"Walks you through wireless security fundamentals, attack methods, and remediation tactics in an easy-to-read format with real-world case studies. Never has it been so important for the industry to get its arms around wireless security, and this book is a great way to do that." —*Jason R. Lish, Director, IT Security, Honeywell International*

Second Edition

HACKING Wireless EXPOSED™

Wireless Security Secrets & Solutions

Johnny Cache, Joshua Wright, and Vincent Liu

McGraw Hill

"Finally, a comprehensive look at wireless security, from Wi-Fi to emerging wireless protocols not covered elsewhere, addressing the spectrum of wireless threats facing organizations today."
—Mike Kershaw, author of Kismet

"A practical guide to evaluating today's wireless networks. The authors' clear instruction and lessons learned are useful for all levels of security professionals."
—Brian Soby, Product Security Director
salesforce.com

"The introduction of wireless networks in many enterprises dramatically reduces the effectiveness of perimeter defenses because most enterprises depend heavily on firewall technologies for risk mitigation. These mitigation strategies may be ineffective against wireless attacks. With outsiders now gaining insider access, an enterprise's overall risk profile may change dramatically. This book addresses those risks and walks the readers through wireless security fundamentals, attack methods, and remediation tactics in an easy-to-read format with real-world case studies. Never has it been so important for the industry to get their arms around wireless security, and this book is a great way to do that."
—Jason R. Lish, Director, IT Security
Honeywell International

"The authors have distilled a wealth of complex technical information into comprehensive and applicable wireless security testing and action plans. This is a vital reference for anyone involved or interested in securing wireless networking technologies."
—David Doyle, CISM, CISSP, Sr. Manager, IT Security & Compliance
Hawaiian Airlines, Inc.

"Hacking Exposed Wireless is simply absorbing. Start reading this book and the only reason you will stop reading is because you finished it or because you want to try out the tips and techniques for yourself to start protecting your wireless systems."
—Thomas d'Otreppe de Bouvette, author of Aircrack-ng

