

David D. Coleman, David A. Westcott, and Bryan Harkins

CWSP[®]

Certified Wireless Security Professional STUDY GUIDE

Second Edition

EXAM CWSP-205

Covers 100% of exam objectives, including Wireless Network Attacks and Threat Assessment, Security Policy, Wireless LAN Security Design and Architecture, and Monitoring and Management

Includes interactive learning environment and study tools with:

- + Online review questions for each chapter
- + 2 bonus online practice exams
- + 150 electronic flashcards
- + Searchable key term glossary
- + Bonus files for chapter exercises

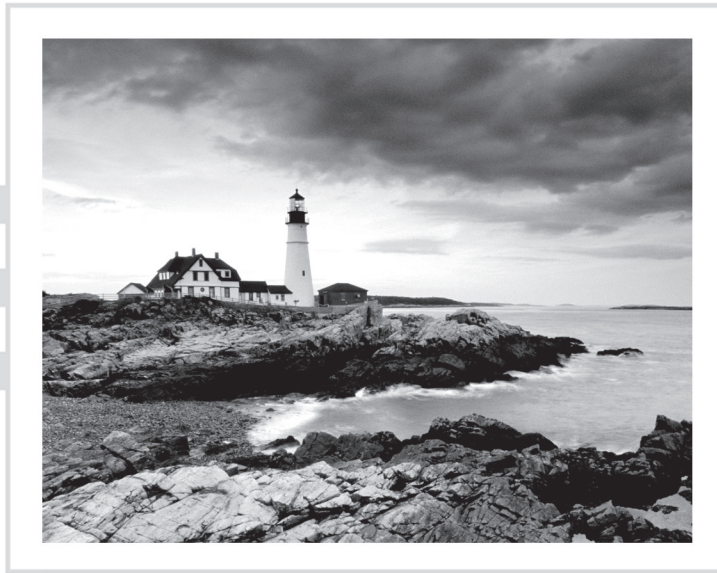


SYBEX
A Wiley Brand

CWSP[®]

Certified Wireless Security Professional

Study Guide CWSP-205
Second Edition



CWSP[®]

Certified Wireless Security

Professional

Study Guide CWSP-205
Second Edition



David D. Coleman
David A. Westcott
Bryan Harkins



Executive Editor: Jim Minatel
Development Editor: Kim Wimpsett
Technical Editors: Chris Lyttle and Ben Wilson
Production Editor: Dassi Zeidel
Copy Editor: Liz Welch
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Book Designers: Judy Fung and Bill Gibson
Proofreader: Rebecca Rider
Indexer: Ted Laux
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: ©Getty Images, Inc./Jeremy Woodhouse

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-21108-2

ISBN: 978-1-119-24413-4 (ebk.)

ISBN: 978-1-119-21109-9 (ebk.)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 9781119211082

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CWSP is a registered trademark of CWNLP, LLC. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

We dedicate this book to the knowledgeable and competent wireless consultants, designers, and installers, and those who are working diligently to become one. You are the front lines of the industry, explaining the technology to customers, including trying to make them understand that more power and more APs often does not mean better WLAN performance. Wireless networking is a shared medium and a shared community, and we are honored to be part of it and to be able to contribute.

Acknowledgments

When we wrote the first edition of the *CWSP Study Guide*, David Coleman's children, Carolina and Brantley, were just entering college. Carolina now holds a master's degree in public policy from the University of Southern California (USC). Brantley graduated from Boston University and is currently working toward his Ph.D. in biochemistry at the University of Washington. David would like to thank his now adult children for years of support and for making their dad very proud. David would also like to thank his mother Marjorie Barnes, stepfather William Barnes, and brother Rob Coleman, for many years of support and encouragement.

David Coleman would also like to thank the entire Aerohive Networks Knowledge Services department. Additionally, David sends many thanks to Matthew Gast, Paul Levasseur, Abby Strong, Gregor Vucajnk, and all of his co-workers at Aerohive Networks (www.aerohive.com). It has been a honor working with you to help build something special.

