252
Code Red worm, 207
code review, 280
code security, 294-296
  application configuration baseline, 301-302
  application hardening, 302-305
  application patch management, 305-306
  client-side validation, 306-307
  cross-site request forgery prevention, 299-301
  error and exception handling, 296-297
  input validation, 297-298
  NoSQL versus SQL databases, 306
  server-side validation, 306-307
  XSS (cross-site scripting), 298-299
cold aisles, 163
cold sites, 190
common access card (CAC), 409
community clouds, 43
compensating controls, 169
complexity of passwords, 425
compliance, 110, 150-152
confidentiality, 194-195
  access controls, 195
  confidential classification level, 149
  encryption, 195
  steganography, 195
configuration baselines, 270
consensus, 239
content inspection, 13
continuity of operations, 176
continuous monitoring, 433-434
control redundancy and diversity, 387-388
controls, 85, 168
  administrative controls, 170
  compensating controls, 169
  defined, 90
  detective controls, 169
  deterrent controls, 169
  environmental controls, 157
    EMI shielding, 160-162
    environmental monitoring, 163
    fire suppression, 158-160
    hot aisles/cold aisles, 163
    HVAC, 158
    temperature and humidity controls, 164
  management controls, 85
  operational controls, 85
  preventive controls, 169
  technical controls, 85, 118-119, 170
cookies, 255-257
COPPA (Children's Online Privacy Protection Act), 87
corporate cloud, 42
corporate policies (BYOD), 327
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 76
CPS (certificate practice statement), 482
CRC (cyclic redundancy check), 127

credential management, 322, 424
critical systems and components, identifying, 175
CRL (certificate revocation list), 487
cross-site request forgery (XSRF) prevention, 299-301
cross-site scripting (XSS), 252, 298-299
cryptography
  asymmetric encryption, 443-444, 460-462
  cipher suites, 466-468
  cryptographic hash functions, 456-458
  definition of, 439
  digital signatures, 447-449
  elliptic curve cryptography (ECC), 444
  encryption algorithms, 440
  hash-based message authentication code (HMAC), 458
  hashing, 449-450
  history of, 439
  IBE (identity-based encryption), 478
  in-band key exchange, 445
  IPsec (Internet Protocol Security), 466
  Kerckhoff's principle, 451
  keys. See keys
  Layer 2 Tunneling Protocol (L2TP), 465
  nonrepudiation, 447-449
  one-time pad (OTP), 462
  out-of-band key exchange, 445
  perfect forward secrecy, 446
  Pretty Good Privacy (PGP), 462-463
  quantum cryptography, 445
  Secure Shell (SSH), 465
  Secure Sockets Layer (SSL), 463-465
  session keys, 445-446
  steganography, 450-451
  symmetric encryption algorithms, 458-460
  transport encryption, 447
  Transport Layer Security (TLS), 463-465
  wireless encryption functions, 455-456
CryptoLocker, 212
cryptosystem, 439
CSR (certificate signing request), 482-483
CSSLP (Certified Secure Software Lifecycle Professional), 295
custody, chain of, 128-130
cyclic redundancy check (CRC), 127

D

damage and loss control, 140
data at-rest, 372-374
data backups, 108-109
data breaches, 139-140
data encryption. See encryption
Data Encryption Standard (DES), 54, 459
data in-transit, 372-374
data in-use, 372-374
data labeling, handling, and disposal, 150
data loss prevention (DLP), 117-119, 354, 372-374
data ownership, 108, 325
data security, 353
  ACL (access control list), 375
  big data, 358-359
  cloud storage, 355-357
  data at-rest, 372-374
  data encryption
    databases, 361-362
    FDE (full disk encryption), 360-361
    files/folders, 363
    mobile devices, 365-366
    removable media, 363-365
    selecting an encryption method, 359-360
  data in-transit, 372-374
  data in-use, 372-374

data policies, 376-378
hardware-based encryption devices, 366
hard drive encryption, 371-372
hardware security module (HSM), 368-369
Trusted Platform Module (TPM), 366-368
USB encryption, 370-371
permissions, 375
privacy, 326
SAN (storage-area network), 357-358
static environments, 382
Android systems, 383
application firewalls, 386
control redundancy and diversity, 387-388
embedded systems, 383
firmware version control, 387
game consoles, 384
in-vehicle computing systems, 385
iOS systems, 383
mainframes, 384
manual updates, 387
network segmentation, 385-386
supervisory control and data acquisition (SCADA) systems, 382
wrappers, 387

databases
data encryption, 361-362
NoSQL databases, 306
SQL databases, 306

DDoS (distributed DoS) attacks, 218-220

decentralized environments, 337

decentralized key management, 484-485

declassification, 377

deep packet inspection (DPI) firewalls, 15

defense in depth, 44

degaussing, 377

demilitarized zone (DMZ), 31-32

denial-of-service (DoS) attacks, 216-218

DES (Data Encryption Standard), 54, 459

design. See secure network design

destruction
of media, 377
PKI (public key infrastructure), 486

detection controls, 271-272

detective controls, 169

deterrents, 96, 169, 261
assessment technique, 280-281
detection controls versus prevention controls, 271-272
hardening, 266-268
network security, 268-269
penetration testing, 284-287
reporting, 270-271
risk calculation, 279-280
security assessment tools, 275
banner grabbing, 278-279
honeypots, 277
passive versus active tools, 278
port scanners, 277
protocol analyzers, 275-276
vulnerability scanners, 276-277
security posture, 269-270
system log monitoring, 263-265
vulnerability scanning, 285-286

device security, 313
application control, 318-319
asset tracking and inventory control, 319
BYOD (bring your own device), 324
acceptance-use policy, 328
architecture/infrastructure considerations, 328
corporate policies, 327
data ownership, 325
data privacy, 326
forensics, 326
legal concerns, 328
onboard camera/video, 329

        onboarding/offboarding, 326-327
        patch and antivirus management, 325
        support ownership, 325
        user acceptance, 327
    device access control, 320
    disabling unused features, 321
    full device encryption, 313-314
    Global Positioning System (GPS) tracking, 317-318
    lockout, 316
    mobile device management (MDM), 319-320
    remote wiping, 314-315
    removable storage, 320
    screen locks, 317
    storage segmentation, 319
DHCP (Dynamic Host Configuration Protocol), 61, 304-305
DHE (Diffie-Hellman Exchange), 446, 461
dictionary attacks, 228-229
Diffie-Hellman key exchange, 446, 461
digital certificates, 478-480
digital signatures, 196, 447-449
directional antennas, 78
directory traversal, 253
disabled accounts, 426-427
disabling unused features, 321
disaster recovery, 176-177, 185-189
discretionary access, 404-405
disks
    clustering, 183
    imaging, 124
    load balancing, 184
    redundant array of independent disks (RAID), 180-183
diversity, 387-388
DLP (data loss prevention), 117-119, 354, 372-374
DMZ (demilitarized zone), 31-32
DNS (Domain Name Service), 54-55, 303
    DNS poisoning, 220-221
DoS (denial-of-service) attacks, 216-218
downloader Trojans, 208
DPI (deep packet inspection) firewalls, 15
drills, 199
drives. See disks
dry-pipe fire-suppression system, 159
dumpster diving, 237-238
duties, separation of, 89, 403
Dynamic Host Configuration Protocol (DHCP), 61, 304-305
dynamic ports, 65