This page intentionally left blank

HACKING EXPOSED™ WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS

SECOND EDITION

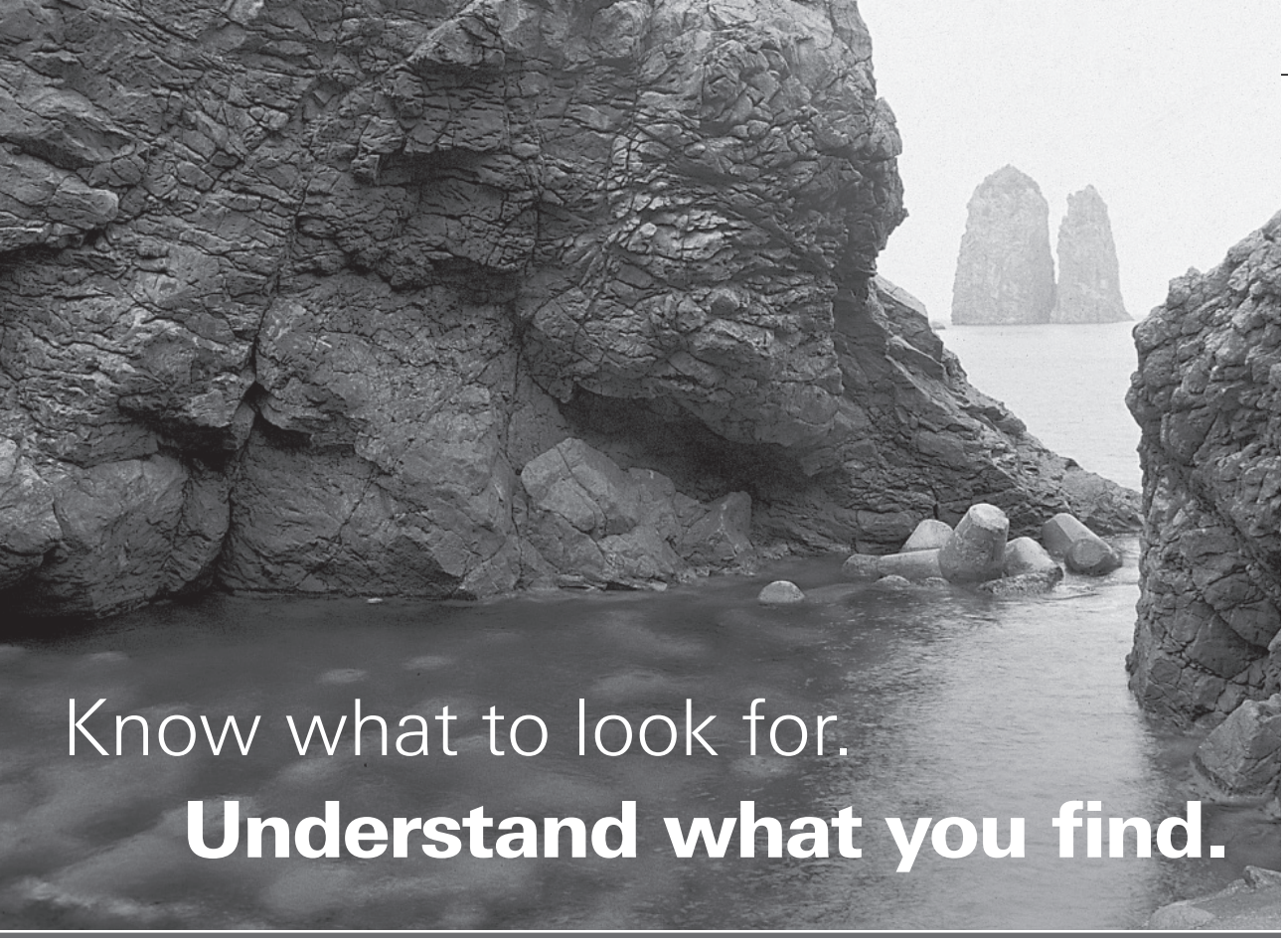
JOHNNY **CACHE**
JOSHUA **WRIGHT**
VINCENT **LIU**

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

ISBN: 978-0-07-166662-6

MHID: 0-07-166662-1

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-166661-9, MHID: 0-07-166661-3.



Now that you've discovered *Hacking Exposed: Wireless*, find out why businesses depend on Stach & Liu for practical advice and effective, real-world security services.

How is Stach & Liu different? Simple. We understand how security impacts business. That's why companies throughout the Fortune 1000 trust us to improve their ability to protect themselves from attack, while also increasing the efficiency of existing IT and security investments.

We don't sell hardware or software. Just our insight and expertise, direct and to the point. With a no-nonsense approach to education and knowledge transfer.

Stach & Liu understands the business of security. To find out more, visit us at **www.stachliu.com**.

ABOUT THE AUTHORS

Johnny Cache

Johnny Cache received his Masters in Computer Science from the Naval Postgraduate School in 2006. His thesis work, which focused on fingerprinting 802.11 device drivers, won the Gary Kildall award for the most innovative computer science thesis. Johnny wrote his first program on a Tandy 128K color computer sometime in 1988. Since then, he has spoken at several security conferences including BlackHat, BlueHat, and Toorcon. He has also released a number of papers related to 802.11 security and is the author of many wireless tools. Most of his wireless utilities are included in the Airbase suite, available at *802.11mercenary.net*. Johnny is currently employed by Harris Corporation as a wireless engineer.

Joshua Wright

Joshua Wright is a senior security analyst with InGuardians, Inc., an information security research and consulting firm, and a senior instructor and author with the SANS Institute. A regular speaker at information security and hacker conferences, Joshua has contributed numerous research papers and hacking tools to the open source community. Through his classes, consulting engagements, and presentations, Joshua reaches out to thousands of organizations each year, providing guidance on penetration testing, vulnerability assessment, and securing complex technologies. Joshua holds a Bachelor of Science from Johnson & Wales University with a major in information science. In his spare time, he enjoys spending time with his family, when he teaches his kids to always start counting from zero.

Vincent Liu

Vincent Liu is a Managing Partner at Stach & Liu, a security consulting firm providing IT security services to the Fortune 1000 and global financial institutions as well as U.S. and foreign governments. Before founding Stach & Liu, Vincent led the Attack & Penetration and Reverse Engineering teams for the Global Security unit at Honeywell International. Prior to that, he was a consultant with the Ernst & Young Advanced Security Centers and an analyst at the National Security Agency. He is currently co-authoring the upcoming *Hacking Exposed: Web Applications, Third Edition*. Vincent holds a Bachelor of Science and Engineering from the University of Pennsylvania with a major in Computer Science and Engineering and a minor in Psychology.

ABOUT THE CONTRIBUTING AUTHORS

Eric Scott, CISSP, is a Security Associate at Stach & Liu, a security consulting firm providing IT security services to the Fortune 1000 and global financial institutions as well as U.S. and foreign governments.

Before joining Stach & Liu, Eric served as a Security Program Manager in the Trustworthy Computing group at Microsoft Corporation. In this role, he was responsible for managing and conducting in-depth risk assessments against critical business assets in observance of federal, state, and industry regulations. In addition, he was responsible for developing remediation plans and providing detailed guidance around areas of potential improvement.

