ÆLEEN FRISCH

the bookworm

Æleen Frisch is a system administrator and writer living in Connecticut (www.aeleen.com).

aeleen@usenix.org

BOOKS REVIEWED IN THIS COLUMN

APPLE I REPLICA CREATION: BACK TO THE GARAGE

Tom Owad

Syngress, 2005, 1-931836-40-X, 359 pp. + CD.

THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE

Peter Szor

Symantec Press/Addison-Wesley, 2005, 0-321-30454-3, 741 pp.

C# PRECISELY

Peter Sestoft and Henrik I. Hansen

The MIT Press, 2004, 0-262-69317-8, 214 pp.

CLASSIC SHELL SCRIPTING

Arnold Robbins and Nelson H.F. Beebe

O'Reilly, 2005, 0-596-00595-4, 560 pp.

HIBERNATE: A J2EE DEVELOPER'S GUIDE

Will Iverson

Addison-Wesley, 2005, 0-321-26819-9, 371 pp.

JAKARTA STRUTS COOKBOOK

Bill Siggelkow

O'Reilly, 2005, 0-596-00771-X, 533 pp.

JOTD: THE WORLD'S GREATEST COMPUTER JOKE BOOK

Hershel Remer ("Rabbs")

Rabbs Publishing (rabbs.com), 2004, 0-615-12449-6, 104 pp.

LINUX DEVICE DRIVERS, 3RD ED.

Jonathan Corbet, Alessandro Rubini, and Greg Kroah-Hartman

O'Reilly, 2005, 0-596-00590-3, 633 pp.

LINUX NETWORK ADMINISTRATOR'S GUIDE, 3RD ED.

Tony Bautts, Terry Dawson, and Gregor N. Purdy

O'Reilly, 2005, 0-596-00548-2, 360 pp.

LINUX QUICK FIX NOTEBOOK

Peter Harrison

Prentice Hall PTR, 2005, 0-13-186150-6, 696 pp.

LINUX SERVER SECURITY, 2ND ED.

Michael D. Bauer

O'Reilly, 2005, 0-596-00670-5, 539 pp.

FEATURED TITLE: THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE

The Art of Computer Virus Research and Defense, by Peter Szor, is a meticulously researched treatment of viruses, worms, and other types of malicious self-propagating programs, both as entities in themselves and in the context of administering real-world computer systems. The book treats its subjects at an excellent level of detail.

The book's first half provides a very up-to-date description of the ways that viruses and worms function. It includes a thorough history of the general topic as well as a study of attacker strategies and their evolution over time. The second half of the book focuses on responses to them. It covers both infection prevention and post-attack disinfection, including postmortem analysis of the code (in terms of how it the code operates and the obfuscation techniques that it employs).

This book is very well written and is interesting to read. Like all good security works, it manages to get across how the bad guys think and operate in ways that are useful for the good guys but without providing any help to black hat wannabes. This book will be very useful for system administrators and other computer security professionals, as well as computer scientists interested in this area of research. It also contains information of interest to programmers concerned about writing secure code.

FOUR PLANETS IN THE PROGRAMMING UNIVERSE

This month brings us four programming titles, each focusing on a specific, specialized programming context.

Classic Shell Scripting, by Arnold Robbins and Nelson H.F. Beebe, is an excellent book in the classic tradition of O'Reilly & Associates. It is an accurate, comprehensive treatment of writing shell scripts using modern Bourne-style shells. The

authors explicitly model their work after the Kerninghan and Plauger classic *Software Tools* volumes, and one could obviously not ask for a better approach. The book also provides an excellent introduction/reference for regular expressions, sed, awk, and many other standard UNIX tools. Although the authors occasionally go a bit too far—they truly believe that the shell is the best solution for virtually any programming problem—this book is nevertheless the definitive work on shell scripting.