E

EAP (Extensible Authentication Protocol), 24, 73
EAPOL (EAP over LAN), 73
ECC (elliptic curve cryptography), 444, 461
ECDH (Elliptic Curve Diffie-Hellman), 446
EFS (Encrypting File System), 363
EIGRPv6, 61
EK (endorsement key), 366
El Gamal encryption algorithm, 461
elasticity, 348-349
elliptic curve cryptography (ECC), 444, 461
Elliptic Curve Diffie-Hellman (ECDH), 446
email, 224-225, 303
embedded encryption, 314
embedded systems, 383
EMI shielding, 160-162
Encapsulating Security Payload (ESP), 51, 466
Encrypting File System (EFS), 363
encryption, 195, 323, 440. See also cryptography

- 3DES (Triple Data Encryption Standard), 54
- asymmetric encryption algorithms, 460-462
- Blowfish, 54
- data in-use, 372-374
- databases, 361-362
- DES (Data Encryption Standard), 54
- FDE (full disk encryption), 360-361
- files/folders, 363
- full device encryption, 313-314
- hardware-based encryption devices, 366
  - hard drive encryption, 371-372
  - hardware security module (HSM), 368-369
  - Trusted Platform Module (TPM), 366-368
  - USB encryption, 370-371
- IDEA (International Data Encryption Algorithm), 54
- keys. *See* keys
- mobile devices, 365-366
- remote wiping, 314-315
- removable media, 363-365
- selecting an encryption method, 359-360
- symmetric encryption algorithms, 458-460

endorsement key (EK), 366

enforcing policy, 424-425

enterprise cloud, 42

environmental controls, 157
- EMI shielding, 160-162
- environmental monitoring, 163
- fire suppression, 158-160
- hot aisles/cold aisles, 163
- HVAC, 158
- temperature and humidity controls, 164

environmental monitoring, 163

ephemeral, 446

error handling, 296-297

escalation of incidents, 135-136

escape plans, 199

escape routes, 200

escrow (key), 450

ESP (Encapsulating Security Payload), 51, 466

events (Windows), 264

evil twins, 243

exception handling, 296-297

expense tracking, 128

expired accounts, 425-426

exploits, 90

exponential key agreement, 461

Extended Terminal Access Controller Access Control System (XTACACS), 398

Extensible Authentication Protocol (EAP), 24, 73

extranets, 32

F

fabric, 62

facial recognition, 415

false negatives, 86

false positives, 85-86

familiarity, 240

Faraday, Michael, 161

fault tolerance, 180, 197
- clustering, 183
- hardware, 180
- load balancing, 184
- redundant array of independent disks (RAID), 180-183
- servers, 184

FC (Fibre Channel), 62

FCoE (Fibre Channel over Ethernet), 62

FDE (full disk encryption), 313-314, 355, 360-361

Federal Information Processing Standards (FIPS), 362, 466

Federal Rules of Civil Procedure (FRCP), 378

federation, 416
fencing, 166, 198
Fibre Channel (FC), 62
Fibre Channel over Ethernet (FCoE), 62
file-format fuzzing, 294
file-level data encryption, 363
file services, 304
File Transfer Protocol (FTP), 63, 303
File Transfer Protocol Secure (FTPS), 57
filtering
  heuristic filtering, 338
  MAC filtering, 74-75
fingerprints, 415
FIPS (Federal Information Processing Standards), 362, 466
fire suppression, 158-160
firewalls
  application firewalls, 386
  DPI (deep packet inspection) firewalls, 15
  explained, 3
  firewall rules, 20-21
  host-based firewalls, 342-343
  network firewalls, 14-15
  NGFW (next-generation firewalls), 15
  web application firewalls, 14-15
firmware version control, 387
first responder, 138
flood guards, 24-25
folder-level data encryption, 363
forensic procedures
  big data analysis, 130-131
  BYOD (bring your own device), 326
  chain of custody, 128-130
  drive imaging, 124
  hashes, 127
  man-hour and expense tracking, 128
  network traffic logs, 125
  order of volatility, 123-124
  screenshots, 127-128
  time offset records, 126
  video capture, 125-126
  witnesses, 128
forgery, 299-301
forward secrecy, 446
Fraggle attacks, 217
FRCP (Federal Rules of Civil Procedure), 378
frequency of backups, 188-189
FTP (File Transfer Protocol), 63, 303
FTPS (File Transfer Protocol Secure), 57
full disk encryption (FDE), 313-314, 355, 360-361
functions
  cryptographic hash functions, 456-458
  wireless encryption functions, 455-456
fuzzing, 293-294

G

gait biometrics, 415
game consoles, 384
gateways, 7
geotagging, 323
glass box testing, 287
GPO (Group Policy objects), 424
GPS (Global Positioning System) tracking, 317-318
gray box testing, 287
group-based privileges, 431-432
group policies, 269, 424-425
group privileges, 431-432
guards, 167

H

H.323, 38
HA (high availability), 177-178
hand/palm geometry, 415
hard drive encryption, 371-372

hard zoning, 358
hardening applications, 266-268, 302-305
  DHCP services, 304-305
  DNS services, 303
  email services, 303
  file and print services, 304
  FTP services, 303
  NNTP services, 303
  OS hardening, 335-336
  web services, 302
hardware-based encryption devices, 366
  hard drive encryption, 371-372
  hardware security module (HSM), 368-369
  Trusted Platform Module (TPM), 366-368
  USB encryption, 370-371
hardware locks, 165
hardware security, 344
  cable locks, 345
  locked cabinets, 346
  safes, 345-346
hardware security module (HSM), 357, 368-369
hashing, 127, 196, 449-450
  hash algorithms, 456-458
  hash-based message authentication code (HMAC), 411, 458
  hash functions, 449-450
header manipulation, 253
Health Insurance Portability and Accountability Act (HIPAA), 105, 270
heuristic filtering, 338
heuristic IDSs, 11
heuristic scanning, 337
HIDS (host-based intrusion detection system), 9, 86, 344
high availability, 177-178
high classification level, 148
HIPAA (Health Insurance Portability and Accountability Act), 105, 270
HMAC (hash-based message authentication code), 411, 458
hoaxes, 238-239
honeynets, 277
honeypots, 277
host security, 311
  application security, 321-324
  bastion hosts, 7
  BYOD (bring your own device), 324
    acceptance-use policy, 328
    architecture/infrastructure considerations, 328
    corporate policies, 327
    data ownership, 325
    data privacy, 326
    forensics, 326
    legal concerns, 328
    onboard camera/video, 329
    onboarding/offboarding, 326-327
    patch and antivirus management, 325
    support ownership, 325
    user acceptance, 327
  device security, 313
    application control, 318-319
    asset tracking and inventory control, 319
    device access control, 320
    disabling unused features, 321
    full device encryption, 313-314
    Global Positioning System (GPS) tracking, 317-318
    lockout, 316
    mobile device management (MDM), 319-320
    remote wiping, 314-315
    removable storage, 320
    screen locks, 317
    storage segmentation, 319
  firewalls, 342-343
  host availability/elasticity, 348-349
  host-based integration, 40
  operating system security, 333-335