Brad Antoniewiecz is the leader of Foundstone's network vulnerability and assessment penetration service lines. He is a senior security consultant with a focus on internal, external, web application, device, and wireless vulnerability assessments and penetration testing. Antoniewicz developed Foundstone's Ultimate Hacking: Wireless class and teaches both Ultimate Hacking: Wireless and the traditional Ultimate Hacking classes. Brad has spoken at many events, authored various articles and whitepapers, is a contributing author to *Hacking Exposed: Network Security Secrets & Solutions,* and developed many of Foundstone's internal assessment tools.

ABOUT THE TECHNICAL EDITORS

Joshua Wright, Johnny Cache, and Vincent Liu technically edited one another's chapters.

Christopher Wang, aka "Akiba," runs the FreakLabs Open Source ZigBee Project. He's currently implementing an open source ZigBee protocol stack and open hardware development boards for people who want to customize their ZigBee devices and networks. He also runs a blog and wireless sensor network (WSN) newsfeed from his site at *http://www.freaklabs.org/* and hopes that someday wireless sensor networks will be both useful and secure. Christopher supplied valuable feedback and corrections for Chapter 11, "Hack ZigBee."

To my parents, for having the foresight to realize that breaking into computers would be a growth industry.
—Jon

To Jen, Maya, and Ethan, for always believing in me.
—Josh

To my parents, for their countless sacrifices so that I could have opportunity.
—*Vinnie*

This page intentionally left blank

AT A GLANCE

This page intentionally left blank

CONTENTS

Part II Hacking 802.11 Clients

Part III Hacking Additional Wireless Technologies

This page intentionally left blank

FOREWORD

Thinking back, I must have been in fifth grade at Jack Harvey Elementary School at the time. Always a little bit short as a kid, I had to stand on my tippy toes in the school library to reach the shelf of biographies that I read each week. I distinctly remember reading about Ben Franklin, Betsy Ross, Thomas Edison, and Gandhi. But of all the biographies I devoured back then, there was one that totally enthralled me—the life story of Nikola Tesla.

The enigmatic inventor's picture on the cover of the book was arresting—deep-set eyes, funky hair, and lightning bolts emanating all around him during his heyday in the early 1900s. The back cover illustration actually showed Tesla shooting lightning bolts out of his eyeballs! That sealed the deal for me. How could you *not* read a book with a dude who shoots lightning-bolts out of his eyes?

As I turned the pages, Tesla's ideas sparked my imagination. Electricity! Wireless! Power! Amps and volts, wires and wireless, all built up through Tesla's genius to X-rays, wireless power transmission, a vision of futuristic battles fought with electricity zapping airships in the sky, resonance experiments to shake buildings or shatter the very crust of the Earth itself, and much more. I was inspired by Tesla, a steampunk wizard of electricity, a real-life Willy Wonka devoted to electrons and photons instead of chocolates.

In my crude home lab, I started to build little electric circuits on my own. Nothing too Earth shattering, of course. Just a breadboard and a few components to light up some LEDs, receive AM radio signals, and provide mild electric shocks to my kid brother. Heck, I could even *send* radio signals and control a little stepper motor I scrounged from the garbage. Action at a freakin' distance! I was in preteen geek heaven.

But then… Software security gobbled up my life. In school, I had started focusing on electronics, but then diverted from my true tech love to analyzing software for security flaws. At the time, I made the move for purely economic reasons. The Internet was growing and its software was (and remains) quite flawed. The job market needed software security folks, so I repurposed my career in that direction. But I always missed my first true love—wireless and hacking the electronic world at a fundamental level.

But here's the beautiful thing. When reading this book, I could feel my interest in wireless and electronics rekindled. As wireless technologies have permeated so many aspects of our lives, we now live in the world Tesla envisioned and helped to conjure.

In *Hacking Exposed Wireless,* Johnny Cache, Joshua Wright, and Vincent Liu have written a guidebook explaining it all and telling us how to tackle this vast playground. They provide awesome coverage of wireless protocols, access points, client software, supporting infrastructure, and everything in between, and step-by-step directions for manipulating this technology. As I read through the chocolaty goodness of chapter after chapter, I not only learned how all these wireless protocols and systems actually work, but I also discovered practical techniques for improving their security.

As I thought about it, it occurred to me that Cache, Wright, and Liu are really latter-day Nikola Teslas, wielding powerful magic in their labs and sharing their deep secrets for all to come and play. This is powerfully cool stuff. I urge you to read this book and build an inexpensive lab based on what you learn so that you can explore.

