;login:

THE MAGAZINE OF USENIX & SAGE

August 2001 • Volume 26 • Number 5

Special Focus Issue:Clustering

Guest Editor: Joseph L. Kaiser

inside:

THE BOOKWORM
by Peter H. Salus

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

the bookworm

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>

For about 16 months now dot-coms have been dropping all over the place. NASDAQ is down, though higher than it's been, and everyone is looking glum. Well, cheer up.

The market soared. Did we really think it would go straight up forever? Moreover, don't despair: look at those income projections again. By and large, it's the growth rate that has changed. This happens with mature markets. It happened with cars, with TV sets, with washing machines.

E-Commerce

We had a fitful, feverish period where e-commerce was concerned. But the vast majority of automobile manufacturers (Cord, Maxwell, Stanley, LaSalle, DeSoto, Nash, Kaiser, Hudson, Pierce-Arrow, etc., etc.) are no more, yet there are vastly more vehicles. Their failure did not bode the death of the industry. Similarly, I think there is a great future for e-commerce, just not for many of the start-ups.

All of this is a prelude to my comments on a valuable book. Neidorf and Neidorf have turned out a relatively small volume (under 300 pp.) which will reward the reader.

They supply a "tour" of merchandising and management and informed me on a large number of topics I'd not really considered before: inventory management, pricing and promotion, profitability, vendor relations, and even organizational structure. There's also a brief glossary, a bibliography [!], and references to several useful Web sites (including that of the American Bar Association).

A worthwhile and informative read.

Applied Mathematics

Welschenbach's book on "cryptography" isn't really that. In actuality it's a first-rate introduction to the mathematical bases of cryptography.

The meat of the book is divided into two parts: "Arithmetic and Number Theory in C" and "Arithmetic in C++ with the Class LINT." I read the early chapters ("Number Formats," "Fundamental Operations," "Modular Arithmetic," and "Modular Exponentiation") at one go, while waiting for a car dealership to get around to tough tasks like changing oil and rotating tires. It was a great way to spend several hours (though the guy sitting beside me kept asking what the equations and lines beginning "#define" meant).

It's not easy stuff. Applied math isn't really for the faint of heart. But exponentiation and its application to cryptography is important. Welschenbach's class "LINT" (for Large INTegers) contains the data structures and functions that he utilizes in his analysis.

Welschenbach then uses this in talking about RSA (chapter 16) and then moving on to Rijndael, "a successor to the data encryption standard."

David Kramer has done a splendid job in translating Welschenbach's German.

LEGO Mindstorms

LEGO Mindstorms is the toy of choice for those of us who read *Popular Mechanics* and *Popular Electronics*. It is also a useful tool in education. Erwin's volume is, quite honestly, the best I've seen.

Erwin was involved in developing ROBOLAB, so it's not at all surprising that his volume enables the reader to

BOOKS REVIEWED IN THIS COLUMN

E-MERCHANT
JOANNE NEIDORF & ROBIN NEIDORF
Boston: Addison-Wesley, 2001. Pp. 276 + CD-ROM. ISBN 0-201-72169-4.

CRYPTOGRAPHY IN C AND C++
MICHAEL WELSCHENBACH
Berkeley, CA: Apress, 2001. Pp. 432 + CD-ROM. ISBN 1-893115-95-X.

CREATIVE PROJECTS WITH LEGO MINDSTORMS
BENJAMIN ERWIN
Boston: Addison-Wesley, 2001. Pp. 303 + CD-ROM. ISBN 0-201-70895-7.

DNS AND BIND
PAUL ALBITZ & CRICKET LIU
4th ed. Sebastopol, CA: O'Reilly & Associates, 2001. Pp. 624.ISBN 0-596-00158-4.

construct several robots (e.g., Walking Dog) as well as kinetic sculptures and some quite sophisticated projects.

There's a brief foreword by Seymour Papert and a good list of references and further readings.

Revisiting BIND

Albitz and Liu has been the standard handbook on DNS and BIND for nearly a decade. It is not a book for the raw beginner. You need to know something about the Domain Name System prior to cracking it. But it's invaluable. And it keeps getting better. The 4th edition is bigger and yet more useful.

It would have been really useful to Microsoft back in January, when a number of Microsoft-related Web sites just vanished. These included microsoft.com, slate.com, expedia.com, hotmail.com, and msnbc.com.

Microsoft had a DNS problem, which was compounded by a DDoS attack. Apparently, all four of Microsoft's DNS servers share the same routers, which means that all of them are vulnerable to hardware glitches or a technician's error.

There are, of course, reliable DNS services available to nervous customers. Nominium, for example, claims that it has a variety of collections of DNS servers, each with at least two different hardware and OS platforms, and each connected to two different ISPs.

Microsoft's errors and foolishness are obvious. The problem that Microsoft experienced once again illustrated the fact that even if you are a technically competent organization, your business is at significant risk without a highly reliable DNS infrastructure.

Though the apparent lack of diversity in Microsoft's name servers is a major error, there is a more general problem which also affects networks using BIND.

Using FreeBSD and BIND on every name server may be just as bad as employing Windows 2000 and Microsoft DNS on each of them.

If you use identical servers and identical software, no matter how geographically dispersed, a software flaw will affect all your servers at the same time.

And here's the kicker: Men&Mice found that 38% of the dot-com domains surveyed had all their name servers on the same subnet. And 75% had one or more configuration errors (see *http://www.menandmice.com/dnsplace/healthsurvey.html*).

DNS, like most databases, suffers from information entropy. It takes a lot of energy to keep information correctly updated while it is being changed. Anyone who has been hostmaster for even a moderately sized ISP knows there is an amazing number of ways for people to err.

And it's important to realize that one can't assume that IP addresses that are numerically contiguous represent hosts that are topologically close on the network.

The most obvious solution – and one which would take care of many problems – is diversity. The notion behind diversity isn't that diversity is error-free but that the error, whatever it is, is unlikely to strike more than one hardware platform, OS, or application at a time.

So here you are. Try running some Intel boxes and some SPARC or MIPS boxes. Try using UltraDNS on half your DNS servers and BIND on the other half. Try running Solaris on one SPARC and Linux or NetBSD on another; try running Windows 2000 on one Intel box and Linux on another.

And don't be like Microsoft. We've got proverbs that tell us the right thing: don't put all your eggs in one basket; variety is the spice of life.

Finally, understand what you're doing. Albitz and Liu will help with that.