- antivirus software, 336-338
- hardware security, 344-346
- host-based firewalls, 342-343
- host intrusion-detection systems (HIDS), 9, 86, 344
- host software baselining, 346-347
- OS hardening, 335-336
- patch management, 339-341
- pop-up blockers, 338-339
- trusted OSs, 342
- virtualization, 347-349
- white listing versus black listing applications, 342

host software baselining, 346-347

hot aisles, 163

hot sites, 190

hotfixes, 267, 340

HOTPs (HMAC-based one-time passwords), 411

hover ads, 339

HSM (hardware security module), 357, 368-369

HTTP (Hypertext Transfer Protocol), 64, 253

HTTPS (HTTP Secure), 57-58, 464-465

humidity controls, 164

HVAC, 158

hybrid attacks, 229

hybrid clouds, 43

Hypertext Transfer Protocol (HTTP), 64

Hypertext Transfer Protocol Secure (HTTPS), 57-58, 464-465

I

IaaS (infrastructure-as-a-service), 42, 356

IAX (Inter Asterisk eXchange), 38

IBE (identity-based encryption), 478

ICMP (Internet Control Message Protocol), 59-61

ICS (Internet Connection Sharing), 36

IDEA (International Data Encryption Algorithm), 54

identification, 413. See also authentication
- biometrics, 414-415
- defined, 407
- federation, 416
- personal identity verification (PIV) card, 416
- transitive trust/authentication, 417
- usernames, 416

identity-based encryption (IBE), 478

IDS (intrusion-detection system)
- anomaly-based IDSs, 10-11
- behavior-based IDSs, 10
- heuristic IDSs, 11
- HID (host-based intrusion-detection system), 9
- NID (network-based intrusion-detection system), 8-9
- NIP (network-based intrusion-prevention system), 9-10
- signature-based IDSs, 10

IEEE 802.1X standard, 24

IETF (Internet Engineering Task Force), 476

IKE (Internet Key Exchange), 466

impersonation, 238

implementation. See network implementation

implicit deny, 25-26, 412, 432

in-band key exchange, 445

incident response, 114-115
- damage and loss control, 140
- data breaches, 139-140
- escalation and notification, 135-136
- first responder, 138
- incident identification, 135
- incident isolation, 138-139
- lessons learned, 137
- mitigation steps, 136
- preparation, 134-135
- recovery/reconstitution procedures, 137-138
- reporting, 137

influence, principles of, 239-240

information classification levels, 148-149

Information Technology Security Evaluation Criteria (ITSEC), 95

informed spoofing, 223

infostealer Trojans, 208

infrastructure-as-a-service (IaaS), 42, 356

inline integration, 39

input validation, 297-298

inspection, 13

integer overflows, 255

integrity, 196-197

Inter Asterisk eXchange (IAX), 38

interconnection security agreement (ISA), 102, 105

interference, 243

internal cloud, 42

International Data Encryption Algorithm (IDEA), 54

Internet Connection Sharing (ICS), 36

Internet Control Message Protocol (ICMP), 59

Internet Engineering Task Force (IETF), 476

Internet Key Exchange (IKE), 466

Internet Protocol Security (IPsec), 51-52, 466

Internet Security Association and Key Management Protocol (ISAKMP), 52

Internet Small Computer System Interface (iSCSI), 61

interoperability agreements, 104-105

intimidation, 239

intranets, 32

intrusion-detection systems. See IDSs

in-vehicle computing systems, 385

inventory control, 319

iOS systems, 383

iostat, 275

IPsec (Internet Protocol Security), 51-52, 466

IPv4, 60

IPv6, 60-61

iris scanning, 415

ISA (interconnection security agreement), 102, 105

ISAKMP (Internet Security Association and Key Management Protocol), 52

iSCSI (Internet Small Computer System Interface), 61

isolating incidents, 138-139

IT contingency planning, 177

ITSEC (Information Technology Security Evaluation Criteria), 95

J-K

jamming, 243

job rotation, 89

Kerberos, 395-397

Kerckhoff's principle, 451

keylogger Trojans, 209

keys. See also cryptography
  Diffie-Hellman key exchange, 446
  EK (endorsement key), 366
  in-band key exchange, 445
  Internet Key Exchange (IKE), 466
  key escrow, 450
  key management, 321-322
  key stretching, 468
  out-of-band key exchange, 445
  perfect forward secrecy, 446
  PKI (public key infrastructure)
    CA (certificate authority), 480
    centralized versus decentralized key management, 484-485
    certificate policies, 481-483
    destruction, 486
    digital certificates, 478-480
    IBE (identity-based encryption), 478
    key escrow, 486
    key recovery, 484
    M of N control, 484

- multiple key pairs, 483
- overview, 473
- RA (registration authority), 481
- revocation, 486-487
- standards, 475-477
- storage, 485
- trust models, 487-488
- session keys, 445-446
- SRK (storage root key), 366-367
- symmetric key cryptography, 442-444

KoolSpan's TrustChip, 314

L

L2TP (Layer 2 Tunneling Protocol), 465

labeling data, 150

LAN Manager hash (LM hash), 457

land attacks, 217

LANMan hash, 457

Layer 2 Tunneling Protocol (L2TP), 465

layered security, 44

LDAP (Lightweight Directory Access Protocol), 397-398
- LDAP injection, 252
- Secure LDAP, 398

LEAP (Lightweight Extensible Authentication Protocol), 74

least privilege, 90, 336, 403

length of passwords, 428-429

lessons learned, 137

lighting, 166, 198

Lightweight Directory Access Protocol. See LDAP

Lightweight Extensible Authentication Protocol (LEAP), 74

likelihood of risk, 91, 95

link-local addresses, 36

LM hash (LAN Manager hash), 457

load balancers, 6

load balancing, 184

local shared object (LSO), 256

locked cabinets, 346

lockout, 316, 427

locks, 165, 199, 345

log analysis, 26-27

logic bombs, 210-211

logical unit number (LUN) masking, 358

logon rights, 432

logs
- access logs, 265
- Application, 263
- audit logs, 265
- monitoring, 263-265
- network traffic logs, 125
- security logs, 265
- System, 263-265

