book reviews

ELIZABETH ZWICKY, WITH RIK FARROW AND SAM STOVER

A few introductory notes. First, this isn't just the security issue; it's also the issue before Christmas, and somehow, despite the fact that I'm in the middle of a heat wave as I type, it's Christmas that caught me up as a theme. So I've thrown some less technical books into the mix.

Second, this issue marks my adoption of eBooks as a reviewing medium. A lot of factors drove me in that direction. There's the arrival of the iPad, which may be an overgrown phone, but it's a form factor that works for me for reading books. There's the sheer waste of shipping paper around, when I don't always like every book enough to review it. And then there's the fact that the first book I'm reviewing weighs more than my laptop, and at that is printed on paper thin enough to make turning pages challenging. So far, I'm enjoying the eBook experience, aside from distribution issues, which are often different for review copies than for release copies. I choose to always review final copy, but eBooks allow me to review that before the paper copies print, which usually means the eBook isn't officially available either.

UNIX AND LINUX SYSTEM ADMINISTRATION HANDBOOK, FOURTH EDITION

Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, et al.

Prentice Hall, 2010. 1232 pp.
ISBN 978-0-13-148005-6

The fourth edition is also the twentieth-anniversary edition, which means that words like "classic" are pretty much inevitable. It also means that lots and lots of people already have opinions about previous editions. If you are such a person, you can stop reading now; this edition is unlikely to change your mind in any direction. Probably the only thing you need to know is that it covers old-style big-company UNIX (Solaris, HP-UX, AIX) and Linux, but not any BSD variants. I miss the BSD variants, particularly because Mac OS is a BSD variant; on the other hand, I really wouldn't want the book to be any longer than it already is.

If you haven't previously encountered the book, its strengths are in its technical coverage. It assumes that you know the absolute basics of how to use UNIX, and covers most of the bases you'll need to know to run a UNIX-based site, from scripting through mail sending and security. It's not evenly deep; it will teach you a great deal about mail, and hardly anything about cryptography. But it will teach you something about close enough to everything. There's a degree of old-fashioned UNIX attitude, which leavens the experience (and, to my taste, occasionally descends into annoying snark, but one person's well-founded negative opinion lightly expressed is the next person's annoying snark, and, in any case, it's lightly sprinkled).

Its weaknesses are, as always, the flip side of its strengths. It often fails to structure information, particularly non-technical information, so that you get a list of rules of thumb for something (security, or laying out file systems, or doing backups) but no overarching principles. The result is that you can use it to figure out how to do something, but, in most cases, you're not going to get much useful help on what you ought to be doing in the first place. (For that, see *The Practice of System and Network Administration*, ISBN 978-0321492661.)

Also, because it covers everything, it has trouble hitting a "just-right" level of abstraction. Some things are covered quickly enough to be indigestible for a beginner. A combination of factors, ranging from sheer lack of page space to a heritage dating back to days when all text all the time was the standard, means that it is critically short on illustrations.

As a resource, it's much more efficient than trying to paw through vendor documentation, and it covers more territory. Most system administrators will want a copy to look things up in, or learn about a new area.

COOKING FOR GEEKS

Jeff Potter

O'Reilly, 2010. 398 pp.
ISBN 978-0-596-80588-3

RATIO: THE SIMPLE CODES BEHIND THE CRAFT OF EVERYDAY COOKING

Michael Ruhlman

Simon and Schuster, 2009. 272 pp.
ISBN 978-1-4165-7172-8

In case you're Christmas shopping for a cook or somebody who might want to be a cook, here are two immensely geeky cookbooks. Or at least, one of them makes an explicit claim to be both intended for geeks and a cookbook; the other one wasn't even filed with the cookbooks at my bookstore and doesn't specify an audience, but don't let that fool you.

I started out feeling a bit hostile about *Cooking for Geeks*. Yeah, I call myself a geek, but it's not like it defines my life. I think I cook like a human being, and I am suspicious of things that treat "geek" like it's necessarily a meaningful group identifier. Plus, does the world really need more cookbooks? More introductory cookbooks, even?

It's not that my suspicions were totally unfounded, but I was won over pretty rapidly. Mostly, the book covers territory that other cookbooks don't, and regardless of how you feel about the title, it's a fun read for people at almost any level of interest in food. There are interviews with technical/foodie types you've heard of and you haven't, and it takes approaches you're not going to find anywhere else, such as discussions of protein denaturation and the biomechanics of taste.

