;login:

THE MAGAZINE OF USENIX & SAGE
November 2000 • volume 25 • number 7

THEME ISSUE: SECURITY

edited by Rik Farrow

inside:

THE BOOKWORM

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

the bookworm

BOOK REVIEWED IN THIS COLUMN

SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD

BRUCE SCHNEIER

New York: John Wiley, 2000. Pp. 412.
ISBN 0-471-25311-1.

by Peter H. Salus

Peter H. Salus is a member of the ACM, the Early English Text Society, and the Trollope Society, and is a life member of the American Oriental Society. He is Editorial Director at Matrix.Net. He owns neither a dog nor a cat.

<peter@matrix.net>

This is an “extra” issue, so I want to break with tradition and discuss one (!) book.

Bruce Schneier’s *Applied Cryptography* (1994; 2nd ed., 1996) is a truly splendid book. His new *Secrets and Lies: Digital Security in a Networked World* is really outstanding.

Schneier’s byword is “Security is a process, not a product.” Just as locking your apartment or your house (or your car) is a first step – not a solution – to the problems introduced by those few who want to prey on others’ possessions, passwords, etc., are but a first step.

Schneier admits that he saw mathematics as a solution in 1994, but that he was wrong: cryptography (applied mathematics) doesn’t exist in a vacuum; like everything else, we function within a highly complex environment. *Secrets and Lies* is an attempt at both describing the complexities of the digital environment and elucidating the methods available to render it more secure.

There are three parts to *Secrets and Lies*: The Landscape (with chapters on “Digital Threats,” “Attacks,” “Adversaries,” and “Security Needs,” pp. 11–81); Technologies (“Cryptography,” “Cryptography in Context,” “Computer Security,” “Identification and Authentication,” “Networked-Computer Security,” “Network Security,” “Network Defenses,” “Software Reliability,” “Secure Hardware,” “Certificates and Credentials,” “Security Tricks,” and “The Human Factor, pp. 83–269); and Strategies (“Vulnerabilities and the Vulnerability Landscape,” “Threat Modeling and Risk Assessment,” “Security Policies and Countermeasures,” “Attack Trees,” “Product Testing and Verification,” “The Future of Products,” “Security Processes,” and “Conclusion,” pp. 271–395).

I happen to think security is important. It was while I was executive director of USENIX that we held the first security workshop (August 1988 in Portland, OR, chaired by Matt Bishop). Over the years I’ve reviewed a large number of books on security – ranging from Denning, Diffie, and Landau, to Bellovin and Cheswick; to Rubin, Geer, and Ranum and (last month) the new edition of *Building Internet Firewalls*. *Secrets and Lies* is up there with the best of them.

In fact, I think that Schneier has put the entire range of digital threats into appropriate context. I think that this is the book that every business executive should read. And it’s written in a manner that every executive can understand. There’s no code in it. No cryptographic algorithms.

There are lots of good examples and true stories.

In our increasingly digital world, the dangers need to be comprehended. Just as children need to learn how to cross the street, businesses need to know just how dangerous the networked world can be.