loop protection, 25

loss control, 140

Love Bug, 206

low classification level, 149

LSO (local shared object), 256

LUN (logical unit number) masking, 358

M

M of N control, 484

MAC (Media Access Control), 5, 404
- MAC filtering, 74-75
- MAC flooding, 222

MAC (message authentication code), 450

macro viruses, 206

mainframes, 384

malicious add-ons, 252

malicious insider threat, 226-227

malware
- adware, 205
- anti-malware, 336-339
- armored viruses, 213
- backdoors, 210
- botnets, 211-212
- logic bombs, 210-211

  malware inspection, 13-14
  polymorphic malware, 213
  ransomware, 212-213
  rootkits, 209-210
  spyware, 207-208
  Trojan horses, 208-209
  viruses, 205-206
  worms, 207
MAM (mobile application management), 104, 318
man-hour and expense tracking, 128
man-in-the-middle attacks, 216
management. See account management; credential management; risk management
mandatory vacations, 88
mantraps, 165
manual updates, 387
MD (message digest) series algorithm, 456-457
MD5 (Message Digest 5) hash value, 127
MDM (mobile device management), 104, 319-320, 365
mean time between failures (MTBF), 93-94
mean time to failure (MTTF), 93
mean time to repair (MTTR), 93
measurement, 94-95
Media Access Control. See MAC
media sanitation, 377
medium classification level, 149
Melissa virus, 206
memorandum of understanding (MOU), 101, 104
message authentication code (MAC), 450
Message Digest 5 (MD5) hash value, 127
message digest series algorithm, 456-457
message integrity code (MIC), 76
metrics, 154
Michelangelo virus, 206
MIC (message integrity code), 76
Microsoft Message Analyzer, 275
MIMO (multiple-input, multiple-output) antennas, 77
mitigation (risk), 96. See also deterrents
  audits, 116-117
  change management, 114
  data loss prevention (DLP), 117-119
  incident management, 114-115
  incident response, 136
  technology controls, 118-119
  user rights and permissions reviews, 115-116
mobile application management (MAM), 104, 318
mobile device management (MDM), 104, 319-320, 365-366
mobile device security. See device security
Mocmex, 209
monitoring
  continuous monitoring, 433-434
  system logs, 263-265
Morris worm, 207
motion detection, 168
MOU (memorandum of understanding), 101, 104
MTBF (mean time between failure), 93-94
MTTF (mean time to failure), 93
MTTR (mean time to repair), 93
multifactor authentication, 409-410
multipartite viruses, 206
multiple accounts, 423
multiple-input, multiple-output (MIMO) antennas, 77
multiple key pairs, 483
Mydoom worm, 207

N

NAC (network access control), 39-40

NAT (Network Address Translation), 36

National Institute of Standards and Technology (NIST), 91, 115

near-field communication (NFC), 247-248

NetBIOS (Network Basic Input/Output System), 64-65

NetStumbler, 244

network access control (NAC), 39-40

Network Address Translation (NAT), 36

network-based intrusion-detection system (NID), 8-9

network-based intrusion-prevention system (NIP), 9-10

Network Basic Input/Output System (NetBIOS), 64-65

network design, 1

- ACL (access control list), 23
- application-aware devices, 15-16
- cloud computing, 41
  - community clouds, 43
  - hybrid clouds, 43
  - infrastructure-as-a-service (IaaS), 42
  - platform-as-a-service (PaaS), 41
  - private clouds, 42
  - public clouds, 43
  - software-as-a-service (SaaS), 41
- defense in depth, 44
- DMZ (demilitarized zone), 31-32
- firewalls
  - DPI (deep packet inspection) firewalls, 15
  - explained, 3
  - firewall rules, 20-21
  - network firewalls, 14-15
  - NGFW (next-generation firewall), 15
  - web application firewalls, 14-15
- flood guards, 24-25
- IDS (intrusion-detection system)
  - anomaly-based IDSs, 10-11
  - behavior-based IDSs, 10
  - heuristic IDSs, 11
  - HID (host-based IDS), 9
  - NID (network-based IDS), 8-9
  - NIP (network-based intrusion-prevention system), 9-10
  - signature-based IDSs, 10
- IEEE 802.1X standard, 24
- implicit deny, 25-26
- layered security, 44
- load balancers, 6
- log analysis, 26-27
- loop protection, 25
- NAC (network access control), 39-40
- NAT (Network Address Translation), 36
- network separation, 26
- port security, 23
- protocol analyzers, 11-12
- proxy servers, 6-7
- RBAC (rule-based access control), 20
- remote access, 37
- routers, 4-5, 22-23
- spam filters, 12
- subnetting, 32-34
- switches, 5
- telephony, 37-39
- UTM (unified threat management), 12-14, 27
- virtualization, 40-41
- VLAN (virtual local-area network), 21-22, 34-35
- VPN concentrators, 8
- web security gateways, 7

network firewalls, 14-15

network implementation, 49

- Network Basic Input/Output System (NetBIOS), 64-65
- OSI model, 67
- ports, 65-66

  - protocols. *See* individual protocols
  - wireless networks
    - antenna placement, 76-77
    - antenna types, 78
    - captive portals, 78
    - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 76
    - Extensible Authentication Protocol (EAP), 73
    - Lightweight Extensible Authentication Protocol (LEAP), 74
    - MAC filtering, 74-75
    - power-level controls, 77-78
    - Protected EAP (PEAP), 73-74
    - service set identifier (SSID), 75
    - site surveys, 79
    - Temporal Key Integrity Protocol (TKIP), 75-76
    - VPN (virtual private network), 80
    - Wi-Fi Protected Access (WPA), 71
    - Wired Equivalent Privacy (WEP), 72
    - WPA2, 71-72

Network News Transfer Protocol (NNTP), 303

network security, 268-269

network segmentation, 385-386

network separation, 26

network traffic logs, 125

New Technology File System (NTFS), 335

next-generation firewalls (NGFW), 15

NFC (near-field communication), 247-248

NGFW (next-generation firewall), 15

NID (network-based intrusion-detection system), 8-9

Nimda worm, 207

NIP (network-based intrusion-prevention system), 9-10

NIST (National Institute of Standards and Technology), 91, 115

NNTP (Network News Transfer Protocol), 303

nonrepudiation, 197, 447-449

NoSQL databases, 306

notifications, 135-136

NTFS (New Technology File System), 335

NTLM hash (NT LAN Manager hash), 457

Nuker, 209

O

OCSP (Online Certificate Status Protocol (OCSP), 487

off-boarding, 102-103, 326-327

omnidirectional antennas, 78

onboard camera/video (BYOD), 329

on-boarding, 102-103, 326-327

one-time password (OTP), 322, 411, 462

Online Certificate Status Protocol (OCSP), 487

Open Vulnerability Assessment Language (OVAL), 276

operating system security, 333-335
  - antispyware software, 338
  - antivirus software, 336-338
  - hardware security, 344-346
  - host-based firewalls, 342-343
  - host intrusion-detection systems (HIDS), 344
  - host software baselining, 346-347
  - OS hardening, 335-336
  - patch management, 339-341
  - pop-up blockers, 338-339
  - trusted OSs, 342
  - virtualization, 347-349
  - white listing versus black listing applications, 342

operational controls, 85

operations, continuity of, 176

Orange Book (TSCEC), 405

order of volatility, 123-124

OSI model, 67
OTP (one-time password), 322, 411, 462
out of band integration, 39
out-of-band key exchange, 445
OVAL (Open Vulnerability Assessment Language), 276
overwriting, 377
ownership of data, 108

