

Book Reviews

TREY DARLEY AND MARK LAMOURINE

Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents

Jean-François Blanchette

MIT Press, 2012, 280 pp.

ISBN: 978-0262017510

Reviewed by Trey Darley

Blanchette's thesis is that while cryptographers spend their days in the world of pure mathematics, they exist in messy, human socio-historical contexts, and, consequently, efforts to model that world in protocol form are fraught with latent, oftentimes unconsidered, assumptions. Blanchette provides sufficient background in both the history and practice of cryptography and of evidence law to draw both technical and legal audiences into his discussion. As IANAL, I found the background material on contracts, witnesses, the notarial system (as opposed to common law practices more familiar to me), and the privileged evidentiary status of authenticated acts both fascinating and helpful. On the cryptographic side, Blanchette does an admirable job capturing technical details whilst still writing in language that should be understandable to a general audience, albeit hopefully a well-caffinated one.

He narrates how, back in the '90s, various interest groups, feeling themselves encroached upon by the advance of technology, drove the legislative reform agenda on cryptographic signatures. Shockingly, it seems that the resultant regulations for the most part failed to address the vital point of signature verification. Blanchette shows how the concept of nonrepudiation flies in the face of traditional judicial discretion. Cryptographers assume, he argues, that judges will think about cryptographic primitives like cryptographers would and, as such, existing protocols make unhelpfully high crypto-literacy demands.

This is a wide-ranging book. I was taken aback by how many avenues for further research it opened. For example, I never considered the impact that format-transcoding (necessary to maintain future-proof digital archives) has on signature verification (and, hence, document authentication). If we're building a paperless world in which 500-year-old documents will be more transparent than 50-year-old ones, then clearly the modeling has gone badly off the rails. Anyway, just something to think about. If you are at all interested in crypto, you'll probably dig this book. Pay close attention to Blanchette's chapter summaries, which are remarkably trenchant.

Practical Lock Picking: A Physical Penetration Tester's Training Guide, Second Edition

Deviant Ollam

Syngress Media, 2012, 296 pp.

ISBN: 978-1597499897

Reviewed by Trey Darley

The idea that information security begins in meatspace is an accepted cliché, but in practice it's all too easy to get distracted by OSI layers 2-7. There's nothing quite like the experience of popping your first lock to awaken your senses to weak physical security all around you. If you haven't had the pleasure already, I would encourage you to let Deviant Ollam be your guide through the world of picking, raking, shimmying, and bumping. After you read this book, with its diagrams clear enough to be understood by a child and plenty of helpful hints on assembling a toolkit, you probably won't look at your front door the same way again.

Vintage Tomorrows

James H. Carrott and Brian David Johnson

Maker Media, 2013, 398 pp.

ISBN 978-1-449-33799-5

Reviewed by Mark Lamourine

Carrott and Johnson had a beer and a question. Three questions, actually: "Why Steampunk?" "Why now?" and "What does it mean for the Future?" The book is the story of their inquiries and reflections. Along the way they visit Australia, the UK, Seattle, Dallas, Comicon, and Burning Man (twice), among other places. They accidentally spawn a documentary film, which they end up documenting.

This isn't your average sociology paper. The text alternates between first person accounts by each of the authors as they travel to meet the people they interview, visit conventions, and even host a dinner gathering of Steampunk luminaries. The authors invite the reader to participate in the journey and the conversations.

Carrott is a historian who likes to immerse himself in his subject. As a teen, he was a Civil War reenactor, and for this book he first visits and then participates in Burning Man in Nevada. His tech background includes managing the development of the Xbox 360. Johnson is a professional futurist, projecting trends as much as 10 years out to help Intel guide their research. The historian and the futurist use each other as sounding boards for their ideas and questions.

If you're familiar with Steampunk at all you'll probably know at least a couple of the authors that they meet. You may or may not know of the artists, tailors, craftsmen, many of whom were doing what they do before the term was coined. As a long-time reader of Bruce Sterling and William Gibson, I found myself thinking both "Oh, cool" and "Well, of course" within a single sentence more than once.

Carrott and Johnson find that the Steampunk movement isn't a simple one-dimensional fad of nostalgia. The visual and literary trappings of the 19th century resonate with different groups of people and, remarkably, none of them are Luddites who want to live in the past. There are the hangers-on who think that to make something Steampunk you just "stick a gear on it," but a central tenet of the Steampunk movement is individual active participation in the process of shaping our surroundings, clothing, tools, and technology. Participants value the craftsmanship of unique items as a response to what they see as the modern sterile cookie-cutter design ethic. They are optimistic about the use of technology that contrasts sharply with the trend toward dystopian literature since World War II.