David Westcott would like to thank Janie for her love and support. I know that my travel and book-writing schedule is difficult to deal with. I say it all of the time and I will continue to say it: "thank you" and "I love you" for your support and for everything that you do for me.

Bryan Harkins would like to thank his wife, Ronda, and his two daughters, Chrystan and Catelynn, and their families, including his three granddaughters, Kaylee, Mikynlee, and Lorali, for allowing him the ability to work with constant travel and the time away from them it has taken to create this book. He would also like to thank his parents for always being there and his brother Chris for getting him involved with IT in the first place. Additionally, he would like to thank Ed Walton, Jeff Manning, and Kent Woodruff for the chance to build something great at Cradlepoint and the team there for their assistance in doing so.

Writing *CWSP: Certified Wireless Security Professional Study Guide* has once again been an adventure. We would like to thank the following individuals for their support and contributions during the entire process.

We must first thank Sybex acquisitions editor Jim Minatel for reaching out to us and encouraging us to write this second edition of our wireless security book. We would also like to thank our development editor, Kim Wimpsett, who has been a pleasure to work with. We also need to send special thanks to our editorial manager, Mary Beth Wakefield; our production editors, Rebecca Anderson and Dassi Zeidel; and Liz Welch, our copyeditor.

We also need to give a big shout-out to our technical editor, Chris Lyttle, CWNE #156. We have personally known Chris for many years. His Wi-Fi background and knowledge were invaluable to providing the amazing technical editing that this book deserved. We encourage you to follow Chris on his blog www.wifikiwi.com or on Twitter: @wifikiwi. And of course, we offer many thanks to our technical proofreader, Ben Wilson. Ben has accumulated years of Wi-Fi experience working for three major WLAN vendors. We encourage you to follow Ben on Twitter: @AirNetworkBen. We would also like to thank Shawn Jackman for his contributions to the first edition of the *CWSP Study Guide*.

We also need to thank Keith Parsons, CWNE #3, and his team at wirelessLAN Professionals. Keith has built a worldwide community of WLAN experts that share knowledge. You can learn more about the wirelessLAN Professionals conferences at www.wlanpros.com. You can also follow Keith on Twitter: @KeithRParsons.

We would also like to thank the CWNP program (www.cwnp.com). All CWNP employees, past and present, should be proud of the internationally renowned wireless certification program that sets the education standard within the enterprise Wi-Fi industry. It has been a pleasure working with all of you the past 16 years.

Finally, we would like to thank Lee Badman for writing his very gracious forward for this book. Lee is also a Wi-Fi expert and he maintains a blog at wirednot.wordpress.com. We encourage you to follow Lee's Wi-Fi question-of-the-day on Twitter via #WIFIQ. You can also follow Lee on Twitter: @wirednot.

About the Authors

David D. Coleman is the Senior Mobility Leader for Aerohive Networks, www.aerohive.com. David collaborates with the Aerohive Knowledge Services team and travels the world for WLAN training sessions and speaking events. He has instructed IT professionals from around the globe in WLAN design, security, administration, and troubleshooting. David has written multiple books, blogs, and white papers about wireless networking, and he is considered an authority on 802.11 technology. Prior to working at Aerohive, he specialized in corporate and government Wi-Fi training and consulting. In the past he has provided WLAN training for numerous private corporations, the US military, and other federal and state government agencies. When he is not traveling, David resides in both Atlanta, Georgia and Seattle, Washington. David is CWNE #4, and he can be reached via email at mistermultipath@gmail.com. Please follow David on Twitter: [@mistermultipath](https://twitter.com/mistermultipath).