P

P2P (peer-to-peer) services, 153-154
PaaS (platform-as-a-service), 41, 356
packet sniffing, 245
PAP (Password Authentication Protocol), 411, 458
passcode unlock screens, 316
passive versus active tools, 278
password attacks, 227-230
Password Authentication Protocol (PAP), 411, 458
Password-Based Key Derivation Function 2 (PBKDF2), 468
passwords
- complexity, 425
- HOTP (HMAC-based one-time password), 411
- length of, 428-429
- OTP (one-time password), 322, 411, 462
- password history, 427-428
- reusing, 428
- user habits, 151

patch compatibility, 348
patches, 198, 267, 305-306, 325, 339-341
pathping, 59
Payment Card Industry Data Security Standard (PCI-DSS), 362
PBKDF2 (Password-Based Key Derivation Function 2), 468
PBX (private branch exchange), 37
PCI-DSS (Payment Card Industry Data Security Standard), 362
PDP (policy decision point), 39
PDS (protected distribution system), 167
PEAP (Protected EAP), 73-74
peer-to-peer services, 153-154
pen tests. See penetration testing
penetration testing, 284-287
PEP (policy enforcement point), 39
perfect forward secrecy, 446
performance standards, 110
permissions, 115-116, 375
personal identity verification (PIV) card, 409, 416
personally identifiable information (PII), 147-148
personally owned devices, 152
PGP (Pretty Good Privacy), 462-463
pharming, 226
phishing, 152, 225-226
physical security, 164-165
- access lists, 166
- alarms, 168
- barricades, 167
- biometrics, 167
- fencing, 166
- guards, 167
- hardware locks, 165
- lighting, 166
- mantraps, 165
- motion detection, 168
- protected distribution system (PDS), 167
- proximity readers, 166
- video surveillance, 166

PII (personally identifiable information), 147-148
Ping floods, 217
Pingv6, 61
PIV (personal identity verification) card, 409, 416
PKCS (Public Key Cryptography Standards), 369, 476-477

PKI (public key infrastructure)
  CA (certificate authority), 480
  centralized versus decentralized key management, 484-485
  certificate policies, 481-483
  destruction, 486
  digital certificates, 478-480
  IBE (identity-based encryption), 478
  key escrow, 486
  key recovery, 484
  M of N control, 484
  multiple key pairs, 483
  overview, 473
  RA (registration authority), 481
  revocation, 486-487
  standards, 475-477
  storage, 485
  trust models, 487-488
PKIX working group (IETF), 476
platform-as-a-service (PaaS), 41, 356
plenum, 162
policies
  acceptable use policy, 88, 328
  account policy, 424-425
  backup policies, 186-187
    backup execution/frequency, 188-189
    cold sites, 190
    hot sites, 190
    warm sites, 190
  BYOD (bring your own device), 327
  certificate policies, 481-483
  clean desk policies, 151
  data policies, 376-378
  group policies, 269
  privacy policy, 87
  security policy, 88, 109
policy decision point (PDP), 39
policy enforcement point (PEP), 39
polymorphic viruses, 205, 213
pop-up blockers, 338-339
ports, 65-66
  port scanners, 277
  port stealing, 222
  port zoning, 358
  security, 23
power-level controls, 77-78
Pretty Good Privacy (PGP), 462-463
prevention controls, 169, 271-272
principle of least privilege, 90, 336
principles of influence, 239-240
print services, 304
privacy
  BYOD (bring your own device), 326
  policy, 87
  risk management and, 105-106
private branch exchange (PBX), 37
private classification level, 149
private clouds, 42
private key algorithms, 442
private ports, 65
privileges
  group-based privileges, 431-432
  privilege escalation, 226
  user-assigned privileges, 432
probability, 95
program viruses, 206
protected distribution system (PDS), 167
Protected EAP (PEAP), 73-74
protocol analyzers, 11-12, 275-276
protocol fuzzing, 294
proximity readers, 166
proxy servers, 6-7
ps, 275
public clouds, 43
public data, 149-150
Public Key Cryptography Standards (PKCS), 369, 476-477
public key infrastructure. See PKI

Q-R

qualitative measures, 94
quantitative measures, 94
quantum cryptography, 445

race conditions, 298
RACE Integrity Primitives Evaluation Message Digest (RIPEMD), 456
RADIUS (Remote Authentication Dial-In User Service), 52, 394
RAID (redundant array of independent disks), 180-183
rainbow tables, 229
ransomware, 212-213
RA (registration authority), 481
RAS (Remote Access Services), 37
RBAC. See role-based access control; rule-based access control
RC (Rivest Cipher), 459
realms, 394
reconstitution procedures, 137-138
recovery. See also risk management
  account management, 426
  availability, 197-198
  business continuity concepts, 174
    business continuity planning (BCP), 175-176
    business impact analysis (BIA), 174-175
    continuity of operations, 176
    critical systems and components, 175
    disaster recovery, 176-177
    high availability, 177-178
    IT contingency planning, 177
    redundancy, 178-179
    risk assessment, 176
    single points of failure, 175
    succession planning, 177
    tabletop exercises, 179-180
  confidentiality, 194-195
  control types, 168-170
  disaster recovery, 185-191
  environmental controls, 157
    EMI shielding, 160-162
    environmental monitoring, 163
    fire suppression, 158-160
    hot aisles/cold aisles, 163
    HVAC, 158
    temperature and humidity controls, 164
  integrity, 196-197
  physical security, 164-165
    access lists, 166
    alarms, 168
    barricades, 167
    biometrics, 167
    fencing, 166
    guards, 167
    hardware locks, 165
    lighting, 166
    mantraps, 165
    motion detection, 168
    protected distribution system (PDS), 167
    proximity readers, 166
    video surveillance, 166
  PKI (public key infrastructure), 484
  safety, 198-200
  security-awareness training, 144-145
    compliance, 150-151
    data labeling, handling, and disposal, 150
    information classification levels, 148-149
    metrics, 154
    new threats, 152-153
    peer-to-peer services, 153-154
    personally identifiable information (PII), 147-148
    public data, 149-150
    role-based training, 147
    security policy training, 145-146
    social networking, 153-154
    user habits, 151-152
recovery point objective (RPO), 91, 97-98

