book reviews

ELIZABETH ZWICKY

zwicky@greatcircle.com

with Sam Stover and Rik Farrow

STATISTICS HACKS: TIPS & TOOLS FOR MEASURING THE WORLD AND BEATING THE ODDS

Bruce Frey

O'Reilly, 2006. 336 pages.
ISBN 0-596-10164-3.

I have to admit, I am a pro-statistics person. Yes, I know, that kind of redefines "geeky." I'm still whining about a bad experience years ago where somebody decided to move all the "average-sized" mailboxes first. She meant the mean. The mean mailbox size was something like 34 kilobytes. The standard deviation was something like 145 kilobytes. Not surprisingly, there were no "average-sized" mailboxes. And you know what? When I tell this story most people smile and nod politely and edge away. (The rest of them mutter supportive indignant things about non-normal distributions and appropriate uses of averages.)

Anyway, I happen to think that a basic understanding of statistics and probability is *really important*. It will keep you from making all sorts of stupid mistakes, ranging from the above mistake (she wanted the mode, which would have led her to the 100,000 empty mailboxes), to submitting conference papers where you draw sweeping conclusions based on 7 data points per category, to saying confidently, "Oh, that's a one-in-a-million chance" without noting that you're talking about one in a million file writes on a system that does 20 million a day.

Some day, somebody is going to write the perfect math book for system administrators. This is not that book, but it does have what you really need: the basics of statistics and probability required to do something intelligent with most of the problems you encounter. The information on testing is particularly hard to find elsewhere in any useful and palatable form. It will also teach you how to win games of chance, in case you wish to spend your spare time on bar bets or, more likely these days, poker.

To use this book, you're going to need to be reasonably comfortable with math. You don't need to actually be good at it or anything; it doesn't ask you to do anything more complicated than addition and multiplication. But it doesn't have the space to do a lot of hand-holding. On the flip side, if you are seriously interested in statistics, you're going to want more than this. But for an average system administrator, this book provides just the right amount of detail, enough for a clever person to do a good-enough approximation.

GOOGLE, THE MISSING MANUAL, 2ND EDITION

Sara Milstein, J. D. Biersdorfer, and Matthew MacDonald

O'Reilly, 2006. 446 pages.
ISBN 0-596-10019-1.

More true confessions: I spend an absurd amount of time at dinner tables where I'm the only person employed in the computer industry who does not work for Google. You might be surprised how unenlightening this is if you actually want to use Google. Still, I expected that I knew most of what there was to know. I didn't.

I mean, I knew how to use Google as a calculator (try searching for "6 tsp to sticks of butter") and what Adsense and Google Answers are, and I have a Google home page and a Gmail account and all that fun stuff. I can Froogle and search for images. (Anybody with a toddler and a computer must learn to use image search!) But I didn't know about using Google via SMS, or Google Analytics, or some of the tricks for getting phrase searches to work right.

So on the whole I found this book educational—more educational than I had expected. My Google-employee husband found out some things, too. I'm willing to bet pretty much anybody will get something useful about Google out of it.

It has some flaws; first, Google changes too fast for a mere book to keep up. Second, there are way too many platforms and interests out there, so any given user is going to be skipping lots of stuff. I use a Treo and a Macintosh. I'm sure the coverage on how to make your cell phone use Google well is really handy if you don't have a keyboard. And if you use a PC, it's nice to have all the PC-specific goodies covered too (although if you use something that's neither a PC or a Mac, those sections are going to be a big yawn, as there's little to no mention of UNIX platforms).

Even so, I liked it. It's hard to see how one technically minded person would get enough out of it to justify the purchase cost, but it would probably be worth it for a computer-literate family member with an interest who wasn't a serious geek, or as a shared resource for a group.

LINUX TROUBLESHOOTING FOR SYSTEM ADMINISTRATORS AND POWER USERS

James Kirkland, David Carmichael, Christopher L. Tinker, and Gregory L. Tinker

Prentice-Hall, 2006. 571 pages.
ISBN 0-13-185515-8.

If you are an experienced system administrator who wants Linux information, you will find useful troubleshooting information in this book. Unfortunately, it tries to cover all of system administration as well. Sometimes it's right (if you are going to cover all of system security in 60 pages, it is in fact important to tell people not to try to fix a compromised machine but instead to reinstall it), sometimes it's misguided (if you are going to cover all of backups in 20 pages, the towers of hanoi schedule is not one of the things you ought to be including), and sometimes it's just too compressed to make sense.

Mostly, it simply avoids providing explicit instruction about troubleshooting techniques. There are lists of useful tools and samaple problems with solutions, but these are more hints than procedures you could apply to your own problems. Unfortunately, when there are instructions about troubleshooting, they're not very good ones. For instance, they advise troubleshooting network problems from the lowest stack layer up. This is very logical, but it isn't what anybody ever does, for a variety of good and not-so-good reasons. (For instance, the hardware is rarely broken, and it's way more trouble to get out of your chair and look at it than it is to type commands without moving.) Recommending it suggests that the authors felt the need to provide a system, but they don't have experience actually teaching people to troubleshoot.

I love the idea of this book, and I'm pretty fond of some of the information. But for system administration advice, you'd be better served by any current system administration text, for troubleshooting I still don't know of a good reference, and all that leaves is Linux basics, which are nicely covered, but don't take up that much of the space, and are widely available elsewhere.

