Wi-Foo: The Secrets of Wireless Hacking

Andrew Vladimirov, Konstantin V. Gravrilenko,
and Andrei A. Mikhailovsky

Pearson Education, 2004, \$34.99, ISBN: 0-321-20217-1

Anyone who is interested and involved in wireless networking will be nicely surprised by a book that explains and supports WLAN (wireless local area network) security implementers, security managers, and (last but not least) hackers. The book is not primarily aimed at hackers,

but rather instructs security-responsible professionals on how to study their wireless networks through hackers' eyes, to find flaws and build appropriate countermeasures.

Quite a few books are already available on WLAN security, and more are sure to appear now that IEEE has endorsed the ultimate security standard, 802.11i. Most of these books, however, stop at a dry overview of specifications related to WLAN security, WEP (wired equivalent privacy), 802.1x EAP (extensible authentication protocol), and WPA (Wi-Fi protected access). *Wi-Foo* does a better job. It explains the bits and pieces of technology internals, and links this information to reality. It teaches readers to understand what is important and why, and how to implement what and when, in which networking situation.

The authors guide readers through the steps that regular and advanced hackers have to go through to break into the WLAN. Only through this process, penetration testing, may the insightful security manager find out the vulnerabilities of the network, and implement the necessary remedies to eliminate these vulnerabilities.

The authors balance wireless networking security theory and practice (without delving into the mathematical basis of cryptography)—offering step-by-step walkthroughs of wireless-specific attacks; recommendations on building a wireless hacking/auditing toolkit; and information on network mapping and site surveying, implementing multilayered defenses, and wireless IDSs (intrusion detection systems).

The book is full of practical advice, including guides on how to use both open and proprietary means to perform wireless penetration testing and hacking. It would be a very good investment for anyone concerned with WLAN security, from security auditors, network administrators, systems administrators, and security consultants, to home users and hackers.—*Rita Puzmanova*

Network Distributed Computing: Fitscapes and Fallacies

Max K. Goff

Prentice Hall Professional Technical Reference, 2003,
\$39.99, ISBN: 0-131-00152-3

The first few chapters of this text were the best I have read in a computer book in a long time, classifying, clarifying, and unifying the various threads of distributed computing in the finest discussion I have ever encountered on the subject. My expectations, however, so buoyed by the first three chapters,

were not fully met by the remaining nine. That is not to say they were badly written or undeserving of attention. In fact, they covered current frameworks and protocols very nicely and spent some time describing future frameworks. By themselves, I would normally characterize them as “good.” Yet, somehow, I came to the end of this text, disappointed that it never rose again to the level of its opening.

I still heartily recommend this book. For those who need to understand the history, future, philosophies, and problems of networked programming, this is the book to read. If you lead designers or programmers of networked systems, you need to read this book, and then pass it on to them; they should quote Goff as *Lord of the Rings* fans quote Tolkien. The “Eight Fallacies of Distributed Computing,” attributed by Goff to Peter Deutsch and referred to in the title, should be taped to the monitor of every distributed program designer and recited aloud in computer science classes.

Instead of presenting a comparative survey of APIs (application programming interfaces) and protocols, *Network Distributed Computing* proceeds from a discussion of the problems to be solved, to the various philosophical postures that have been taken regarding those problems, and, finally, to the frameworks those philosophies have produced. It also discusses how the “laws” or “meta trends” that influence the entire computing industry have shaped, and will continue to shape, network designs and programs. It concentrates on presenting the questions that computer scientists must ask, not on providing oversimplified answers for programmers to type in.

—*Bayard Kohlhepp* Q

Reprinted from *Computing Reviews*, © 2004 ACM, <http://www.reviews.com>