David Westcott is an independent consultant and technical trainer with over 31 years of experience. David has been a certified trainer for over 23 years, and he specializes in wireless networking, wireless management and monitoring, and network access control. He has provided training to thousands of students at government agencies, corporations, and universities in over 30 countries around the world. David was an adjunct faculty member for Boston University's Corporate Education Center for over 10 years. David has written seven books as well as numerous white papers, and he has developed many courses on wired and wireless networking technologies and networking security.

David was a member of the original CWNE Roundtable. David is CWNE #7 and has earned certifications from many companies, including Cisco, Aruba, Microsoft, Ekahau, EC-Council, CompTIA, and Novell. David lives in Concord, Massachusetts with his wife Janie, his step-daughters Jennifer and Samantha, and his granddaughter Savannah. David can be reached via email at david@westcott-consulting.com. Please follow David on Twitter: [@davidwestcott](https://twitter.com/davidwestcott).

Bryan Harkins has over 30 years experience in the IT field. He has been involved in areas ranging from customer support and sales to network security and design. He has developed custom curriculum for government agencies and Fortune 500 companies alike and delivers both public and private wireless security classes around the world. Previously, Bryan worked as the senior global enablement leader for Aerohive Networks and as the training and courseware development manager for Motorola AirDefense (now Zebra). Currently, Bryan is the Director of Cradlepoint University, where he oversees the training department of Cradlepoint, www.Cradlepoint.com. Bryan also serves on the Board of Advisors for 802Secure, www.802secure.com.

Bryan has presented at multiple industry conferences, including IP Expo, Secure World Expo, Armed Forces Communications and Electronics Association (AFCEA) events, and Microsoft Broad Reach events. He holds a degree in aviation from Georgia State University. He is also a member of the CWNE Roundtable as well as a member of the CWNE Advisory Board. Bryan is CWNE #44, and he can be followed on Twitter: [@80211University](https://twitter.com/80211University).

Contents at a Glance

<i>Foreword</i>		<i>xxv</i>
<i>Introduction</i>		<i>xxvii</i>
<i>Assessment Test</i>		<i>xxxviii</i>
Chapter 1	WLAN Security Overview	1
Chapter 2	Legacy 802.11 Security	29
Chapter 3	Encryption Ciphers and Methods	61
Chapter 4	802.1X/EAP Authentication	87
Chapter 5	802.11 Layer 2 Dynamic Encryption Key Generation	151
Chapter 6	PSK Authentication	193
Chapter 7	802.11 Fast Secure Roaming	215
Chapter 8	WLAN Security Infrastructure	257
Chapter 9	RADIUS and LDAP	291
Chapter 10	Bring Your Own Device (BYOD) and Guest Access	319
Chapter 11	Wireless Security Troubleshooting	365
Chapter 12	Wireless Security Risks	397
Chapter 13	Wireless LAN Security Auditing	439
Chapter 14	Wireless Security Monitoring	469
Chapter 15	Wireless Security Policies	517
Appendix A	Answers to Review Questions	553
Appendix B	Abbreviations and Acronyms	597
<i>Index</i>		<i>615</i>

Contents

<i>Foreword</i>		<i>xxv</i>
<i>Introduction</i>		<i>xxvii</i>
<i>Assessment Test</i>		<i>xxxviii</i>
Chapter 1	WLAN Security Overview	1
	Standards Organizations	3
	International Organization for Standardization (ISO)	3
	Institute of Electrical and Electronics Engineers (IEEE)	4
	Internet Engineering Task Force (IETF)	5
	Wi-Fi Alliance	7
	802.11 Networking Basics	12
	802.11 Security Basics	14
	Data Privacy	14
	Authentication, Authorization, Accounting (AAA)	16
	Segmentation	17
	Monitoring	17
	Policy	18
	802.11 Security History	18
	802.11i Security Amendment and WPA Certifications	18
	Robust Security Network (RSN)	20
	Summary	21
	Exam Essentials	22
	Review Questions	24
Chapter 2	Legacy 802.11 Security	29
	Authentication	30
	Open System Authentication	31
	Shared Key Authentication	33
	Wired Equivalent Privacy (WEP) Encryption	35
	TKIP	40
	Virtual Private Networks (VPNs)	44
	Point-to-Point Tunneling Protocol (PPTP)	46
	Layer 2 Tunneling Protocol (L2TP)	46
	Internet Protocol Security (IPsec)	47
	Secure Sockets Layer (SSL)	47
	VPN Configuration Complexity	48
	VPN Scalability	48
	MAC Filters	49
	SSID Segmentation	50
	SSID Cloaking	51

