Editors: Martin R. Stytz, mstytz@att.net
Shari Lawrence Pfleeger, pfleeger@rand.org
Charles P. Pfleeger, chuck@pfleeger.com

BookReviews

Why We Won't Review Books by Hackers

Charles P. Pfleeger
Pfleeger Consulting Group

Shari Lawrence Pfleeger
RAND Corp.

Our goal with the book reviews is to inform *IEEE Security & Privacy* readers about books that are useful or provocative, interesting or funny, but always relevant to what we do as security professionals. We sometimes scratch our heads when publishers send us books that are extremely narrow or overly broad—designing very specific kinds of software modules for specialized applications or explaining why users should pay attention to security issues, for example. Consequently, we often browse the shelves in technical bookstores, trawling for books that will excite readers while extending their understanding of topics or issues. Recently, we came across Kevin Mitnick and William Simon's new book, *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders & Deceivers* (John Wiley & Sons, 2005).

At first glance, we thought a review might provoke discussion about hackers and their exploits, ethics, and careers; in the end, however, we decided that it would be inappropriate to review this book for two reasons. Mitnick and Simon describe a handful of hacking exploits as case studies, explaining how they could have been prevented, but the prevention advice is pretty mundane: "tell your employees not to be fooled by social engineering." More important, we decided that a review of this book (or others of its ilk) would tacitly endorse a convicted computer criminal who now wants to pass himself off as a consultant. Eugene Spafford makes a compelling case that computer break-ins—even when no obvious damage results—are unethical because the activity itself is disruptive and immoral.[1] Thus, rewarding hackers by touting their books in effect promotes what we consider unethical behavior.

So what are good candidate books for review? Books on cryptography and network, enterprise, and applications security can inform and enlighten. But our readership is already quite well-informed. For example, the crypto community already knows about most of the new cryptography books being published, and the non-crypto community isn't likely to be very interested in a heavily detailed crypto book. Instead, we prefer to review books that offer a little something to everyone.

Consequently, we will often review books that are slightly afield from what our readers normally read. For example, we asked Whit Diffie to review *Chatter: Dispatches from the Secret World of Eavesdropping* (Random House, 2005) because electronic surveillance is something security people tend to be interested in, but it isn't an obscure subspecialty. And the perspective of a key contributor to cybersecurity, such as Diffie, is always welcome. Similarly, we chose Sara Baase's *A Gift of Fire* (Prentice Hall, 2002) because it addresses almost every aspect of ethics, including privacy and security. Books describing the social impact or technical limitations of a security aspect would help to inform any security practitioner's worldview. Thus, we might choose a book on data mining uses or social network analysis because such techniques often enable or invoke security analyses.

As always, we invite readers to suggest books, provide feedback on past reviews, or review books for this column. And if you disagree with our selection strategy, please let us know. ▢

Reference

1. E.H. Spafford, "Are Computer Hacker Break-ins Ethical?" *J. Systems and Software*, vol. 17, no. 1, 1992, pp. 41–47.

Charles P. Pfleeger *is an independent consultant, author, and speaker specializing in computer and information system security. Contact him at chuck@pfleeger.com.*

Shari Lawrence Pfleeger *is a senior information scientist at the RAND Corp. Contact her at pfleeger@rand.org.*