recovery procedures, 137-138
recovery time objective (RTO), 91
redundancy, 178-179, 197, 387-388
redundant array of independent disks (RAID), 180-183
registered ports, 65
registration authority (RA), 481
remote access, 37
Remote Access Services (RAS), 37
Remote Authentication Dial-In User Service (RADIUS), 52, 394
remote code execution, 257
remote wiping, 314-315
removable media, 320, 363-365
replay attacks, 220
reporting, 137, 270-271, 280
Reset Account Lockout Counter After policy setting, 427
response. See also risk management
  availability, 197-198
  business continuity concepts, 174
    business continuity planning (BCP), 175-176
    business impact analysis (BIA), 174-175
    continuity of operations, 176
    critical systems and components, 175
    disaster recovery, 176-177
    high availability, 177-178
    IT contingency planning, 177
    redundancy, 178-179
    risk assessment, 176
    single points of failure, 175
    succession planning, 177
    tabletop exercises, 179-180
  confidentiality, 194-195
  control types, 168-170
  disaster recovery, 185-191
  environmental controls, 157
    EMI shielding, 160-162
    environmental monitoring, 163
    fire suppression, 158-160
    hot aisles/cold aisles, 163
    HVAC, 158
    temperature and humidity controls, 164
  integrity, 196-197
  physical security, 164-165
    access lists, 166
    alarms, 168
    barricades, 167
    biometrics, 167
    fencing, 166
    guards, 167
    hardware locks, 165
    lighting, 166
    mantraps, 165
    motion detection, 168
    protected distribution system (PDS), 167
    proximity readers, 166
    video surveillance, 166
  safety, 198-200
  security-awareness training, 144-145
    compliance, 150-151
    data labeling, handling, and disposal, 150
    information classification levels, 148-149
    metrics, 154
    new threats, 152-153
    peer-to-peer services, 153-154
    personally identifiable information (PII), 147-148
    public data, 149-150
    role-based training, 147
    security policy training, 145-146
    social networking, 153-154
    user habits, 151-152
retention policies, 377-378
retina scanning, 415
reusing passwords, 428
reverse social engineering, 235
revocation, 486-487
rights, 115-116
Rinjdael, 459

RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 456

risk management, 83. See also deterrents
  acceptable use policy, 88
  acceptance, 96
  avoidance, 96
  business continuity concepts, 174
    business continuity planning (BCP), 175-176
    business impact analysis (BIA), 174-175
    continuity of operations, 176
    critical systems and components, 175
    disaster recovery, 176-177
    high availability, 177-178
    IT contingency planning, 177
    redundancy, 178-179
    risk assessment, 176
    single points of failure, 175
    succession planning, 177
    tabletop exercises, 179-180
  cloud computing, 96-97
  control types, 85
  deterrence, 96
  disaster recovery, 185-191
  false negatives, 86
  false positives, 85-86
  fault tolerance, 180
    clustering, 183
    hardware, 180
    load balancing, 184
    redundant array of independent disks (RAID), 180-183
    servers, 184
  forensic procedures
    big data analysis, 130-131
    chain of custody, 128-130
    drive imaging, 124
    hashes, 127
    man-hour and expense tracking, 128
    network traffic logs, 125
    order of volatility, 123-124
    screenshots, 127-128
    time offset records, 126
    video capture, 125-126
    witnesses, 128
  incident response
    damage and loss control, 140
    data breaches, 139-140
    escalation and notification, 135-136
    first responder, 138
    incident identification, 135
    incident isolation, 138-139
    lessons learned, 137
    mitigation steps, 136
    preparation, 134-135
    recovery/reconstitution procedures, 137-138
    reporting, 137
  job rotation, 89
  least privilege, 90
  mandatory vacations, 88
  mitigation, 96
  privacy policy, 87
  probability, 95
  qualitative measures, 94
  quantitative measures, 94
  recovery point objective (RPO), 97-98
  recovery time objective (RTO), 97-98
  risk assessment, 176
  risk awareness, 106-107
  risk calculation, 90-91
    annual rate of occurrence (ARO), 92
    annualized loss expectancy (ALE), 92
    impact, 91
    likelihood, 91
    mean time between failures (MTBF), 93-94
    mean time to failure (MTTF), 93
    mean time to repair (MTTR), 93

        single loss expectancy (SLE), 91-92
    risk defined, 90
    risk mitigation
        audits, 116-117
        change management, 114
        data loss prevention (DLP), 117-119
        incident management, 114-115
        technology controls, 118-119
        user rights and permissions reviews, 115-116
    security policy, 88
    separation of duties, 89
    third parties
        applications, 103-104
        compliance and performance standards, 110
        data backups, 108-109
        data ownership, 108
        interoperability agreements, 104-105
        on-boarding/off-boarding business partners, 102-103
        privacy considerations, 105-106
        risk awareness, 106-107
        security policy and procedures, 109
        social media networks, 103-104
        unauthorized data sharing, 107
    threat likelihood, 95
    threat vectors, 95
    transference, 96
    virtualization, 96-97
    vulnerabilities, 94-95

Rivest Cipher (RC), 459

Rivest, Shamir, and Adleman encryption algorithm (RSA), 461

rogue access points, 243-244

role-based access control, 406

role-based training, 147

rootkits, 209-210

round-trip time (RTT), 59

routers, 4-5, 22-23

Routing and Remote Access (RRAS), 37

RPO (recovery point objective), 91, 97-98

RRAS (Routing and Remote Access), 37

RSA (Rivest, Shamir, and Adleman) encryption algorithm, 461

RTO (recovery time objective), 91, 97-98

RTT (round-trip time), 59

rule-based access control (RBAC), 20, 405-406

rules
    firewall rules, 20-21
    RBAC (rule-based access control), 20, 405-406

S

SaaS (software-as-a-service), 41, 356-357

SAFECode (Software Assurance Forum for Excellence in Code), 295

safes, 345-346

safety, 198-200
    closed-circuit television (CCTV), 199
    drills, 199
    escape plans, 199
    escape routes, 200
    fencing, 198
    lighting, 198
    locks, 199
    testing controls, 200