	Summary	54
	Exam Essentials	55
	Review Questions	56
Chapter 3	Encryption Ciphers and Methods	61
	Encryption Basics	62
	Symmetric and Asymmetric Algorithms	63
	Stream and Block Ciphers	65
	RC4/ARC4	66
	RC5	66
	DES	66
	3DES	67
	AES	67
	WLAN Encryption Methods	68
	WEP	70
	WEP MPDU	70
	TKIP	72
	TKIP MPDU	72
	CCMP	73
	CCMP MPDU	76
	WPA/WPA2	78
	Future Encryption Methods	79
	Proprietary Layer 2 Implementations	80
	Summary	80
	Exam Essentials	81
	Review Questions	82
Chapter 4	802.1X/EAP Authentication	87
	WLAN Authentication Overview	89
	AAA	90
	Authentication	91
	Authorization	92
	Accounting	93
	802.1X	95
	Supplicant	96
	Authenticator	99
	Authentication Server	102
	Supplicant Credentials	106
	Usernames and Passwords	106
	Digital Certificates	107
	Protected Access Credentials (PACs)	109
	One-Time Passwords	109
	Smart Cards and USB Tokens	110
	Machine Authentication	112

802.1X/EAP and Certificates	114
Server Certificates and Root CA Certificates	115
Client Certificates	119
Shared Secret	120
Legacy Authentication Protocols	121
PAP	121
CHAP	121
MS-CHAP	121
MS-CHAPv2	121
EAP	122
Weak EAP Protocols	125
EAP-MD5	125
EAP-LEAP	126
Strong EAP Protocols	128
EAP-PEAP	130
EAP-TTLS	133
EAP-TLS	134
EAP-FAST	136
Miscellaneous EAP Protocols	141
EAP-SIM	141
EAP-AKA	141
EAP-TEAP	142
Summary	144
Exam Essentials	144
Review Questions	146

Chapter 5	802.11 Layer 2 Dynamic Encryption	
	Key Generation	151
	Advantages of Dynamic Encryption	152
	Robust Security Network (RSN)	156
	RSN Information Element	161
	Authentication and Key Management (AKM)	166
	RSNA Key Hierarchy	170
	4-Way Handshake	174
	Group Key Handshake	177
	PeerKey Handshake	179
	TDLS Peer Key Handshake	180
	RSNA Security Associations	181
	Passphrase-to-PSK Mapping	182
	Roaming and Dynamic Keys	183
	Summary	184
	Exam Essentials	184
	Review Questions	186

Chapter 6	PSK Authentication	193
	WPA/WPA2-Personal	194
	Preshared Keys (PSK) and Passphrases	195
	WPA/WPA2-Personal Risks	200
	Entropy	201
	Proprietary PSK	203
	Simultaneous Authentication of Equals (SAE)	205
	Summary	208
	Exam Essentials	208
	Review Questions	209
Chapter 7	802.11 Fast Secure Roaming	215
	History of 802.11 Roaming	216
	Client Roaming Thresholds	217
	AP-to-AP Handoff	218
	RSNA	220
	PMKSA	221
	PMK Caching	224
	Preauthentication	225
	Opportunistic Key Caching (OKC)	227
	Proprietary FSR	230
	Fast BSS Transition (FT)	231
	Information Elements	235
	FT Initial Mobility Domain Association	236
	Over-the-Air Fast BSS Transition	238
	Over-the-DS Fast BSS Transition	239
	802.11k	243
	802.11v	246
	Voice Enterprise	247
	Layer 3 Roaming	248
	Troubleshooting	250
	Summary	251
	Exam Essentials	251
	Review Questions	253
Chapter 8	WLAN Security Infrastructure	257
	802.11 Services	258
	Integration Service (IS)	258
	Distribution System (DS)	259
	Management, Control, and Data Planes	259
	Management Plane	260
	Control Plane	260
	Data Plane	261

