the bookworm

BOOKS REVIEWED IN THIS COLUMN

SECURITY WARRIOR
CYRUS PEIKARI AND ANTON CHUVAKIN
Sebastopol, CA: O'Reilly, 2004. Pp. 531. ISBN 0-596-00545-8.

BIOMETRICS FOR NETWORK SECURITY
PAUL REID
Upper Saddle River, NJ: Prentice Hall, 2004. Pp. 252.ISBN 0-13-101549-4.

ESSENTIAL CHECK POINT FIREWALL-1 NG
DAMEON D. WELCH-ABERNATHY [AKA PHONEBOY]
Boston: Addison-Wesley, 2004. Pp. 612. ISBN 0-321-18061-5.

EXPLOITING SOFTWARE
GREG HOGLUND AND GARY MCGRAW
Boston: Addison-Wesley, 2004. Pp. 471. ISBN 0-201-78695-8.

CODE READING
DIOMIDIS SPINELLIS
Boston: Addison-Wesley, 2003. Pp. 495 + CD-ROM. ISBN 0-201-79940-5.

LINUX PROGRAMMING BY EXAMPLE
ARNOLD ROBBINS
Upper Saddle River, NJ: Prentice Hall, 2004. Pp. 492. ISBN 0-13-142964-7.

LINUX POCKET GUIDE
DANIEL J. BARRETT
Sebastopol, CA: O'Reilly, 2004. Pp. 191. ISBN 0-596-00628-4.

HARDWARE HACKING PROJECTS FOR GEEKS
SCOTT FULLHAM
Sebastopol, CA: O'Reilly, 2004. Pp. 331. ISBN 0-596-00314-5.

BEOWULF CLUSTER COMPUTING WITH LINUX, 2ND ED.
WILLIAM GROPP, EWING LUSK, AND THOMAS STERLING
Cambridge, MA: MIT Press, 2004. Pp. 617. ISBN 0-262-69292-9.

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 owns neither a dog nor a cat.

peter@netpedant.com

Rik Farrow wrote a review of *Security Warrior* in the February *;login:*. I was going to review it at length, but decided that just a few words will suffice. (I've written a longer review for *http://www.UnixReview.com*.) I just wanted to say that I liked Peikari and Chuvakin's book more than Rik seems to.

Peikari and Chuvakin have written a valuable book which will soon find its way onto the shelf of everyone involved in network and machine security. I think of it as a supplement to Cheswick, Bellovin, and Rubin on firewalls and Schneier on cryptography, and a number of other works.

There are parts of Peikari and Chuvakin's book that are quite frightening. But war is frightening and computer/information war is no exception to this.

Further on this topic . . .

There are over a thousand books on computer security listed at Amazon. About a dozen of them are really worthwhile. That short list has just grown to include Peikari and Chuvakin's volume. Also quite informative is Reid's *Biometrics for Network Security*.

Fingerprints, footprints, hand geometry, iris and retina scans, voice, face, handwriting – they're all used. Reid's book is a first-rate summary of methods as well as a guide for system and network engineers.

Biometrics ends up with a very useful glossary and an extensive bibliography.

Essential Check Point FireWall-1 NG is by "PhoneBoy," who knows more about installing and maintaining FireWall-1 than anyone else. My problem is that FireWall-1 is proprietary. But if you're going to use it, PhoneBoy has produced the ultimate installation and configuration guide.

Hoglund and McGraw have devoted themselves to informing the good guys about what the black hats already know about how to take advantage (exploit) cracks and weak spots in the software we use. I see their *Exploiting Software* as a follow-up to Viega and McGraw's *Building Secure Software* of a few years ago. It's a worthwhile addition to the security bookcase (one shelf will no longer do).

Looking at Code

About 20 years ago, Marc Donner pointed out to me the importance of reading code carefully. He later taught a course at NYU on code reading. Spinellis has turned out a fine book on *Code Reading*, accompanied by a CD full of source and examples. He makes the same point that Donner did: You will write better code if you make it a habit to read good code.

Two Stray Penguins

Linux Programming by Example is a very fine book. I happen to be an admirer of Robbins' *Effective AWK Programming* (which lives next to my desk) and his book on vi (which I recommend frequently). But *Linux Programming* is exemplary. Interestingly, Robbins begins with, "One of the best ways to learn about programming is to read well-written programs." Donner and Spinellis would agree.

Robbins supplies the reader with a vast number of programs and a lot of elucidation. This is a primer in Linux pro-

gramming, but also serves as a tract on UNIX programming. Most of the illustrations are from actual GNU and UNIX V7 code. With ever more companies converting to Linux, this will be an invaluable resource for those converting from another [which one?] system.

I keep *Essential System Administration* and *Essential CVS* nearby for emergencies. Another valuable addition to O'Reilly's pocket guides is *Linux*. Barrett includes all the commands and flags I looked for and is so up-to-date that Fedora is covered.

Tinkering

If you believe that taking apart alarm clocks and building tuners or receivers is the right way to gain a technical education, *Hardware Hacking Projects for Geeks* is for you! "How to Hack 802.11b Antennas" and "How to Build an Internet Toaster" may be my favorite chapters, but "How to Hack a Furby" is useful, too. All of us who used to read *Popular Electronics* or *Popular Mechanics* or who still have a copy of an AARL handbook (my hand's up) will really love this book.

Beowulf Redux

The second edition of Gropp, Lusk, and Sterling's *Beowulf Cluster Computing with Linux* is over double the size of Sterling's volume on Beowulf of five years ago. But if you're into building a Linux cluster, you need it.