Bill Siggelkow's *Jakarta Struts Cookbook* provides useful information and a plethora of helpful examples for programmers creating Web applications with Java. After some preliminary information about installing and configuring Struts, the book contains a well chosen and organized collection of code excerpts. The examples are structured as problems (goals) and solutions, a technique which results in well-planned examples (rather than merely a somewhat random collection of them). The solutions themselves usually cover not only the specific task at hand but also several variations. All in all, this is one of the very best volumes in the O'Reilly *Cookbook* series.

C# Precisely, by Peter Sestoft and Henrik I. Hansen, is a reference for the new version 2.0 of C# (Microsoft's Java-like object-oriented programming language, designed for use with its .NET Framework). The book focuses on the programming language itself, choosing to ignore most of the .NET class libraries. Language features are discussed on lefthand pages, with related examples on the corresponding righthand pages. The book will be found to be both readable and useful for programmers who use C#.

Hibernate: A J2EE Developer's Guide, by Will Iverson, provides comprehensive coverage of Hibernate, a widely used package designed to automate the process of mapping relational database structures to ordinary Java objects (typically saving a lot of programming effort and development time over using JDBC). Unlike other works on Hibernate, this book is organized around building a real application from the ground up. It begins with discussions of creating schema and mappings, the essential infrastructure required by every application. Later chapters cover the resulting Java classes, queries within the Hibernate framework, transactions, application performance, and so on. I find this organizational structure to be both logical and natural if the ultimate goal is to create real-world Java applications.

A DIFFERENT APPROACH TO LINUX SYSTEM ADMINISTRATION

The *Linux Quick Fix Notebook*, by Peter Harrison, takes an unusual approach to Linux system administration. Its audience is system administrators who want to configure a Linux system for use as a Web server (although much of its discussion would also apply to a system designed to be a file server). It is designed to be useful to both Linux users moving to this particular administration task and Windows Web server administrators who are moving to Linux. The book uses the command line for every configuration task in order to sidestep the Linux distribution quagmire, a clever tactic in my opinion. The work is procedure-oriented, avoiding most conceptual discussions in favor of focusing on how to get specific tasks done. Nevertheless, the book provides sufficient and accurate information which will enable members of its target audience to successfully configure a Linux Web server.

NEW EDITIONS OF LINUX CLASSICS

New editions of several Linux references are now available. The third edition of *Linux Device Drivers*, by Jonathan Corbet, Alessandro Rubini, and Greg Kroah-Hartman, updates that work for the 2.6.10 kernel. The book remains the definitive treatment of this topic, and it provides an excellent means for an experienced programmer to write a device driver for the first time.

The third edition of the *Linux Network Administrator's Guide*, by Tony Bautts, Terry Dawson, and Gregor N. Purdy, is an extensive rewrite. The new version removes discussions of outdated technologies (e.g., IPX, uucp, Internet newsgroups) and adds brief overviews of Apache, Samba, LDAP, IMAP, and wireless networking. Existing discussions have also been updated to cover IPv6 and iptables (instead of earlier tools, in the latter case).

The second edition of *Linux Server Security*, by Michael D. Bauer, is a revision of *Building Secure Servers with Linux* and is probably the least extensive revision here. It adds coverage of LDAP and databases to the previous work.

WAY, WAY OFF THE BEATEN TRACK

I'll close this column with a brief look at two quite eccentric works. *JOTD: The World's Greatest Computer Joke Book*, by Hershel Remer (a.k.a. UnixRabbi, a.k.a. Rabbs), does not live up to the claim in its subtitle, but it did provide me with a fair amount of mild humor. I suspect that readers with a greater tolerance for gender and ethnic stereotype-based humor and Microsoft bashing will find it quite amusing.

I have a friend who recently came across an IBM mainframe emulator on the Internet and thus had an urgent need for books on JCL (of which there are, unbelievably, some actually still in print). If that seems cool rather than bizarre to you, then Tom Owad's *Apple I Replica Creation: Back to the Garage* may be of interest. The book takes you through the process of building an Apple I replica and then programming it. It comes with a copy of the McCAD EDS-SE400 integrated design software. Happy building.