book reviews

ELIZABETH ZWICKY, WITH BRANDON CHING AND SAM STOVER

THE MYTHS OF SECURITY: WHAT THE COMPUTER SECURITY INDUSTRY DOESN'T WANT YOU TO KNOW

John Viega

O'Reilly, 2009. 232 pp.
ISBN 978-0-596-52302-2

I like the book, but hate the subtitle. Most of the security industry desperately wants you to know the truth. I don't think the author really believes the subtitle either—surely the security industry, even in its most evil fear-spreading moments, does not actually want everybody to believe that the antivirus companies spread viruses? That is one of the myths he talks about.

Quibbling aside, this is a nice common-sense discussion of security, in the form of a lot of short essays. They are casual in tone and mostly non-technical. It's written by an insider, and the audience varies a bit; some essays are solidly aimed at non-technical people, some at technical people, and the occasional one is really insider-to-insider (those are the only people who need to be told to suck it up and live with the name "antivirus" for all sorts of malware prevention). There are lots of people who could enjoy this (I did), but its best audience is probably developers, who ought to know something about security, and the young and security-obsessed, who are prone to myths. I suspect the scandal-mongering subtitle is aimed at sucking in the latter group.

FATAL SYSTEM ERROR: THE HUNT FOR THE NEW CRIME LORDS WHO ARE BRINGING DOWN THE INTERNET

Joseph Menn

Public Affairs, 2010. 265 pp.
ISBN 978-1-58648-748-5

This is a believable, gripping non-fiction story about computer crime and the Russian mafia. You'd think that would be somewhat redundant; how could you write a boring story about computer crime and the Russian mafia? Sadly, I recently heard three speakers talk about computer crime and the Russian mafia, and one of them managed to make it considerably less gripping than, say, billing procedures. So boring is possible, and unbelievable is easy, which makes this book all the more surprising.

It lays out the story clearly, so you can see how it makes human sense. Some bits are obvious; my life is full of people who could easily have gotten in the middle of multiple crime families by a combination of technical focus and inability to recognize when people are really not trustworthy. Shadowy secretive gangs protected by the police sound a lot harder to believe in when brought up out of context, but actually make plenty of sense when set in their proper background. These days, when people ask me if I really believe that there are international crime rings involved in most computer crime, I tell them that it's like the drug trade. Sure, people whip up viruses in their own homes; they also grow marijuana in their own homes. But sooner or later, if they keep it up, they're going to run into serious criminals, and then they're going to become very small players in loosely coupled but large international crime rings.

This book reads like a novel, only with endnotes, and, like good spy fiction, is simultaneously enjoyable to read and somewhat depressing.

THE NUMBERS GAME: THE COMMONSENSE GUIDE TO UNDERSTANDING NUMBERS IN THE NEWS, IN POLITICS, AND IN LIFE

Michael Blastland and Andrew Dilnot

Gotham Books, 2009. 202 pp.
ISBN 978-1-592-40485-8

This is another book of nice, digestible essays loosely held together. It has some perceptive explanations I haven't seen elsewhere, including a good discussion of why numbers might, in fact, mean nothing at all. It's aimed primarily at helping you interpret the news, but is also a good start on thinking about numbers you may have dug up yourself. The section on how performance measurement changes things is especially important reading; it may be relevant to your management structure, and it will certainly be critical to you if you want to display metrics from your trouble-ticket or bug-tracking system.

I particularly resonated with the chapter in which you ask yourself, "Is this really a big number?" having recently spent a good bit of time contemplating the question, "Is 500,000 computers a big botnet?" (Yes, but not fascinatingly large.)

STATISTICS EXPLAINED: AN INTRODUCTORY GUIDE FOR LIFE SCIENTISTS

Steve McKillup

Cambridge University Press, 2006. 262 pages.
ISBN 978-0-521-54316-3

I have to admit that even system administration is generally not considered a life science, and almost everything else involving computers is even farther away. On the other hand, I haven't yet found a good book on statistics for the computer industry. You'd think business books on statistics would be the way to go, but those I can only find for students, they weigh 10 pounds and are printed in full color with the highlighting already done for you, and they make me too cranky to read, let alone review, them. (Also, they cost the better part of $200 each, which makes it very hard to suggest that anybody buy them.)

Apparently, biology students are less free-spending, at least on math books, because this is a reasonably sized black-and-white paperback. It assumes that you are intelligent and motivated and not terrified by mathematics, but probably not all that mathematical, and it goes through a *lot* of statistics and experimental design. It speeds right through some of the basics (probability gets a page-and-a-half sidebar) and doesn't really slow down until it gets to things like ANOVAs. This makes it a good follow-up to really beginning statistics books. There's also a helpful multipage decision chart on picking experimental designs and tests which, in itself, is worth the price of entry. If you really don't know any statistics, start somewhere else, but if you've mastered dice rolls and how to tell averages apart, this is a good next place to go. You may not be measuring fish, but it will still be useful to you.