Will it teach you to cook? Eh, maybe. Hard to tell. Most people I know either cook or they don't, and I'm not certain that a book is going to move people from one camp to another, but this book is going to intrigue the cooks. In addition, it certainly could have saved many semi-cooks I know from a number of unpleasant surprises.

Will it teach you new tricks? Oh, surely. Unless you already work for a cutting-edge restaurant, there are techniques here you haven't tried, probably haven't heard of, and almost certainly didn't think you could achieve at home. Some of them require more daring than others, some of them are actually actively recommended against (useful in itself), but you're certainly not going to walk away thinking, "I already knew all of that," and you probably will be thinking, "That sounds like fun, I might try that."

However, any geeky cook is also going to want *Ratio*. It's almost as technical as *Cooking for Geeks* and, in a way, is much more tightly focused. There's something a little contradictory about calling a book that ranges from bread to soup to custard "focused," but it's a much more integrated, less multi-threaded experience. It takes a wide range of recipes that can be thought of as ratios, provides ratios, explains them (both books talk about baking and gluten and air and the difference between popovers and crepes, which is a lot less than you'd think when you look at them, or eat them), and talks about how to modify them. It's a bolt of clarity, which will open whole new vistas of experimentation.

THE LEGO TECHNIC IDEA BOOK: SIMPLE MACHINES

Yoshihito Isogawa

No Starch Press, 2010. 157 pp.
ISBN 976-1-59327-277-7

This is an eccentric but seductive book. It consists almost entirely of pictures of Lego constructions, with the occasional number. Most of the Lego constructions are very simple machines: a few gears, or some pulleys, or some tracks. They build up to combinations that do things, examples of lots of things you could do with a single car chassis, or many, many different doors.

People with any reasonable amount of interest in Lego are rapidly sucked in; they start going "Oh! That's clever!" or "Hmm. What could I do with that?" The simplest mechanics are shown in pretty much every possible configuration, so if you don't have the precise parts shown in later constructions, you should be able to figure out how to replace them. Many of the pieces used are in non-classical Technic colors, which helps suggest improvisation. I was worried that you might need all sorts of Technic to have a good time with the book, but one good-sized Technic set produced enough parts to play with the book satisfyingly, if not to build every single thing.

It could actually use a few more words, or at least some words repeated; there are titles in the table of contents, but not on the pages. The titles help in figuring out what's being shown, and they provide

vocabulary for kids; mine was frustrated by seeing pictures of a group of things and not knowing what they were called. Still, she enjoyed it greatly. A child who cared more about understanding the author's intent would have a harder time.

CONFIGURATION MANAGEMENT BEST PRACTICES

Bob Aiello and Leslie Sachs

Addison Wesley, 2010. 217 pp.
ISBN 978-0-321-68586-5

"Configuration management" here means primarily software configuration management, not system configuration management, in case you're a hopeful system administrator. The wars it carefully stays out of are Ant vs. Maven, not cfengine vs. Puppet.

If you're interested in configuration management as a career, this will give you a good framework in which to think about how configuration management goes together and how it fits into companies. It also has a nice variety of anecdotes, and a sensible approach to psychology as a part of configuration management.

If you're not already passionate, it's not likely to convince you, unfortunately. It's unevenly edited, gripping in spots and totally flat in others. And I know I just complained about *UNIX and Linux System Administration* being short on illustrations, but somebody seems to have decided that *Configuration Management* needed illustrations for their own sake. The resulting picture of the globe did not actually deepen my understanding of distributed configuration management issues.

YOUR MONEY: THE MISSING MANUAL

J.D. Roth

O'Reilly Media, 2010. 324 pp.
ISBN 978-0-59-680940-9

REVIEWED BY RIK FARROW

As sometimes happens, this book appeared in the post, out of the blue. And while I felt comfortable about my own finances, I thought that I knew of some people who might profit by reading it. The book is better than I had expected, and I wound up learning a lot by reading it.

Roth started out, as he writes, living paycheck-to-paycheck and getting deeper in debt. He began researching to learn how to extricate himself from his predicament, then started a Web site that shares his findings: GetRichSlowly.org.