WLAN Architecture	261
Autonomous WLAN Architecture	261
Centralized Network Management Systems	263
Cloud Networking	265
Centralized WLAN Architecture	265
Distributed WLAN Architecture	270
Unified WLAN Architecture	272
Hybrid Architectures	272
Enterprise WLAN Routers	272
WLAN Mesh Access Points	273
WLAN Bridging	274
VPN Wireless Security	275
VPN 101	275
Layer 3 VPNs	277
SSL VPN	278
VPN Deployment	278
Infrastructure Management	279
Protocols for Management	280
Summary	285
Exam Essentials	285
Review Questions	286
Chapter 9	RADIUS and LDAP
	291
LDAP	292
RADIUS	293
Authentication and Authorization	294
Accounting	295
RADIUS Configuration	296
LDAP Proxy	298
RADIUS Deployment Models	299
RADIUS Proxy	303
RADIUS Proxy and Realms	304
RADIUS Failover	305
WLAN Devices as RADIUS Servers	306
Captive Web Portal and MAC Authentication	306
RadSec	307
Attribute-Value Pairs	307
Vendor-Specific Attributes	308
VLAN Assignment	309
Role-Based Access Control	310
LDAP Attributes	311
Summary	311
Exam Essentials	311
Review Questions	313

Chapter 10	Bring Your Own Device (BYOD) and Guest Access	319
	Mobile Device Management	322
	Company-Issued Devices vs. Personal Devices	323
	MDM Architecture	324
	MDM Enrollment	325
	MDM Profiles	329
	MDM Agent Software	331
	Over-the-Air Management	332
	Application Management	335
	Self-Service Device Onboarding for Employees	336
	Dual-SSID Onboarding	337
	Single-SSID Onboarding	338
	MDM vs. Self-Service Onboarding	339
	Guest WLAN Access	339
	Guest SSID	340
	Guest VLAN	340
	Guest Firewall Policy	341
	Captive Web Portals	342
	Client Isolation, Rate Limiting, and Web Content Filtering	345
	Guest Management	345
	Guest Self-Registration	347
	Employee Sponsorship	348
	Social Login	349
	Encrypted Guest Access	351
	Network Access Control (NAC)	352
	Posture	352
	OS Fingerprinting	353
	AAA	354
	RADIUS Change of Authorization	355
	Single Sign-On	356
	Summary	358
	Exam Essentials	359
	Review Questions	360
Chapter 11	Wireless Security Troubleshooting	365
	Five Tenets of WLAN Troubleshooting	366
	Troubleshooting Best Practices	366
	Troubleshoot the OSI Model	369
	Most Wi-Fi Problems Are Client Issues	370
	Proper WLAN Design Reduces Problems	372
	WLAN Always Gets the Blame	372
	PSK Troubleshooting	372

