

;login:

THE MAGAZINE OF USENIX & SAGE

April 2003 • volume 28 • number 2

inside:

BOOK REVIEWS

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

the bookworm

BOOKS REVIEWED IN THIS COLUMN

COMPUTER SECURITY:

ART AND SCIENCE

MATT BISHOP

Boston: Addison-Wesley, 2003. Pp. xli+1084.
ISBN 0-201-44099-7.

FIREWALLS AND INTERNET SECURITY

WILLIAM R. CHESWICK, STEVEN M. BELLOVIN,
AND AVIEL D. RUBIN

Boston: Addison-Wesley, 2003. Pp. 430.
ISBN 0-201-63466-X.

802.11 SECURITY

BRUCE POTTER AND BOB FLECK

Sebastopol, CA: O'Reilly, 2003. Pp. 176.
ISBN 0-596-00290-4.

SHARING EXPERTISE

MARK ACKERMAN ET AL., EDS.

Cambridge, MA: MIT Press. Pp. 438.
ISBN 0-262-01195-6.

BGP

ILJITSCH VAN BEIJNUM

Sebastopol, CA: O'Reilly, 2002. Pp. 272.
ISBN 0-596-00254-8.

DNS & BIND COOKBOOK

CRICKET LIU

Sebastopol, CA: O'Reilly, 2003. Pp. 222.
ISBN 0-596-00410-9.

C POCKET REFERENCE

PETER PRINZ AND ULLA KIRCH-PRINZ

Sebastopol, CA: O'Reilly, 2003. Pp. 134.
ISBN 0-596-00436-2.

PHP POCKET REFERENCE, 2D ED.

RASMUS LERDORF

Sebastopol, CA: O'Reilly, 2002. Pp. 132.
ISBN 0-596-00402-8.

ESSENTIAL SYSTEM ADMINISTRATION POCKET REFERENCE

ALEEN FRISCH

Sebastopol, CA: O'Reilly, 2003. Pp. 137.
ISBN 0-596-00449-4.

WORD POCKET GUIDE

WALTER GLENN

Sebastopol, CA: O'Reilly, 2003. Pp. 143.
ISBN 0-596-00445-1.

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

There are many books to talk about this month, as well as two I'm shoving into my "history" column. The holidays gave me lots of time both to read and to ignore football. In fact, not watching football contributed to my time for reading.

Security

I reported on the security symposium last December. Little did I know that two important volumes would overburden my postman so soon.

The larger of these is Matt Bishop's monster.

In some ways, *Computer Security* is a perfect book for me – that is, someone interested in security but not involved in the field professionally. Matt has produced 1,100 pages that will most likely be the "standard" for a number of years. If there are topics omitted from this book, I haven't located them. From "Access Controls" to "Policies," "Cryptography" and "Malice" to "Auditing" and well over a dozen other topics, Matt has been there and done that. He has called upon Elisabeth Sullivan to contribute a section on "Assurance," and he concludes with chapters on "Network Security" and "System Security." Even if Matt had not thanked me in his acknowledgments, I would think this is an important and masterful tome.

The 1994 book on firewalls by Bellovin and Cheswick is in Bishop's bibliography; several of Bishop's papers are in the

new edition of that book, now Cheswick, Bellovin, and Rubin. When I reviewed the first edition, I was full of praise. The book is now nearly 150% of what it was eight years ago. The new edition comprises 19 chapters in six sections. The fourth ("Firewalls and VPNs"), fifth ("Protecting an Organization"), and sixth ("Lessons Learned") are worth the price of admission. The introduction to cryptography in the first appendix is excellent.

Potter and Fleck's volume on 802.11 security failed to reassure me. I still fear that we've not reconciled the convenience of wireless with confidentiality. But it's a solid presentation of the topic.

Knowledge

The concept of "knowledge management" was extremely popular in the '90s. Typically, it referred to the ways in which organizations could manage their intellectual property. This meant that "knowledge" was some sort of bankable resource ready for transfer and reuse.

More recently, as demonstrated by *Sharing Expertise's* very title, knowledge management has taken on aspects of humanity – recognizing the human components of knowledge work and sharing, rather than merely storage and retrieval.

This anthology, a truly interesting one, exemplifies this approach.

Networking

If you work on or with the Internet, you work with DNS, BIND, and BGP. Liu's *DNS & BIND* lives next to my computer. His "cookbook" will live on my reference/how-to shelf. I found "How to prevent Windows computers from trying to update your zones" (pp. 106ff.) useful just yesterday.

Iljitsch van Beijnum's *BGP* is the best thing I've looked at on the subject since

book reviews

Stewart's booklet five years ago. Really useful.

A Handful of Useful Pocket References

O'Reilly began producing pocket references a few years ago. I find many of them very handy. Three recent and valuable additions are those on C, PHP, and system administration. I think they're a bargain at about \$15 each. I also found the *Word Pocket Guide* very useful (my spouse uses Word at work and I was clueless until Glenn's book came my way).

CRACKPROOF YOUR SOFTWARE: PROTECT YOUR SOFTWARE AGAINST CRACKERS

PAVOL CERVEN

San Francisco, CA: No Starch Press, 2002. Pp. 250. ISBN 1-886-41179-4.

