

"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 TM

Wireless Security Secrets & Solutions

Johnny Cache, Joshua Wright, and Vincent Liu

**Mc
Graw
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

Copyright © 2010 by The McGraw-Hill Companies. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

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.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

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

Trademarks: McGraw-Hill, the McGraw-Hill Publishing logo, Hacking Exposed™ and related trade dress are trademarks or registered trademarks of The McGraw-Hill Companies and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. The McGraw-Hill Companies is not associated with any product or vendor mentioned in this book.

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

TERMS OF USE

This is a copyrighted work and The McGraw-Hill Companies, Inc. (“McGrawHill”) and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill’s prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED “AS IS.” MCGRAW-HILL AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.



Know what to look for. **Understand what you find.**

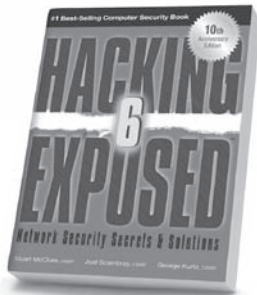
Now that you've discovered *Hacking Exposed: Wireless*, find out why businesses depend on Stach & Liu for practical advice and effective, real-world security services.

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.

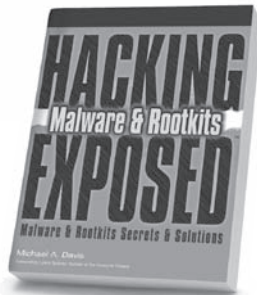
We don't sell hardware or software. Just our insight and expertise, direct and to the point. With a no-nonsense approach to education and knowledge transfer.

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

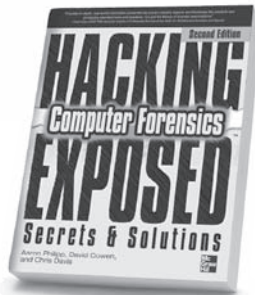
Stop Hackers in Their Tracks



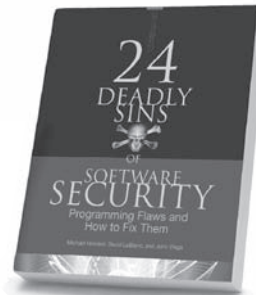
Hacking Exposed,
6th Edition



Hacking Exposed
Malware & Rootkits



Hacking Exposed Computer
Forensics, 2nd Edition



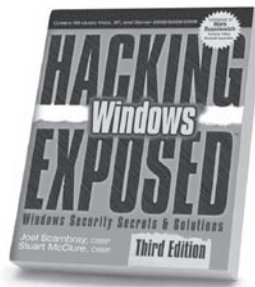
24 Deadly Sins of
Software Security



Hacking Exposed Wireless,
2nd Edition



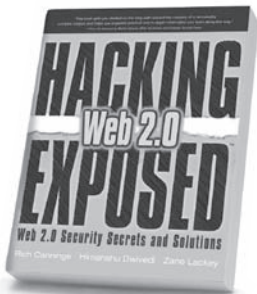
Hacking Exposed:
Web Applications, 3rd Edition



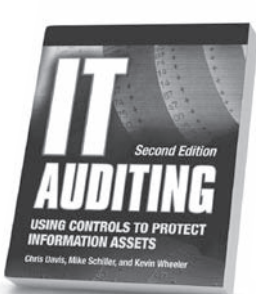
Hacking Exposed Windows,
3rd Edition



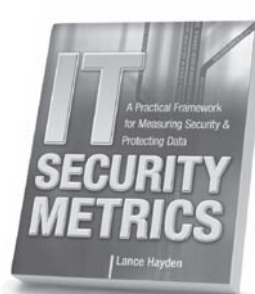
Hacking Exposed Linux,
3rd Edition



Hacking Exposed Web 2.0



IT Auditing,
2nd Edition



IT Security Metrics



Gray Hat Hacking,
2nd Edition

Available in print and ebook formats

Learn more.  Do more.
MHPROFESSIONAL.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 Antoniewicz 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

Part I Hacking 802.11 Wireless Technology

- ▼ 1 Introduction to 802.11 Hacking 7
- ▼ 2 Scanning and Enumerating 802.11 Networks 41
- ▼ 3 Attacking 802.11 Wireless Networks 79
- ▼ 4 Attacking WPA-Protected 802.11 Networks 115