	802.1X/EAP Troubleshooting	374
	802.1X/EAP Troubleshooting Zones	375
	Zone 1: Backend Communication Problems	376
	Zone 2: Supplicant Certificate Problems	378
	Zone 2: Supplicant Credential Problems	380
	Roaming Troubleshooting	382
	VPN Troubleshooting	384
	Summary	387
	Exam Essentials	387
	Review Questions	388
Chapter 12	Wireless Security Risks	397
	Unauthorized Rogue Access	398
	Rogue Devices	398
	Rogue Prevention	402
	Eavesdropping	404
	Casual Eavesdropping	404
	Malicious Eavesdropping	406
	Eavesdropping Risks	407
	Eavesdropping Prevention	409
	Authentication Attacks	409
	Denial-of-Service Attacks	411
	Layer 1 DoS Attacks	412
	Layer 2 DoS Attacks	416
	MAC Spoofing	420
	Wireless Hijacking	423
	Management Interface Exploits	427
	Vendor Proprietary Attacks	428
	Physical Damage and Theft	428
	Social Engineering	430
	Guest Access and WLAN Hotspots	432
	Summary	433
	Exam Essentials	433
	Review Questions	434
Chapter 13	Wireless LAN Security Auditing	439
	WLAN Security Audit	440
	OSI Layer 1 Audit	442
	OSI Layer 2 Audit	447
	Penetration Testing	449
	Wired Infrastructure Audit	453
	Social Engineering Audit	453

	WIPS Audit	454
	Documenting the Audit	455
	Audit Recommendations	456
	WLAN Security Auditing Tools	457
	Linux-Based Tools	459
	Summary	462
	Exam Essentials	463
	Review Questions	464
Chapter 14	Wireless Security Monitoring	469
	Wireless Intrusion Detection and Prevention Systems (WIDS and WIPS)	470
	WIDS/WIPS Infrastructure Components	471
	WIDS/WIPS Architecture Models	474
	Multiple Radio Sensors	478
	Sensor Placement	479
	Proprietary WIPS	480
	Device Classification	482
	Rogue Detection	484
	Rogue Mitigation	488
	Device Tracking	491
	WIDS/WIPS Analysis	496
	Signature Analysis	496
	Behavioral Analysis	497
	Protocol Analysis	498
	Spectrum Analysis	500
	Forensic Analysis	501
	Performance Analysis	502
	Monitoring	503
	Policy Enforcement	503
	Alarms and Notification	505
	False Positives	507
	Reports	508
	802.11n/ac	508
	802.11w	510
	Summary	511
	Exam Essentials	511
	Review Questions	513
Chapter 15	Wireless Security Policies	517
	General Policy	519
	Policy Creation	519
	Policy Management	522
	Functional Policy	523
	Password Policy	524
	RBAC Policy	525

	Change Control Policy	526
	Authentication and Encryption Policy	526
	WLAN Monitoring Policy	527
	Endpoint Policy	527
	Acceptable Use Policy	528
	Physical Security	529
	Remote Office Policy	529
	Government and Industry Regulations	530
	The U.S. Department of Defense (DoD) Directive 8420.1	531
	Federal Information Processing Standards (FIPS) 140-2	532
	The Sarbanes-Oxley Act of 2002 (SOX)	534
	Graham-Leach-Bliley Act (GLBA)	536
	Health Insurance Portability and Accountability Act (HIPAA)	538
	Payment Card Industry (PCI) Standard	540
	Compliance Reports	543
	802.11 WLAN Policy Recommendations	544
	Summary	545
	Exam Essentials	545
	Review Questions	547
Appendix A	Answers to Review Questions	553
	Chapter 1: WLAN Security Overview	554
	Chapter 2: Legacy 802.11 Security	556
	Chapter 3: Encryption Ciphers and Methods	558
	Chapter 4: 802.1X/EAP Authentication	561
	Chapter 5: 802.11 Layer 2 Dynamic Encryption Key Generation	563
	Chapter 6: PSK Authentication	567
	Chapter 7: 802.11 Fast Secure Roaming	570
	Chapter 8: WLAN Security Infrastructure	573
	Chapter 9: RADIUS and LDAP	576
	Chapter 10: Bring Your Own Device (BYOD) and Guest Access	578
	Chapter 11: Wireless Security Troubleshooting	581
	Chapter 12: Wireless Security Risks	584
	Chapter 13: Wireless LAN Security Auditing	587
	Chapter 14: Wireless Security Monitoring	590
	Chapter 15: Wireless Security Policies	594
Appendix B	Abbreviations and Acronyms	597
	Certifications	598
	Organizations and Regulations	598
	Measurements	599
	Technical Terms	599
	<i>Index</i>	615