COMPUTER PRIVACY ANNOYANCES: HOW TO AVOID THE MOST ANNOYING INVASIONS OF YOUR PERSONAL AND ONLINE PRIVACY

Dan Tynan

O'Reilly, 2005. 177 pages.
ISBN 0-596007752.

On the good side, this is a level-headed discussion of the various ways of protecting your privacy on-line. It's written for a not-extremely-technical-but-not-yet-extremely-paranoid audience and should help those people become appropriately nervous. It walks a fine line between sounding alarms about everything and ignoring genuine risks, and it seems to me to hit about the right balance. That is, sometimes I think it's too cavalier and sometimes I think it's paranoid enough to turn off a reader who believes in the fundamental trustworthiness of business and government, and yes, such people do exist in this day and age, and they need to read this kind of book, too.

So mostly I liked it. Once again, however, it's mostly oriented toward Windows machines. Actually, the Macintosh gets mentioned a couple of times but UNIX (in any form or flavor) is never even whispered, as far as I can tell. This is not such a big deal, because most of the book deals with platform-independent issues such as workplace privacy, public information, and government issues. (I think my father the Windows-hater would find it plenty useful.)

I'd also like to see some more mention of encryption. It comes up occasionally, but not with an explanation of what terms such as "weak" and "strong" might mean to an average user, or big warning boxes saying "HEY! Don't lose your password! That would be bad!" And that whole public-key private-key thing? It's neither explained nor mentioned.

This is a good book for handing out to your PC-using friends and relatives who're somewhat worried and pretty technically savvy. Because it spends a considerable time on issues that aren't related to computers you personally own, it will have information of interest to serious technical people who're not already privacy activists, but you may have to skip largish parts if you run your own UNIX boxes at home—you probably understand the issues and can't apply the suggested solutions in a couple of sections.

WRITING SECURITY TOOLS AND EXPLOITS

James C. Foster

Syngress, 2005. 664 pp.
ISBN 1-59749-997-8.

Reviewed by Sam Stover

I'd like to start out by saying that this book is not designed for people new to security, nor to programming, for that matter. While the first chapter definitely has that "read this if you just want to talk the talk," after that it goes uphill fast.

The moment you turn the page from Chapter 1 to Chapter 2, it's go time. The tutorial on assembly (with the goal of making sense of shellcode) is not for the weak of heart. I'll admit I had to reread several of the sections in this chapter, taking me back to my college days. In some ways this book really does read like an academic text, but the goal is to teach, and it certainly does that. When a certain point would just "click," it made it all worthwhile.

Once you get through the shellcode chapter, you'll jump into a chapter for each of the three main types of exploits: stack overflows, heap overflows, and format string vulnerabilities. All three chapters follow the same basic format, with just the right number of examples, along with discussion on hurdles to overcome when trying to find and/or prevent these types of vulnerabilities.

Now that you've seen the three main classes of exploits, we move into the second part of the book, which shows you how to find vulnerabilities and code exploits for them. Chapters 6 and 7 focus on local and remote exploits, race conditions, and socket coding. Both chapters contain a fair number of case studies where actual exploits are used to apply the concepts you learned in the first five chapters.

The remaining five chapters focus on application-specific coding for Ethereal, Nessus/NASL, and Metasploit, with Metasploit getting a total of three chapters. I found these chapters to be useful, with the caveat that the information is extremely redundant if you have certain other Syngress books. For example, I recently reviewed *Penetration Tester's Open Source Toolkit*, which contains the first two "Extending Metasploit" chapters as well as the "Coding for Nessus" chapter. The names of the chapters were the same, as were all of the figures, tables, etc. I found the cut-and-paste mentality a bit disappointing in spite of the technical value of the chapters. Fortunately, at least for Metasploit, there is a third chapter that addresses topics such as Inline Egg and Meterpreter, so all is not lost. Although I haven't read it yet, there is another book, *Buffer Overflow Attacks*, by the same author and publisher, that appears to have a lot of overlap as well. Just glancing over the table of contents shows that the stack, heap, and format string chapters look very similar, as do the shellcode and assembly sections. They are not exact duplicates, but too close for my comfort.

All in all, I think this book is a valuable reference, and I would recommend it to anyone interested in learning about exploit development from top to bottom. The chapter recycling from other books is a big disappointment, but this is only relevant if you have the other books. And maybe now that you've read this review, your expectations will be managed, and you won't be as annoyed as I was.

I don't want to let the duplicate chapters overshadow the value of this book as a whole though. It's a decent exploit book with plenty of examples. If you don't have the other books, this is probably just as good a place to start as any.

PGP & GPG: EMAIL FOR THE PRACTICAL PARANOID

Michael Lucas

No Starch Press, 2006,
216 pages.
ISBN 1-59327-071-2.

Reviewed by Rik Farrow

Lucas's book is aimed squarely at the people who know they should be using PGP or GnuPG but just haven't gotten there yet. His easy-going writing style gets across key ideas—for example, the differences between private-key and public-key cryptography. But the real strength of the book lies in the chapters devoted to using either the command line GnuGP tools or the GUI-based PGP. Lucas takes you step by step through creating your own key pair, sharing your public key, and maintaining your own keychain. You should buy this book for your boss or less technical buddies, or for the people who should have started using GPG by now.