SAML (Security Assertion Markup Language), 398

SAN (storage-area network), 357-358

sandboxing, 349, 383

sanitization, 377

SCADA (supervisory control and data acquisition) systems, 382

Scalable Encryption Processing (SEP) modules, 8

scanning
  heuristic scanning, 337
  port scanners, 277
  vulnerability scanning, 276-277, 285-286
scarcity, 240
SCP (Secure Copy Protocol), 58, 465
screen locks, 317
screenshots, 127-128
sealed storage, 367
secret key algorithms, 442
secure coding concepts, 294-296
  application configuration baseline, 301-302
  application hardening, 302-305
  application patch management, 305-306
  client-side validation, 306-307
  cross-site request forgery prevention, 299-301
  error and exception handling, 296-297
  input validation, 297-298
  NoSQL versus SQL databases, 306
  server-side validation, 306-307
  XSS (cross-site scripting), 298-299
Secure Copy Protocol (SCP), 58, 465
Secure File Transfer Protocol (SFTP), 63
Secure Hash Algorithm (SHA), 456
Secure Hypertext Transport Protocol (S-HTTP), 58
Secure LDAP, 398
Secure Login (slogin), 465
secure network design, 1
  ACL (access control list), 23
  application-aware devices, 15-16
  cloud computing, 41
    community clouds, 43
    hybrid clouds, 43
    infrastructure-as-a-service (IaaS), 42
    platform-as-a-service (PaaS), 41
    private clouds, 42
    public clouds, 43
    software-as-a-service (SaaS), 41
  defense in depth, 44
  DMZ (demilitarized zone), 31-32
  firewalls
    DPI (deep packet inspection) firewalls, 15
    explained, 3
    firewall rules, 20-21
    network firewalls, 14-15
    NGFW (next-generation firewalls), 15
    web application firewalls, 14-15
  flood guards, 24-25
  IDS (intrusion-detection system)
    anomaly-based IDSs, 10-11
    behavior-based IDSs, 10
    heuristic IDSs, 11
    HID (host-based IDS), 9
    NID (network-based IDS), 8-9
    NIP (network-based intrusion-prevention system), 9-10
    signature-based IDSs, 10
  IEEE 802.1X standard, 24
  implicit deny, 25-26
  layered security, 44
  load balancers, 6
  log analysis, 26-27
  loop protection, 25
  NAC (network access control), 39-40
  NAT (Network Address Translation), 36
  network separation, 26
  port security, 23
  protocol analyzers, 11-12
  proxy servers, 6-7
  RBAC (rule-based access control), 20
  remote access, 37
  routers, 4-5, 22-23
  spam filters, 12
  subnetting, 32-34
  switches, 5
  telephony, 37-39

  UTM (unified threat management), 12-14, 27
  virtualization, 40-41
  VLAN (virtual local-area network), 21-22, 34-35
  VPN concentrators, 8
  web security gateways, 7

Secure Shell (SSH), 53-54, 465

Secure Sockets Layer (SSL), 55-56, 463-465

Security Assertion Markup Language (SAML), 398

security assessment tools, 275
  banner grabbing, 278-279
  honeypots, 277
  passive versus active tools, 278
  port scanners, 277
  protocol analyzers, 275-276
  vulnerability scanners, 276-277

security-awareness training, 144-145
  compliance, 150-151
  data labeling, handling, and disposal, 150
  information classification levels, 148-149
  metrics, 154
  new threats, 152-153
  peer-to-peer services, 153-154
  personally identifiable information (PII), 147-148
  public data, 149-150
  role-based training, 147
  security policy training, 145-146
  social networking, 153-154
  user habits, 151-152

security control testing, 349

security guards, 167

security information and event management (SIEM), 119

security logs, 265

security policy, 88, 109, 145-146

security posture, 269-270

security templates, 269

SED (self-encrypting drive), 371

segmentation
  network segmentation, 385-386
  storage segmentation, 319

self-encrypting drive (SED), 371

separation of duties, 89, 403

SEP (Scalable Encryption Processing) modules, 8

server-side validation, 306-307

servers
  DNS servers, 54-55
  fault tolerance, 184
  proxy servers, 6-7

service level agreement (SLA), 104, 177

service packs, 267, 340

service set identifier (SSID), 75

services
  DHCP (Dynamic Host Configuration Protocol), 304-305
  DNS (Domain Name Service), 303
  email services, 303
  file and print services, 304
  FTP (File Transfer Protocol), 303
  NNTP (Network News Transfer Protocol), 303
  web services, 302

session hijacking, 251

Session Initiation Protocol (SIP), 38

session keys, 445-446

SFTP (Secure File Transfer Protocol), 63

SHA (Secure Hash Algorithm), 456

sharing
  shared accounts, 423
  shared secret algorithms, 442
  unauthorized data sharing, 107

shielded twist pair (STP), 162

Shiva Password Authentication Protocol (SPAP), 458

shoulder surfing, 236-237

S-HTTP (Secure Hypertext Transport Protocol), 58

SIEM (security information and event management), 119
signatures
  digital signatures, 196, 447-449
  signature-based IDs, 10
  signature biometrics, 415
Simple Network Management Protocol (SNMP), 52-53, 264
Simpsons, 209
single loss expectancy (SLE), 91-92
single points of failure, 175
single sign-on (SSO), 412
SIP (Session Initiation Protocol), 38
site surveys, 79
SLA (service level agreement), 104, 177
slag code, 211
slash (/) separator, 33
SLE (single loss expectancy), 91-92
slogin (Secure Login), 465
smart cards, 409
smishing, 226
smoke detection, 158
SMS phishing, 226
smurfing, 217
snapshots, 347-348
sniffers, 275
SNMP (Simple Network Management Protocol), 52-53, 264
social engineering attacks
  dumpster diving, 237-238
  explained, 235-236
  hoaxes, 238-239
  impersonation, 238
  principles of influence, 239-240
  shoulder surfing, 236-237
  tailgating, 238
social networking
  risk management, 103-104
  security-awareness training, 153-154
social proof, 239
"soft" systems, 266
software-as-a-service (SaaS), 41, 356-357
software assurance, 295
Software Assurance Forum for Excellence in Code (SAFECode), 295
software exploitation, 306
software zoning, 358
spam, 12, 224-225, 337-338
spanning-tree algorithm, 25
Spanning Tree Protocol (STP), 25
SPAP (Shiva Password Authentication Protocol), 458
spear phishing, 225
spoofing, 223-224
spyware, 207-208, 338
SQL databases, 306
SQL injection, 252
SRK (storage root key), 366-367
SSH (Secure Shell), 53-54, 465
SSID (service set identifier), 75
SSL (Secure Sockets Layer), 55-56, 463-465
SSO (single sign-on), 412
standards
  compliance and performance standards, 110
  PKI (public key infrastructure), 475-477
stateful connections, 56
static environments, 382
  Android systems, 383
  application firewalls, 386
  control redundancy and diversity, 387-388
  embedded systems, 383
  firmware version control, 387
  game consoles, 384
  in-vehicle computing systems, 385
  iOS systems, 383
  mainframes, 384
  manual updates, 387
  network segmentation, 385-386

- supervisory control and data acquisition (SCADA) systems, 382
- wrappers, 387

steganography, 195, 450-451

storage

- cloud storage, 355-357
- PKI (public key infrastructure), 485
- SAN (storage-area network), 357-358
- sealed storage, 367
- segmentation, 319
- storage and retention policies, 377-378

storage root key (SRK), 366-367

Storm botnet, 212

STP (shielded twisted pair), 162

STP (Spanning Tree Protocol), 25

stream ciphers, 444, 459

subnetting, 32-34

succession planning, 177

sudo, 423

supervisory control and data acquisition (SCADA) systems, 382

support ownership (BYOD), 325

switch-based integration, 40

switches, 5

symmetric encryption algorithms, 458-460

symmetric key cryptography, 442-444

SYN floods, 217

System event log, 263-265

system image capture, 124

system logs, 263-265

T

tabletop exercises, 179-180

TACACS (Terminal Access Controller Access Control System), 394-395

tailgating, 152, 238

Target, 139

TCG (Trusted Computing Group), 371

TCO (total cost of ownership), 88

TCP/IP (Transmission Control Protocol/Internet Protocol), 56-57

TCSEC (Trusted Computer System Evaluation Criteria), 335, 405

Teardrop attack, 218

technology controls, 85, 118-119, 170

telephony, 37-39

Telnet, 64

temperature controls, 164

TEMPEST, 161

templates, security, 269

Temporal Key Integrity Protocol (TKIP), 75-76, 455

Terminal Access Controller Access Control System (TACACS), 394-395

testing

- penetration testing, 284-287
- sandboxing, 349
- security control testing, 349
- testing controls, 200

