

# ;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

by Peter H. Salus

```
!" #"  
$ % & ' (   
) * + #"  
-# ) * . ' ; /  
0 -# ) * . #"  
#& $ % & '   
($ # - * # * & '  
-# ) # " . # #/  
# -  
# , 1 *"  
* # ' . + *  
-
```



ware, Ó Certificates and Credentials, Ó Security Tricks, Ó and Ó The Human Factor, pp. 83Ð269); and Strategies (Ó Vulnerabilities and the Vulnerability Landscape, Ó Threat Modeling and Risk Assessment, Ó Security Policies and Countermeasures, Ó Attack Trees, Ó Product Testing and Verification, Ó The Future of Products, Ó Security Processes, Ó and Ó Conclusion, Ó pp. 271Ð395).

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 Óve reviewed Ð a large number of books on security Ð 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 Ós written in a manner that every executive can understand. There Ós 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.

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

Bruce Schneier Ós 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 Ós byword is ÓSecurity is a process, not a product.Ó Just as locking your apartment or your house (or your car) is a first step Ð not a solution Ð to the problems introduced by those few who want to prey on others Ó possessions Ð 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 Ót 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 Ó Digital Threats, Ó Attacks, Ó Adversaries and Ó Security Needs, Ó pp. 11Ð81); Technologies (Ó Cryptography, Ó Cryptography in Context, Ó Computer Security, Ó Identification and Authentication, Ó Networked-Computer Security, Ó Network Security, Ó Network Defenses, Ó Software Reliability, Ó Secure Hard-