Table of Exercises

Exercise 2.1	Viewing Open System and Shared Key Authentication Frames	34
Exercise 2.2	Viewing Encrypted MSDU Payload of 802.11 Data Frames	39
Exercise 2.3	TKIP-Encrypted Frames	44
Exercise 2.4	Viewing Hidden SSIDs	53
Exercise 3.1	CCMP Encrypted Frames	77
Exercise 4.1	802.1X/EAP Frame Exchanges	142
Exercise 5.1	Dynamic WEP	155
Exercise 5.2	Authentication and Key Management	170
Exercise 5.3	The 4-Way Handshake	177
Exercise 6.1	Passphrase-PSK Mapping	198
Exercise 7.1	FT Initial Mobility Domain Association	237
Exercise 7.2	Over-the-Air Fast BSS Transition	240
Exercise 7.3	Radio Resource Management and Neighbor Reports	245

Foreword

Though wireless security options haven't changed significantly since the introduction of 802.11i, the world in which they function certainly has. We are living in strange times for wireless networking. Though our WLAN standards are bringing ever-faster connectivity and more networked devices are coming without Ethernet ports, today's Wi-Fi practitioner operates in a hyper-nuanced security landscape. The media has no shortage of gloom and doom to report on network data breaches, yet many of today's wireless clients are delivered with outdated or limited security capabilities. Where client devices are capable of supporting robust security, users may well opt for ease of use over security. In other situations, WLAN professionals might find themselves being asked to provide an expensive and complicated multitiered security strategy in an environment where there's very little to really protect. Today's CWSPs need be savvy in not only their range of security solutions and analysis tools, but also in how to choose the right option (or combination of options) for complicated situations with diverse user groups and WLAN client devices.

For those just embarking on a wireless career, or for seasoned professionals trying to broaden their knowledge base, I applaud you for choosing this text. From captive portals to VPN, and MDM solutions to WIPS, the authors give you a knowledge base foundation on which you can build an operational career. David Coleman, Bryan Harkins, and David Westcott bring you decades of wireless security knowledge that spans the gamut from wardriving to Hotspot 2.0. CWSP helps you understand the strengths and disadvantages of any security option you're likely to be faced with in today's real world. It doesn't matter whether you're a one-person company servicing the SMB market or if you support a giant corporate WLAN, you'll do well for yourself and your clients by learning what CWSP has to offer. BYOD, IoT, legacy WLAN concerns—it's all here.

As a long-time wireless professional, I can promise you that there are no shortcuts to building high-quality networks. Good networks support operational goals, and good wireless experts help to make sure those goals are clearly defined and understood before they can be matched with the right solution. When it comes to WLAN security, there are no silver bullets or one-size-fits-all solutions. Thankfully, you're in good hands with David, Bryan, and David as you learn how to think about the broad topic of WLAN security. Best of luck to you.

Lee Badman
CWNA, CWSP, CWDP
Network Architect

Introduction

If you have purchased this book or if you are even thinking about purchasing this book, you probably have some interest in taking the CWSP® (Certified Wireless Security Professional) certification exam or in learning what the CWSP certification exam is about. The authors would like to congratulate you on this first step, and we hope that our book can help you on your journey. Wireless local area networking (WLAN) is currently one of the hottest technologies on the market. Security is an important and mandatory aspect of 802.11 wireless technology. As with many fast-growing technologies, the demand for knowledgeable people is often greater than the supply. The CWSP certification is one way to prove that you have the knowledge and skills to secure 802.11 wireless networks successfully. This study guide is written with that goal in mind.