But wait … it gets even better. Not only is this stuff fun; it's also inherently practical and useful! In fact, it is absolutely vital information for information security professionals to know, as wireless technologies pervade our enterprises, homes, government agencies, and even the military. In other words, you *need* to know this stuff for your job today. This book brings together the wireless world with detailed descriptions of the underlying technologies, protocols, and systems that make it all work, with real-world recommendations for finding and fixing flaws that every security professional must know. That Faustian bargain I made over a decade ago, trading my soul for software security, has come back in my favor. Wireless technologies tie together software, hardware, networking protocols, computing infrastructures, and more. While fun is fun, the bottom line is that there are serious business reasons for learning the deep secrets of wireless. Armed with the knowledge in this book, you'll be able to do your job better and make your workplace (and home) more secure.

I must confess—it is rather unlikely that reading this book will enable you to shoot lightning bolts out of your eyeballs. But it will provide you with a great understanding of the wireless world, which you can directly apply to improving the security of your home and business networks. What's not to like?

—Ed Skoudis
Co-Founder, InGuardians
SANS Instructor

ACKNOWLEDGMENTS

First, I would like to thank all of my friends who have stood by me over the years. Whatever technical achievements I have accomplished in the past, they are largely a result of having so many talented friends. Including them all would fill an appendix, so only an abbreviated list follows.

Jody for writing her first heap exploit better than me. Richard Johnson for talking us both out of a jam. Serialbox, trajek, and #area66 for kicking it old school. Skape and HD for poring over dozens of memory dumps with me. My brother for failing as a lookout. Optyx, spoonm, and samy (each of you is my hero). H1kari for trying to school me on FPGAs (still don't get it h1k). Chris Eagle for skewling me in general. Nick DePetrillo for getting my bags. Dragorn for well, everything. Dwayne Dobson for hosting an awesome BBS. Kiersten, Phil, Don, Craig, Sean, R15, Josh, Jeremiah, Robert, and Pandy for all of the good times. Don, Brian, Ted, and Irfan for always looking out for me. Josh Wright, Vinnie, Brad, and the McGraw Hill editors (especially LeeAnn!) for making me sound so much smarter than I am.

Finally, I would like to thank my friend Josh for helping me connect to that one network that one time. You can quit bringing it up now.

Seriously. I put it in the book.

—Jon

My friends and colleagues at InGuardians provide constant support and invaluable inspiration, which I treasure. Thanks to my friends at McVay Physical Therapy for fixing my back following many years hunched over a keyboard. Thanks to Mike Ossmann for his continued support and critique of the Bluetooth chapters, in which many improvements were made. Thanks to Nick DePetrillo and Mike Kershaw for years of support and camaraderie. Thanks also to my co-authors, editors, and supporting staff at McGraw Hill for the opportunity to work together. Finally, special thanks to my wife and children for their love and considerate understanding while I devoted many hours to this project; without their love and support, I would be lost.

—Josh

To Jon and Josh for being fantastic co-authors—you guys are really the best. Thanks to the entire team at McGraw Hill for your patience and support. The entire team at Stach & Liu for both amazing and humbling me on a daily basis with your curiosity, hard work, and good nature.

—Vinnie

INTRODUCTION

Since the first edition of *Hacking Exposed Wireless,* the technologies and the threats facing these communications have grown in number and sophistication. Combined with the rapidly increasing number of deployments the risk of implementing wireless technologies has been compounded. Nevertheless, the risk is often surpassed by the benefits and convenience of wireless technologies, which have been a large factor in the spread of these devices within homes, offices, and enterprises spanning the globe.

The story of wireless security can no longer be told with a narrow focus on 802.11 technology. The popularity of wireless technologies has created an intense interest in other popular wireless protocols such as ZigBee and DECT—interest that has manifested itself into research into attacks and vulnerabilities within the protocols and the implementation of those protocols in devices. With this growth in wireless technologies, these networks have become increasingly attractive to attackers looking to steal data or compromise functionality. While traditional security measures can be implemented in an effort to help mitigate some of these threats, a wireless attack surface presents a unique and difficult challenge that must first be understood before it can be secured in its own unique fashion.

This book serves as your humble guide through the world of wireless security. For this edition, we have completely rewritten core sections on how to defend and attack 802.11 networks and clients. We also cover rapidly growing technologies such as ZigBee and DECT, which are widely deployed in today's wireless environments.

As with any significant undertaking, this second edition of *Hacking Exposed Wireless* was a result of the efforts of several principals over an extended period of time. When we first returned to this book, we took great care in reviewing all the feedback and comments to figure out where we needed to do better for our readers. We also revisited all the technologies included in the previous volume and researched the interesting technologies that have emerged since the previous edition.

We have a new co-author this time around, Joshua Wright. Josh is one of the most well-respected minds in wireless security, and we are confident that you will immediately notice his contributions in the additional breadth and depth of knowledge found on these pages.