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

CWSP®

Certified Wireless Security Professional

STUDY GUIDE

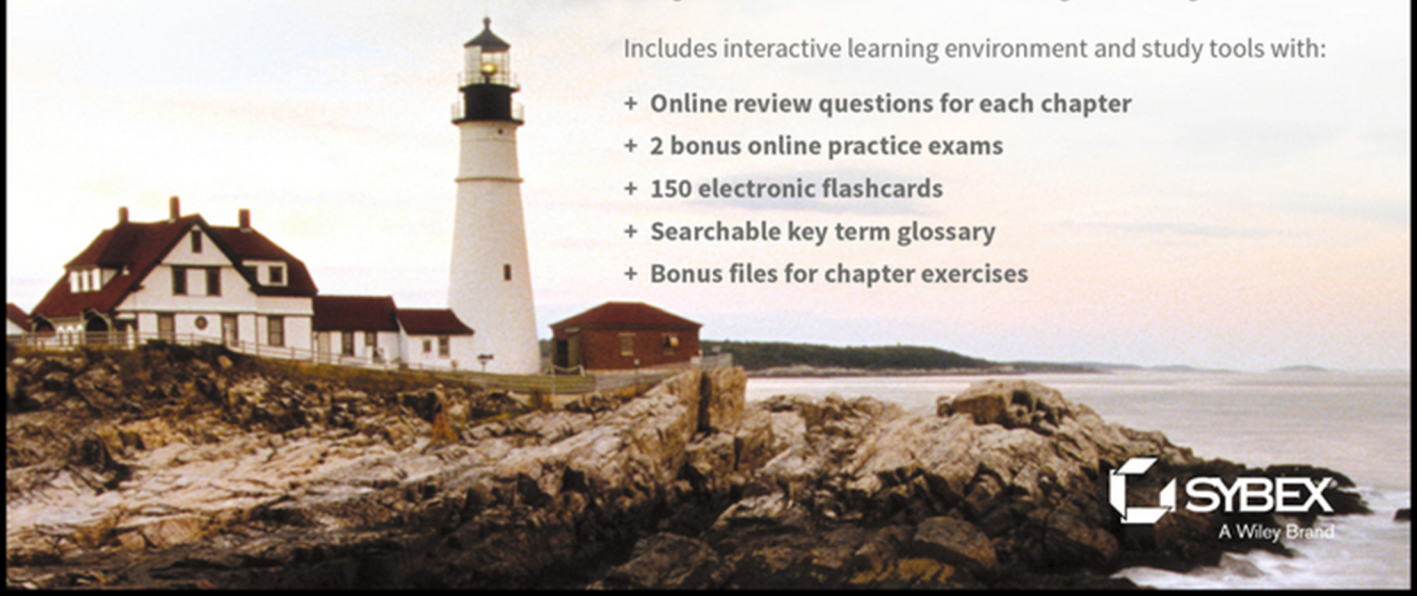
Second Edition

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

SYBEX®
A Wiley Brand

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

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

Library of Congress Control Number: 9781119211082

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.

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 stepdaughters Jennifer and Samantha, and his granddaughter Savannah. David can be reached via email at david@westcott-consulting.com. Please follow David on Twitter: @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.

Contents at a Glance

Contents

Table of Exercises

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 profressionals 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 foundationon 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.