

Book Review: Hacking Exposed: Wireless 2nd Ed

Review by Jon Janego

What does the average security professional know about wireless technology, and wireless security in particular? Sure, it's easy to pwn WEP... but unfortunately, this is the extent of most people's knowledge. Many security testing firms even view wireless security as an "afterthought" or a separate practice entirely.

With the second edition of Hacking Exposed: Wireless, Johnny Cache, Josh Wright, and Vinnie Liu aim to teach us all that there's a lot more to wireless security than WEP cracking. For those who follow the wireless world, the names of these three should be immediately familiar. Josh and Johnny, in particular, have long been known as thought leaders in the wireless security space and have written or contributed to many of the tools and research used in the field. And with this fully revised and expanded edition of the book, these three great minds have come together, and the end product is an excellent book that covers some of the most cutting-edge technology while remaining very readable and down-to-earth. It's a book that deserves space on any hacker's bookshelf.

The book is arranged into three major sections. About two-thirds of the book is dedicated to 802.11 technology with sections dedicated to attacking both infrastructure and clients. The remaining third of the book is dedicated to three emerging wireless technologies, Bluetooth, ZigBee, and DECT.

del.icio.us

The 802.11 section begins with an introduction that is an excellent read, even for those familiar with the technology. The authors cover the basics of the protocol at a high level, as well as the basic techniques for analyzing 802.11 networks. They also make some recommendations on building out a wireless auditing toolkit, including specific recommendations on hardware, including OS platform and driver concerns. This is a very useful section, and helps any interested person get started right away with this expert advice.

After covering the fundamentals of scanning and building a toolkit, the book jumps straight into active attack techniques against WEP networks. They take a nice approach of working through several different scenarios, arranging them in order from easiest to hardest. Each example builds off the previous, and also includes helpful advice on how to protect against the attack that was demonstrated. Unfortunately in the case of many of these, there is only one answer: use better encryption!

Not content to just destroy the faith of any remaining WEP users, the authors then move onto taking apart WPA-TKIP encryption as well. They first demonstrate several attacks against pre-shared-key networks, while providing some good advice on how to protect these types of deployments. WPA-TKIP-PSK isn't quite as broken as WEP, but it should certainly be avoided - and the authors demonstrate this clearly.

The majority of the WPA attacks in the book, however, are built around breaking into the more complicated WPA Enterprise networks. It covers the various options available for implementing WPA Enterprise and the pluses and minuses from both a security and administration side. This is a complicated subject that is hard to find consistent advice on in a single place - until now. The authors do an excellent job explaining this technology both to attackers and administrators.

The authors then put on their cryptologist hats and cover some of the more academic-oriented attacks against WPA, walking through a nice demonstration of the Beck-Tews TKIP attack. From the perspective of an attacker or security analyst, this may not be entirely practical - but it's still a nice addition for those who want to truly geek out over the subject.

After covering attacks against infrastructure and the various wireless protocol weaknesses, the authors then spend a great deal of time on client-side vulnerabilities. They first discuss some of the more traditional client-side attacks available once access to the wireless network has already been established. These types of attacks are well-documented in many other books, so the authors don't dwell on it too extensively. Instead, they demonstrate how the behavior of the wireless cards and drivers on many operating systems can lead to compromise of clients, either by man-in-the-middle attacks or unintentional data leakage. Finally they bring it all together with two long-form walkthroughs, one demonstrating weaknesses in an OSX wireless client and another in a Windows box.

After devoting the first two-thirds of the book to 802.11, the authors move onto some of the less widely understood wireless protocols. They devote significant real estate to bluetooth, providing a well-needed technical background to a

subject that many of us are familiar with only on the consumer level. After the solid technical background, the book moves into reconnaissance techniques, and the various methods available for eavesdropping, attacking, and exploiting bluetooth. There is a lot of good information in this section, and some interesting proof-of-concept attacks, but nothing seemed quite as "slam dunk" as the 802.11 vulnerabilities demonstrated earlier in the book. However, the authors share some excellent information on the security weaknesses found within bluetooth, and this can very well be viewed as a foundational work on the subject. I wouldn't be surprised to see more bluetooth exploits and attacks developed in the next few years, and this book will be an excellent reference point.

Upon publication of this edition of the book, many in the security community were very excited to hear that it would include information about two emerging wireless technologies, ZigBee and DECT. I'm happy to say that they will not be disappointed. The authors provide detailed background on both technologies and cover the security challenges associated with both. The ZigBee chapter demonstrates many security issues by use of the KillerBee tool suite - which incidentally was written by Josh Wright, one of the authors of the book. So we're getting research straight from the source, and it's great stuff. The authors also discuss how to build a toolkit to use with these two wireless technologies, which is great practical advice to anyone wishing to use it in the real world.

Hacking Exposed: Wireless, Second Edition is a phenomenal book that should be considered mandatory reading for anyone interested in wireless technologies. And I would say that any security assessor or penetration tester who isn't interested in wireless should read this book - and learn why they should be paying attention to it. The authors do an excellent job providing concrete examples and clear explanations of the technologies and techniques used, and maintain a comfortable, easily readable writing style throughout. This is a seminal work on the subject of wireless security, and should become the standard for future books on the subject.

Jon Janego is a security consultant. He lives in Chicago.