Part II Hacking 802.11 Clients

- ▼ 5 Attack 802.11 Wireless Clients 155
- ▼ 6 Taking It All The Way: Bridging the Airgap from OS X 203
- ▼ 7 Taking It All the Way: Bridging the Airgap from Windows .. 239

Part III Hacking Additional Wireless Technologies

- ▼ 8 Bluetooth Scanning and Reconnaissance 273
- ▼ 9 Bluetooth Eavesdropping 315
- ▼ 10 Attacking and Exploiting Bluetooth 345
- ▼ 11 Hack ZigBee 399
- ▼ 12 Hack DECT 439
- ▼ A Scoping and Information Gathering 459

- ▼ Index 471

This page intentionally left blank

CONTENTS

Foreword	xvii
Acknowledgments	xix
Introduction	xxi

Part I Hacking 802.11 Wireless Technology

Case Study: Wireless Hacking for Hire	2
Her First Engagement	2
A Parking Lot Approach	2
The Robot Invasion	3
Final Wrap-Up	4
▼ 1 Introduction to 802.11 Hacking	7
802.11 in a Nutshell	8
The Basics	8
Addressing in 802.11 Packets	9
802.11 Security Primer	9
Discovery Basics	13
Hardware and Drivers	21
A Note on the Linux Kernel	21
Chipsets and Linux Drivers	22
Modern Chipsets and Drivers	24
Cards	26
Antennas	33
Cellular Data Cards	37
GPS	38
Summary	40
▼ 2 Scanning and Enumerating 802.11 Networks	41
Choosing an Operating System	42
Windows	42

OS X	42
Linux	43
Windows Discovery Tools	43
Vistumbler	44
inSSIDer	48
Windows Sniffing/Injection Tools	50
NDIS 6.0 Monitor Mode Support (NetMon)	50
AirPcap	54
CommView for WiFi	56
OS X Discovery Tools	61
KisMAC	61
Kismet on OS X	67
Linux Discovery Tools	67
Kismet	67
Mobile Discovery Tools	73
Online Mapping Services (WIGLE and Skyhook)	75
Summary	77
▼ 3 Attacking 802.11 Wireless Networks	79
Basic Types of Attacks	80
Security Through Obscurity	80
Defeating WEP	88
WEP Key Recovery Attacks	88
Bringing It All Together: Cracking a Hidden Mac-Filtering, WEP-Encrypted Network	104
Keystream Recovery Attacks Against WEP	107
Attacking the Availability of Wireless Networks	111
Summary	113
▼ 4 Attacking WPA-Protected 802.11 Networks	115
Breaking Authentication: WPA-PSK	116
Breaking Authentication: WPA Enterprise	129
Obtaining the EAP Handshake	129
LEAP	131
PEAP and EAP-TTLS	133
EAP-TLS	136
EAP-FAST	137
EAP-MD5	139
Breaking Encryption: TKIP	141
Attacking Components	146
Summary	151

Part II Hacking 802.11 Clients

Case Study: Riding the Insecure Airwaves	154
▼ 5 Attack 802.11 Wireless Clients	155
Attacking the Application Layer	157
Attacking Clients Using an Evil DNS Server	161
Ettercap Support for Content Modification	165
Dynamically Generating Rogue APs and Evil Servers with Karmetasplit	167
Direct Client Injection Techniques	172
Injecting Data Packets with AirPWN	172
Generic Client-side Injection with airtun-ng	175
Munging Software Updates with IPPON	177
Device Driver Vulnerabilities	182
Fingerprinting Device Drivers	186
Web Hacking and Wi-Fi	187
Hacking DNS via XSRF Attacks Against Routers	197
Summary	201
▼ 6 Taking It All The Way: Bridging the Airgap from OS X	203
The Game Plan	204
Preparing the Exploit	204
Prepping the Callback	209
Performing Initial Reconnaissance	210
Preparing Kismet, Aircrack-ng	211
Prepping the Package	213
Exploiting WordPress to Deliver the Java Exploit	214
Making the Most of User-level Code Execution	217
Gathering 802.11 Intel (User-level Access)	219
Popping Root by Brute-forcing the Keychain	220
Returning Victorious to the Machine	226
Managing OS X's Firewall	229
Summary	238
▼ 7 Taking It All the Way: Bridging the Airgap from Windows	239
The Attack Scenario	240
Preparing for the Attack	241
Exploiting Hotspot Environments	243
Controlling the Client	247
Local Wireless Reconnaissance	248
Remote Wireless Reconnaissance	255
Windows Monitor Mode	256
Microsoft NetMon	257
Target Wireless Network Attack	263
Summary	267