*Reviewed by Jennifer Davis
sigje@sigje.org*

At first glance *Crackproof Your Software* appears to be an enlightening book on a subject that hasn't been sufficiently covered. Although security is a big topic, most books cover securing your software against attacks on the software itself and on users of the software, data, and other systems on the network that the software is running on. This book hopes to illustrate how to prevent users from cracking the protection of the licensing code on your software.

As I began to read, however, I was immediately disappointed by several assumptions made by the author:

- Commercial software is written only on the Windows platform.
- Visual Basic, Delphi, and assembly language are the only programming languages commercial software is written in.
- Readers do not know what decompilers or debuggers are, but they know how to use them.

Other disappointments included useless diagrams and snapshots, like the 1/4-page size image of a window saying "Please insert the Half Life CD"; descriptions of good and bad securing applications without detailed explanation why a developer should use one and not the other; repetitive comments ("combine protection"); and overemphasis on the cracker's point of view to the detriment of the application developer's perspective in securing applications from cracking.

This book would be more aptly titled "How Crackers Crack Software on the Windows Platform."

Sadly, this book doesn't introduce the idea that future processors might have better capacity for secure programming with such new technologies as the upcoming Transmeta Crusoe chip.

My greatest dissatisfaction with this book may be that I'm not the intended audience. Someone with a great deal of assembler experience and Windows programming might be able to look at the available assembler code snippets and better understand what Mr. Cerven was trying to communicate with this book.

I look forward to seeing alternate coverage of this topic, or a better edited version of this book, since crackproofing software remains an interesting but underexamined subject.

EXTENDING AND EMBEDDING PERL

TIM JENNESS AND SIMON COZENS

Greenwich, CT: Manning Publications, 2002. Pp. 361. ISBN 1-930-110082-0.

*Reviewed by Raymond M. Schneider
ray@securityfoo.net*

Ever found yourself in need of some added functionality in Perl? Ever found yourself in need of an embedded language in your application? *Extending and Embedding Perl* attempts to help the reader with just those situations.

Extending and Embedding Perl, like most technical books, starts off by gearing the reader up with the necessities for understanding the material covered.

The first three chapters are introductory, covering the very basics of the C programming language, the basics of XS (eXternal Subroutines), and more advanced C programming. The experienced C programmer may safely, in my humble opinion, "raid" the first three chapters for any bits that they are either unfamiliar with or in need of brief review.

Chapter 4, "Perl's Variable Types," covers things like how scalar variables map to C

structures under the covers. It provides a nice overview that will help the reader with all the typedefs that point to C structures. On top of that, Perl wizards will be happy to find more “magic” in this chapter as the “magic variables” SvPVMG are covered here.

Midway through the text, the authors introduce the reader to the Perl API. Chapter 5 contains an incredible amount of information, with plenty of example code followed by numbered sections that step through the code and provide explanations. The reader will also find “tip” and “note” sections throughout.

The next chapter builds on the basics of XS and even discusses linking to Fortran or C++.

Now that the reader has learned all about XS, the authors present alternatives. As is common with everything relating to Perl, “there is more than one way to do it.” The reader is introduced to h2xs, SWIG, and the Inline module in an effort to ease the use of XS.

At this point the book makes the transition to embedding, Chapter 8 talking specifically about embedding Perl in C applications, and Chapter 9 covering an example of embedding Perl into an application many of ;login:’s readers are probably familiar with – Mutt.

The last two chapters of the book cover Perl internals and Perl development as the authors encourage the reader to participate in the future of the Perl language.

There is more to *Extending and Embedding Perl* than what the reader gets in the bound book. There is a Web site for the book: <http://www.manning.com/jenness>. There, in an area called “Author Online,” readers may interact with the authors in a sort of question and answer situation. It’s a quite interesting idea. I signed up for it and posted a question. I have to admit that after having to wait a month and a half for a response I consider the online forum a bit of a flop, especially if the reader’s need for a response is in any way urgent. In a month and a half most people will have long since moved on, especially in our industry.

I can, however, recommend this book to anyone interested in extending or embedding Perl. It is a quick read that the professional programmer can devour and the novice can understand.

USENIX and SAGE Need You

People often ask how they can contribute. Here is a list of tasks for which we hope to find volunteers.

The SAGEwire and SAGEweb staff are seeking:

- Interview candidates
- Short article contributors (see <http://sagewire.sage.org>)
- White paper contributors for topics like these:

Back-ups	Emerging technology	Privacy
Career development	User education/training	Product round-ups
Certification	Ethics	SAGEwire
Consulting	Great new products	Scaling
Culture	Group tools	Scripting
Databases	Networking	Security implementation
Displays	New challenges	Standards
Email	Performance analysis	Storage
Education	Politics and the sysadmin	Tools, system
- Local user groups: If you have a local user group affiliated (or wishing to affiliate) with USENIX and/or SAGE, please email the particulars to kolstad@sage.org so they can be posted on the Web site.

;login: always needs conference summarizers for USENIX conferences. Contact Alain Hénon, ah@usenix.org, if you’d like to help.