Book Reviews

ELIZABETH ZWICKY,
WITH RIK FARROW

R Cookbook

Paul Teetor

Finally, an R book that actually answers the questions I need to have answered in a way I understand. It answers a lot of other questions, too, ranging from ones where I think, "Ah! I've wanted to do that!" to ones where I think, "I hope I never want to do that."

The problem with R is that almost everything you want to do is very easy as long as you think about it correctly, for R. Which is at right angles to everything you are used to. (For instance, loops are evil. Never loop. You apply the function to an array—well, no, not an array, but unless you already know R you're going to think of it as an array—and it mystically does the right thing.)

Since books about R are written by people who can think in R, they often make sense only after you have managed to make this right angle turn. Somehow Paul Teetor has managed to maintain more perspective than most authors.

The cookbook format is sometimes constraining and artificial ("Problem: You want to install R on your computer"), but once you get past the beginning it generally works OK. Because of the aforementioned otherworldly nature of R, you may find that you have to read parts of it straight through. If you think a vector has a direction and a length (instead of being basically a one-dimensional array), you're not going to be able to leap right to solving your problem. That's not the book's fault; even real cookbooks end up assuming that you know how to boil water at some point.

If your needs for statistics have outgrown your favorite spreadsheet, but you are not a career statistician, you need R, and you probably need this book to go with it.

Everything Is Obvious Once You Know the Answer

Duncan J. Watts

(Full disclosure: Duncan Watts and I share an employer, currently. I've therefore been exposed to more posters for this book than most people, but I believe it has not otherwise influenced me. It does not appear to me to have made any of my colleagues less willing to tell me what they believe to be obvious, sadly.)

I like this book for a couple of reasons. First, I have a strong tendency to believe that everything is probably complex and unintuitive and one ought to measure things before believing in them. Second, I find reading it brings up the basic emotions of watching a high-wire trapeze act. Here is somebody writing an entire book which can be summed up as, "Sociology has so far told us very little about the world, often because the answers to the questions people are asking are in fact unknowable, but it's worth doing anyway." And it's an engaging and I think convincing book. I am in awe at even trying to do this, much less succeeding.

Another way of summing the book up, of more interest to people who hold no strong opinions about sociology, is, "Stop guessing what people are going to do and why, and start reacting to what they actually do." You think sociology is irrelevant? Marketing is applied sociology, and most of it is the sociological equivalent of avoiding black cats and the number 13. That might be funny, except it costs real money.

If you are interested in prediction of human behavior, or sociological ideas such as "everybody is only 6 steps apart" or "some people are influencers and sway the opinions of lots of other people," this is an interesting new take on things. As for me, I plan on keeping it around to whack people with when they tell me how obvious something I've just found out is. Or how something they have just made up is obviously true.

IT Security Interviews Exposed

Chris Butler, Russ Rogers, Mason Ferratt, Greg Miles, Ed Fuller, Chris Hurley, Rob Cameron, and Brian Kirouac
Wiley, 2007. 205 pp.
ISBN 978-0-471-77988-2

Periodically, I wander off to see what's in bookstores. This looked interesting because I've been interviewing candidates recently (for security, but not specifically IT security) and I wanted to see what advice they might be getting, what questions other people use, and whether there were resources that would help candidates avoid popular mistakes.

This book does steer people away from some common and unfortunate mistakes (e.g., it's a resume, not an autobiography—six pages is overkill, particularly if you've only held two jobs). And on most topics, it gives an overview sufficient to help an experienced person think about what areas they might want to brush up on, and what answers they might want to think out.

On the other hand, the years have not been kind to it; there is no mention of Web security at all, and I'm pretty sure I'm one of the few security interviewers on earth who doesn't ask about XSS. I know this because all my interviewees, if they don't know an answer, say hopefully "I think it's an XSS," regardless of the question. (Hint: if we are not discussing Web sites or I have just told you what I think the problem is, that is not the right answer.) A book that doesn't even get into the general vicinity of Web servers (XSS, XSRF) or database servers (SQL injection) is omitting some of the most important and interview-relevant topics in security.

Aside from that, it's inconsistent, with different format and tone for different chapters, the discussions are telegraphic enough to permanently confuse somebody who doesn't understand the territory already, and it rarely gets into questions that distinguish interviewing from exams. Somebody who could answer all the sample questions correctly would come across as somebody with a CISSP and nothing behind it. If they were lucky. Otherwise they might have picked up some of the book's more perplexing stumbles. No, it is not easy to ensure that no wireless client on your network is willing to connect to a rogue access point. No, it is not important to believe that HIPAA is regulation and Sarbanes-Oxley is legislation. (They are both legislation, implemented as regulation, but I had to look that up; nobody cares unless you carefully and definitively get it wrong.) And if I ask you about the main configuration components in a firewall, and you reply "configuration, policy, and objects," I am going to believe you know exactly one firewall configuration system.