TFTP (Trivial File Transfer Protocol), 64

theft, 117-119

third-party risk

- applications, 103-104
- compliance and performance standards, 110
- data backups, 108-109
- data ownership, 108
- interoperability agreements, 104-105
- on-boarding/off-boarding business partners, 102-103
- privacy considerations, 105-106
- risk awareness, 106-107
- security policy and procedures, 109
- social media networks, 103-104
- unauthorized data sharing, 107

threats, 90

- likelihood, 95
- new threat training, 152-153
- threat vectors, 95

time-of-day restrictions, 406-407

time offset records, 126

TKIP (Temporal Key Integrity Protocol), 75-76, 455
TLS (Transport Layer Security), 55, 463-465
tokens, 408
tools, 275
  banner grabbing, 278-279
  honeypots, 277
  passive versus active tools, 278
  port scanners, 277
  protocol analyzers, 275-276
  vulnerability scanners, 276-277
total cost of ownership (TCO), 88
TPM (Trusted Platform Module), 355, 366-368
traceroute, 59
tracking
  assets, 319
  man-hours and expenses, 128
traffic logs, 125
training (security-awareness), 144-145
  compliance, 150-151
  data labeling, handling, and disposal, 150
  information classification levels, 148-149
  metrics, 154
  new threats, 152-153
  peer-to-peer services, 153-154
  personally identifiable information (PII), 147-148
  public data, 149-150
  role-based training, 147
  security policy training, 145-146
  social networking, 153-154
  user habits, 151-152
transference of risk, 96
Transient Electromagnetic Pulse Emanation Standard, 161
transitive access, 227
transitive trust/authentication, 324, 417
Transmission Control Protocol/Internet Protocol (TCP/IP), 56-57
transmit power control, 78
transport encryption, 447
Transport Layer Security (TLS), 55, 463-465
trends, 271
Triple Data Encryption Standard (3DES), 54, 459
Trivial File Transfer Protocol (TFTP), 64
Trojan horses, 208-209
TrueCrypt, 364
trust, 240
trust models, 487-488
TrustChip, 314
Trusted Computer System Evaluation Criteria (TCSEC), 335, 405
Trusted Computing Group (TCG), 371
trusted operating systems, 342
trusted OS, 412
Trusted Platform Module (TPM), 355, 366-368
twisted-pair cabling, 162
typo squatting, 230-231

U

UAC (User Account Control) technology, 430
ULA (unique local address), 36
unauthorized data sharing, 107
Unicode hash, 457
unified threat management. See UTM (unified threat management)
unique local addresses (ULA), 36
unsealing, 367
unshielded twist pair (UTP), 162
unsolicited entry, 222
updates, manual, 387
urgency, 240
URL filters, 13
URL hijacking, 230-231

USB encryption, 370-371
user access reviews, 433
User Account Control (UAC) technology, 430
user-assigned privileges, 432
user habits, 151-152
user rights and permissions reviews, 115-116
usernames, 416
UTM (unified threat management), 12, 27
  content inspection, 13
  malware inspection, 13-14
  URL filters, 13
UTP (unshielded twist pair), 162

V

vacations, mandatory, 88
validation
  client-side validation, 306-307
  input validation, 297-298
  server-side validation, 306-307
VeriSign, 480
version control, 387
video
  BYOD (bring your own device), 329
  video capture, 125-126
  video surveillance, 166
virtual local-area network (VLAN), 21-22, 34-35
virtual private network (VPN), 8, 80
virtual private storage, 357
virtualization, 40-41, 347
  host availability/elasticity, 348-349
  patch compatibility, 348
  risk management, 96-97
  sandboxing, 349
  security control testing, 349
  snapshots, 347-348
viruses
  antivirus software, 336-337
  armored viruses, 213
  explained, 205-206
  new viruses, 152
vishing, 226
VLAN (virtual local-area network), 21-22, 34-35
vmstat, 275
Voice over IP (VoIP), 37
voiceprint, 415
VoIP (Voice over IP), 37
volatility, order of, 123-124
VPN (virtual private network), 8, 80
vulnerabilities, 90, 94-95, 276-277, 285-286
Vundo, 209

W

war chalking, 75, 244
war driving, 75, 244
warm sites, 190
watering hole attacks, 231
web application firewalls, 14-15
web of trust, 488
web security gateways, 7
web services, 302
well-known ports, 65
WEP (Wired Equivalent Privacy), 72, 245-246, 455
wet-pipe fire-suppression system, 159
whaling, 225
white box testing, 287
white listing, 74, 323-324, 338, 342
whole disk encryption, 360-361
Wi-Fi Protected Access. See WPA
Wi-Fi Protected Setup (WPS), 247
Windows events, 264
wiping data, 314-315, 376-377
Wired Equivalent Privacy (WEP), 72, 245-246, 455
wireless attacks
  bluejacking, 244
  bluesnarfing, 244
  jamming/interference, 243

- near-field communication (NFC), 247-248
- packet sniffing, 245
- rogue access points, 243-244
- war driving, 244
- WEP/WPA attack, 245-246
- WPS attacks, 247

wireless encryption functions, 455-456

wireless networks
- antennas, 76-78
- captive portals, 78
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 76
- Extensible Authentication Protocol (EAP), 73
- Lightweight Extensible Authentication Protocol (LEAP), 74
- MAC filtering, 74-75
- power-level controls, 77-78
- Protected EAP (PEAP), 73-74
- service set identifier (SSID), 75
- site surveys, 79
- Temporal Key Integrity Protocol (TKIP), 75-76
- VPN (virtual private network), 80
- Wi-Fi Protected Access (WPA), 71
- Wired Equivalent Privacy (WEP), 72
- WPA2, 71-72

witnesses, 128

World Wide Numbers (WWN), 358

worms, 207

WPA (Wi-Fi Protected Access), 71, 455
- WEP/WPA attacks, 245-246
- WPA-Enterprise, 455
- WPA-Personal, 455
- WPA2, 71-72, 455-456

WPS (Wi-Fi Protected Setup), 247

wrappers, 367, 387

WWN (World Wide Numbers), 358

X-Y-Z

X.509 standard, 479-480

Xmas Tree attack, 218

XML injection, 252

XSRF (cross-site request forgery) prevention, 299-301

XSS (cross-site scripting), 252, 298-299

XTACACS (Extended Terminal Access Controller Access Control System), 398

zero-day attacks, 153, 253-254

Zimmerman, Phillip R., 462

zombie army, 211

zoning, 358