This book is designed to teach you about WLAN security so that you have the knowledge needed not only to pass the CWSP certification test, but also to be able to design, install, and support wireless networks. We have included review questions at the end of each chapter to help you test your knowledge and prepare for the exam. Extra training resources such as lab materials and presentations are available for download from the book's online resource area, which can be accessed at www.wiley.com/go/sybextestprep.

Before we tell you about the certification process and its requirements, we must mention that this information may have changed by the time you are taking your test. We recommend that you visit www.cwnp.com as you prepare to study for your test to check out the current objectives and requirements.



Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

About CWSP® and CWNP®

If you have ever prepared to take a certification test for a technology with which you are unfamiliar, you know that you are not only studying to learn a different technology, but you are also probably learning about an industry with which you are unfamiliar. Read on and we will tell you about the CWNP Program. CWNP is an abbreviation for *Certified Wireless Network Professional*. There is no CWNP test. The CWNP Program develops courseware and certification exams for wireless LAN technologies in the computer networking industry. The CWNP Program certification path is vendor-neutral.

The objective of the CWNP Program is to certify people on wireless networking, not on a specific vendor's product. Yes, at times the authors of this book and the creators of the certification will talk about or even demonstrate how to use a specific product; however, the goal is the overall understanding of wireless technology, not the product itself. If you

learned to drive a car, you physically had to sit and practice in one. When you think back and reminisce, you probably do not tell anyone that you learned to drive a Ford; you probably say you learned to drive using a Ford.

There are seven wireless certifications offered by the CWNP Program:

CWTS™: Certified Wireless Technology Specialist The CWTS certification is an entry-level certification for sales professionals, project managers, and networkers who are new to enterprise Wi-Fi. This certification is geared specifically toward both WLAN sales and support staff for the enterprise WLAN industry. The CWTS certification exam (PW0-071) verifies that sales and support staffs are specialists in WLAN technology and have all the fundamental knowledge, tools, and terminology to sell and support WLAN technologies more effectively.

CWNA®: Certified Wireless Network Administrator The CWNA certification is a foundation-level Wi-Fi certification; however, it is not considered an entry-level technology certification. Individuals taking this exam (CWNA-106) typically have a solid grasp on network basics such as the OSI model, IP addressing, PC hardware, and network operating systems. Many candidates already hold other industry-recognized certifications, such as the CompTIA Network+ or Cisco CCNA, and are looking for the CWNA certification to enhance or complement existing skills.

CWSP®: Certified Wireless Security Professional The CWSP certification exam (CWSP-205) is focused on standards-based wireless security protocols, security policy, and secure wireless network design. This certification introduces candidates to many of the technologies and techniques that intruders use to compromise wireless networks and that administrators use to protect wireless networks. With recent advances in wireless security, WLANs can be secured beyond their wired counterparts.

CWAP®: Certified Wireless Analyst Professional The CWAP certification exam (CWAP-402) is a professional-level career certification for networkers who are already CWNA certified and have a thorough understanding of RF technologies and applications of 802.11 networks. This certification provides an in-depth look at 802.11 operations and prepares WLAN professionals to be able to perform, interpret, and understand wireless packet and spectrum analysis.

CWDP®: Certified Wireless Design Professional The CWDP certification exam (CWDP-302) is a professional-level career certification for networkers who are already CWNA certified and have a thorough understanding of RF technologies and applications of 802.11 networks. This certification prepares WLAN professionals to properly design wireless LANs for different applications to perform optimally in different environments.

CWNE®: Certified Wireless Network Expert The CWNE certification is the highest-level certification in the CWNP program. By successfully completing the CWNE requirements, you will have demonstrated that you have the most advanced skills available in today's wireless LAN market. The CWNE certification requires CWNA, CWAP, CWDP, and CWAP certifications. To earn the CWNE certification, a rigorous application must be submitted and approved by CWNP's review team.