Part III Hacking Additional Wireless Technologies

- Case Study: Snow Day 270
- ▼ 8 Bluetooth Scanning and Reconnaissance 273
 - Bluetooth Technical Overview 274
 - Device Discovery 275
 - Protocol Overview 275
 - Bluetooth Profiles 278
 - Encryption and Authentication 278
 - Preparing for an Attack 279
 - Selecting a Bluetooth Attack Device 279
 - Reconnaissance 282
 - Active Device Discovery 282
 - Passive Device Discovery 290
 - Hybrid Discovery 293
 - Passive Traffic Analysis 296
 - Service Enumeration 309
 - Summary 313
- ▼ 9 Bluetooth Eavesdropping 315
 - Commercial Bluetooth Sniffing 316
 - Open-Source Bluetooth Sniffing 326
 - Summary 343
- ▼ 10 Attacking and Exploiting Bluetooth 345
 - PIN Attacks 346
 - Practical PIN Cracking 352
 - Identity Manipulation 360
 - Bluetooth Service and Device Class 360
 - Bluetooth Device Name 364
 - Abusing Bluetooth Profiles 374
 - Testing Connection Access 375
 - Unauthorized AT Access 377
 - Unauthorized PAN Access 381
 - Headset Profile Attacks 385
 - File Transfer Attacks 391
 - Future Outlook 396
 - Summary 398
- ▼ 11 Hack ZigBee 399
 - ZigBee Introduction 400
 - ZigBee’s Place as a Wireless Standard 400
 - ZigBee Deployments 401
 - ZigBee History and Evolution 402

ZigBee Layers	402
ZigBee Profiles	406
ZigBee Security	407
Rules in the Design of ZigBee Security	407
ZigBee Encryption	408
ZigBee Authenticity	409
ZigBee Authentication	409
ZigBee Attacks	410
Introduction to KillerBee	411
Network Discovery	416
Eavesdropping Attacks	418
Replay Attacks	424
Encryption Attacks	427
Attack Walkthrough	430
Network Discovery and Location	430
Analyzing the ZigBee Hardware	432
RAM Data Analysis	436
Summary	438
▼ 12 Hack DECT	439
DECT Introduction	440
DECT Profiles	441
DECT PHY Layer	441
DECT MAC Layer	443
Base Station Selection	444
DECT Security	444
Authentication and Pairing	445
Encryption Services	446
DECT Attacks	447
DECT Hardware	448
DECT Eavesdropping	449
DECT Audio Recording	455
Summary	458
▼ A Scoping and Information Gathering	459
Pre-assessment	460
Scoping	460
Things to Bring to a Wireless Assessment	462
Conducting Scoping Interviews	464
Gathering Information via Satellite Imagery	465
Putting It All Together	469
▼ Index	471

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.

- [*The Dhammapada: Buddhist philosophy pdf, azw \(kindle\), epub, doc, mobi*](#)
- [read Tomb of Horrors \(Dungeons & Dragons 4th Ed: Super Adventure\)](#)
- [download Growing Marijuana Indoors: A Foolproof Guide for free](#)
- [download online Addiction-Free Naturally: Liberating Yourself from Sugar, Caffeine, Food Addictions, Tobacco, Alcohol, and Prescription Drugs here](#)

- <http://twilightblogs.com/library/The-Dhammapada--Buddhist-philosophy.pdf>
- <http://twilightblogs.com/library/The-Pumpkin-Muffin-Murder--Fresh-Baked-Mysteries--Book-5-.pdf>
- <http://sidenoter.com/?ebooks/Growing-Marijuana-Indoors--A-Foolproof-Guide.pdf>
- <http://www.rap-wallpapers.com/?library/Short-term-Spoken-Chinese--Threshold--Volume-1--2nd-Edition-.pdf>