RESTFUL WEB SERVICES COOKBOOK: SOLUTIONS FOR IMPROVING SCALABILITY AND SIMPLICITY

Subbu Allamaraju

Yahoo! Press, 2010. 293 pp.
ISBN 978-0596801687

REVIEWED BY BRANDON CHING

The *RESTful Web Services Cookbook* by Subbu Allamaraju is an excellent companion text for Web developers in search of REST solutions. Like most texts in the O'Reilly Cookbook series, the book is not an all-encompassing manual. Rather, Allamaraju outlines a number of commonly faced problems in building RESTful applications and provides concise solutions to those problems.

The book is divided into 14 chapters and a number of appendices. Allamaraju covers a wide range of topics, from resource identification and Atom to security and caching issues. While no single book can encompass all possible problems a REST developer may face, Allamaraju does an excellent job in answering what are likely the most common and far-reaching questions. Coming in at under 300 pages, this book nevertheless contains an impressive breadth of coverage.

I found the coverage of security (Chapter 12) quite useful. While all Web developers know basic HTTP authentication, Allamaraju extensively covers digest and OAuth (both two- and three-legged) authentication methods as well. The sections on conditional requests, cache validation, and concurrency control were also quite valuable. Allamaraju includes the handling of JSON, XML, Atom, and SOAP in a number of examples throughout the book.

Allamaraju's writing is clear and easy to read. All examples in the book use HTTP and XML to demonstrate implementation. While the REST architecture is not the most complicated to understand, it is very often poorly implemented. The author does a very good job of delivering solutions in an understandable way so that when you have to implement a RESTful application, it will be done right.

This book is written for experienced Web developers in any programming language and belongs on the shelf of anyone working in REST applications. However, since the book focuses on higher-level REST methodology, I would recommend a language-specific REST resource in addition to this book (unless you are a serious guru in your project language).

SECURING THE BORDERLESS NETWORK: SECURITY FOR THE WEB 2.0 WORLD

Tom Gillis

Cisco Press, 2010. 125 pp.
ISBN 978-1-57805-886-8

REVIEWED BY SAM STOVER

I should have known. The author of this book is the VP and General Manager for the Security Technology Business Unit at Cisco and was part of the founding team at IronPort Systems (Senior VP of Marketing). Had I read the bio, I wouldn't have been surprised, but I didn't, so I was. I'll be honest: I think this book is more about how awesome Cisco is, not really about securing the "borderless network." That's not to say that it doesn't have merit; Cisco *can* be awesome, and there is a bit of history throughout the book that's interesting. But $45 is a little pricy for what you get.

The book is actually small—really small, only 125 pages. The 15 chapters are very short, most no more than ten pages, so that's great for anyone with a short attention span. Chapter 1 runs through the evolution of the firewall and warns that this type of technology will never handle Web 2.0 traffic properly. Chapter 2, "Collaboration and Web 2.0 Technologies," was especially disturbing to me; it seemed to say that companies not dialed into the new way of the Web will lose their appeal to "Gen Y" employees and ultimately fail. The unfortunate point, as it seemed to me, was that this trend is inevitable, so you had better just give in. Personally, I prefer to believe that while it might be inevitable, it needs to be done right, and I didn't find the emphasis on doing it right that I was hoping for in a (alleged) security book. Well, at least in a book that has "Securing" in its title.

Chapters 3 and 4 go on to show how productive you can be if you just give in to cloud computing and online collaboration. Chapter 5 is basically an advertisement for Cisco's Telepresence and WebEx tools. Chapters 6 and 7 extol the virtues of the smartphone but, again, don't really dive into what can be done to actually secure anything.

Chapters 8 and 9 give an overview of malware and the people who use it. Lots of history and perspective, but a little lean on mitigation and how those technologies impact companies embracing Web 2.0 technologies. For a while there, I forgot that this book is about Web 2.0 and securing it. Chapter 10 claims to offer "Signs of Hope," but all I got out of it was that Cisco's global product footprint and their multicore technology are two great answers to the malware problem. Chapters 11 and 12 discuss AUPs and data loss events: AUPs are too restrictive and just get bypassed, and data loss is bad. If you don't already know this, then maybe this book is for you.

Chapter 13 claims that we need to re-engineer our IT departments to stop denying Web 2.0 technologies by "Saying 'No Thanks' to the 'Culture of No.'" Again, too much of "this is inevitable" (I get it already, seriously) and not much on how to do it right. Chapter 14 follows on its heels with the challenges of authentication and how Cisco is readying their "Identity Fabric." This was pretty interesting, but I'm not sure it came to a solid conclusion—it was more like a discussion on a hard problem, with some ideas Cisco is proposing to address it.

Finally, Chapter 15 looks like it will answer all of our questions. It's entitled "Security for the Borderless Network: Making Web 2.0 and 3.0 Safe for Business" and it contains, well, pretty much nothing we don't already know. Starting with instructing companies to make their policies more flexible and ending with promises of next-gen scanning tools from Cisco, there's not much here for the person looking to actually apply security to their Web 2.0 users and technology.

Maybe I'm just not the right audience for this book, and if that's the case, then most of the *;login:* readership probably isn't either. If you want to learn about next-gen Cisco multicore silver bullets, head to their Web page. If you want to hear that your policies and procedures aren't sufficient to account for Web 2.0 or (shudder) 3.0, ask, well, any audit or assessment firm. If you want someone to tell you that new technologies are coming and that you'd better be ready, well, I'll tell you that for free.