Understanding the math is simple, Roth writes, but controlling your emotions and habits is hard. Roth is always gentle, and very clear, as he lays out techniques for reducing debt, budgeting, saving, investing, and even retiring. I picked up his book wondering whether someone buried in credit card and student loan debt would appreciate getting it as a gift, and the answer is absolutely. For myself, I learned more about investing, and will reread his section on buying a car the next time that comes up.

INSIDE CYBER WARFARE

Jeffrey Carr

O'Reilly Media, 2009. 220 pp.
ISBN 978-0-596-80215-8

REVIEWED BY SAM STOVER

The author of this book acknowledges his role as the "Principal Investigator of the open source intelligence effort Project Grey Goose." I'm going to ignore the possible connotations of this fact, but anyone with a predisposition regarding Project Grey Goose is likely to apply it to this book, especially as the project is referred to often.

Cyber warfare is certainly a high-impact buzzword in today's world, and this book does a reasonable job of discussing the topic in a way that is relevant to techies and managers alike. Chapter 1 starts out by "Assessing the Problem," which is no easy task, since everyone seems to have their own idea of what qualifies as cyber warfare. One important point, that I happen to agree with, is that too many people want to separate cyber crime from cyber warfare, and this book posits that too many bad guys dabble in both.

Chapter 2, "Rise of the Non-State Hacker," discusses the 2008 Russian-Georgian conflict, along with Israeli-Arabic cyber attacks. Specific events are cited to show different methods used by attackers to disrupt, deface, redirect, or otherwise negatively impact their adversary. The chapter ends with the cold hard truth that in China and Russia, attacks against other countries are just not prosecuted by law enforcement (LE). In my experience, this rings true—if "local" citizens are not being attacked, good luck getting international LE support.

Chapter 3 focuses on how different countries deal with cyber attacks. A number of attacks are discussed, as well as any legal action brought to bear. The chapter rounds out with eight mini-scenarios that have occurred in eight different countries since the Russia-Georgia conflict. This

is followed by a return to the question, what exactly is considered a cyber attack? Chapter 4 also deals with legal issues, but is actually a compressed thesis by another author (Lt. Cdr. Matt Sklerov from the DoD). I think this chapter was my favorite, as it discussed when "states may lawfully respond to cyber-attacks in self-defense." "Hacking back" has been a hotly debated topic for, well, forever, and I really found the legal issues explained in this chapter to be interesting, although I'm not sure I completely agree with everything that's said here.

Chapter 5 uses several different incidents, including the Korean DDoS attacks, the 2009 Ingushetia conflict and the Russia-Georgia conflict, to show the value in intelligence gathering when trying to piece together the "big picture." Chapter 6 shows how social networking services play a relevant part in both attack collaboration and attack surface. Chapter 7 deals mainly with how the bad guys are able to work within the confines of the Internet. Bulletproof Hosting is dissected and explained in the context of the Russian-Georgian conflict.

Chapter 8 dives into "Organized Crime in Cyberspace," which is another hotly debated topic, and it's not really surprising that the Russian Business Network (RBN) is the example used for discussion. There is a lot of speculation on what the RBN was/is, where it came from, where it went, and who was involved.

Attribution of attacks and attackers is a huge part of cyber attack investigations, and Chapter 9 goes through a number of methods and sources of information. Open source data such as AS and BGP info, as well as WHOIS, and darknet monitoring are presented. For the techies in the group, this is a decent, albeit short, chapter with a little technical meat to it. Chapter 10, "Weaponizing Malware," also has some good tidbits such as SQL injections, iframe attacks, rootkits, and social engineering attacks. Chapters 11–13 deal with military doctrine, early warning models, and policy advice, respectively. Not to say that I found these chapters boring, but, well, I kinda did, maybe because the preceding two had some decent technical stuff.

The book has lots of quotes and references, which I found a little tedious, but is chock full of details and supporting material, which lots of other books tend to lack. I read this book in softcopy (O'Reilly's Safari), so I don't have a feel for how hefty the book was, but most chapters seemed very short. Lots of references to Project Grey Goose—it seems that a lot of the data/findings were contributed by that effort. There are definitely places where the author's opinion is stated as if it were fact, but I guess that's par for the course. Overall, this is a solid, but brief, look at cyber warfare, with a heavy emphasis on the Russian-Georgian conflict.