Take Control of Media on Your iPad, 2nd Edition

Jeff Carlson
TidBITS Publishing, 2011. 158 pp.
ISBN 978-1-61542-131-2

I was curious about what this series was like, and this seemed like a good topic for a review: simple enough that I can evaluate it, without being so simple as to be mind-numbing. Also, there's something pleasantly ironic about reviewing a book about media on the iPad, as an eBook on an iPad. (It turns out that while it is pleasantly ironic, it makes it impossible to view the instructions and the interface at the same time. This worked out OK for me, but a real novice probably needs a paper copy, or at least to read the book on some other device.)

It was a good experience, all told. The eBook version is formatted to take advantage of the platform, which is rare and convenient, and there's appropriate coverage of the built-in capabilities without totally neglecting the important add-ons (such as GoodReader, the reader I was in fact using to read the book). It told me several things I didn't know and wanted to, and it looked quite useful for its intended audience of basically competent users who may need some help. It was willing to point out useful trivia (how to lock the orientation of your screen and adjust the brightness) without devoting a lot of space to things most people will know.

If you're a contented and knowledgeable iPad user already, it probably won't improve your life by $15 worth (although it did improve my iPad life a bit). On the other hand, it might well be worth it to my father (it certainly would have been before the day I taught him to use smart playlists in iTunes). Although it is a new edition, it is still applicable to first-generation iPads as well as the iPad 2.

The Book of PF, Second Edition

Peter Hansteen
No Starch Press, 2011. 188 pp.
ISBN 978-1-59327-274-6

Tony del Porto reviewed the first edition of this book back in the April 2008 issue of *;login:*, and I was interested in seeing what had changed since then. PF is the OpenBSD firewall and is also available in FreeBSD and NetBSD. PF is configured through a powerful and concise set of rules, and some of the syntax of the rules changed with the release of OpenBSD 4.7 (and FreeBSD 8). And while PF already included support for CARP used for failover, the new version also supports CARP for load balancing.

PF has had the ability to create dynamic rules, something just added to Linux, and you can do some very cool stuff

with this. On page 87, you learn how to add the IP address of someone attempting to brute-force SSH to a rule that will block that IP address based on the number of simultaneous connections and the rate of connections.

PF supports IPv6 without the need for a separate configuration file and command, unlike Linux. What is lacking from this book, and the online OpenBSD PF pages, are examples of firewalls using IPv6. In a way, this is not a problem, because simply enabling the routing of IPv6 (in a gateway firewall) is all that is needed to make your existing PF firewall work with IPv6. But there are some things specific to IPv6, such as ICMPv6 (required for determining the MTU, for example), for which examples would be nice.

But this is a clearly written book and well worth the price.

—*Rik Farrow*

The Silicon Jungle
Shumeet Baluja
Princeton University Press, 2011. 334 pp.
ISBN 978-0-691-14754-3

I was intrigued when a friend mentioned that a book written by a Google employee, about massive data processing, was an exciting novel. And I found myself unable to put the book down as it neared its end. The characters had taken on lives of their own, ones that appeared familiar to me. The big exception here is the antagonist, a greedy multimillionaire, who seemed a bit too simplistic. Then again, I know so few multimillionaires that perhaps Shumeet is being totally accurate here.

This is a story of an intern at a fictional Internet search company which sounds like Google merged with Amazon, Visa, and AT&T. The tech culture is very Google, with all the free caffeinated drinks and food you can ingest, and people working long hours on an eerily familiar campus in Silicon Valley. But this company has access to a much broader swath of data than any company in the world has today. That data, and the ability to process it, is key to the plot.

Stephen, the young intern, lands a highly competitive internship and is selected to work on the hottest internal project, one that can connect information from credit card purchases, email, phone calls, and Web searches to target advertising more precisely than ever before. The interns are an experiment in just how usable the interface to the new software will be, and the interns are soon invading the privacy of unsuspecting people. Stephen, a veteran of a failed startup, has a bit more maturity, but he too gets caught up in the power of the system when he creates a list very similar to one of the US government's terrorist watch lists.

Stephen's girlfriend, Molly, is instrumental in getting him involved with the search company and has her own ties to terrorism, via the unusual path of a doctoral dissertation funded by the DoD. Molly and one other female character add a bit of a balance to this otherwise all-male geek world.

Shumeet's novel is also a speculative tale of what can happen when an organization, whether it is the government or an advertising agency, has access to too much information and the means to process it. The story strongly reminded me of Admiral John Poindexter's failed attempt to create a similar information gathering project, coined Total Information Awareness, back in 2002. With proliferating automated license plate recognition and RFID toll payment devices, and the information available from cell phones (location, contacts, searches), airline reservations lists, and credit cards, TIA would do an even scarier job today. Shumeet is writing about this issue, even as he makes reading about it fun. Yes, there are 16 pages of references at the end, too.

—*Rik Farrow*