Did I mention a movie? The process of writing the book inspired documentary filmmaker Byrd McDonald to follow the authors on many of their visits. A trailer is up at <http://www.vintagetomorrow.com>. A release date hasn't been announced.

The authors are also adding more to the book over time in the form of a companion (DRM-free) ebook: *Steampunking Our Future: An Embedded Historian's Notebook*, available from O'Reilly (though it will take a bit of search-fu to find it apart from *Vintage Tomorrows*).

I got copies of *Vintage Tomorrows* in several ebook formats as well as hard copy. Each has advantages. The photographs in the paper book are rendered in half-tone black and white. The ebook images are full color images; however, I found that, with one exception, the images were cropped in odd ways rather than re-sizing on my ereader (a no-name 7-inch tablet running vendor and third-party reader apps). The exception was the PDF version, in which the images were scaled nicely; however, the PDF version was almost four times bigger than the EPUB or MOBI versions. Also, when you scale the text for easier reading, you're really zooming, and the text is cropped rather than wrapped.

Corsets and top hats making it back into most people's everyday lives is unlikely, but the Steampunk ethos is having an influence on mainstream thought and sensibilities. The optimism and joy of makers, hackers, and geeks are gradually making enthusiasm for learning and technology acceptable again. The nerd of the 1960s, '70s, and '80s is becoming intelligent, witty, and stylish. *Vintage Tomorrows* shines some light on the way that we are constructing both our future and our past.

Testable JavaScript

Mark Ethan Trostler

O'Reilly Media, 2013, 250 pp.

ISBN 978-1-449-32339-4

Reviewed by Mark Lamourine

There are any number of books that will tell you how important it is to write tests. In the ones I've read, little time is given to the elements of software that can make it hard to test. More than once I've found myself looking at a test routine that just smells bad without understanding why.

In *Testable JavaScript*, Trostler explains how to recognize the characteristics of hard-to-test code and how to avoid writing it. The early chapters cover the concepts of code complexity: cycloomatic complexity, fan-out, and coupling. Trostler proceeds to describe how event or message-driven systems can provide the ultimate in decoupling (with their own set of caveats).

This section makes up about the first half of the book and was the most valuable to me. The concepts of complexity are fairly subtle. Recognizing and then mitigating these elements in code will take some practice. I suspect I'll come back here a number of times over the next few months. This isn't something that was in the college curriculum when I was a student, but I'm guessing the concepts glossed in these three chapters could fill a full semester of undergraduate work.

There are references to a number of books, papers, and articles in those opening chapters. Many of the references are accompanied by permanent bit.ly URLs. While I can fish back through the text to find them later, a proper bibliography would be nice.

From here on the title of the book could be seen as a bit of a misnomer. The remainder of the book seems to go back to the more typical topics.

The unit testing and coverage sections continue the mix of theory and practice, though the practice begins to come to the fore. The chapter on unit testing opens by glossing the concepts of mocks, stubs, and spies (a new one on me). The next few sections introduce testing frameworks for client-side testing in Web browsers and Android devices and closes with more traditional server-side testing in Node.js.

The next chapter introduces the concept of code coverage, that is, the idea of exercising every path and branch in your code. The concept is generally applicable, but the tool and techniques presented are for JavaScript only. Trostler is cautious about the value of code coverage metrics, but shows how the use of automated instrumentation can improve the quality of the results.

The book closes with chapters on integration and performance testing, in-browser debugging, and test automation. The tools

available in most browsers are both impressive and pretty slick, taking advantage of the capabilities of the graphical interface.

This is a book about JavaScript programming. It could take some additional effort to puzzle through for someone who's not fluent. If you can manage, most of the techniques and patterns in the first half of the book are applicable to (and valuable for) other object-oriented and procedural languages. I would recommend this book if only for that. If you're also looking for some new tricks, you'll find something here.

EPUB 3 Best Practices

Matt Garrish and Markus Gylling

O'Reilly Media, 2013, 345 pp.

ISBN 978-1-449-32914-3

Reviewed by Mark Lamourine

I think the most important thing I learned from *EPUB 3 Best Practices* is that there's a lot more to building electronic documents than I would have imagined. The authors sum up an EPUB document this way: It's a Web server in a box.

EPUB 3 is the most recent open electronic document standard. It's actually defined by four specifications. These define the format for the content, structure, packaging, and "media overlays." This last one is new to EPUB and it describes how to sync audio and text for things such as subtitles. The specifications define the function and limitations of each of the features. *EPUB 3 Best Practices* describes how to use them.

Each of the chapters covers an aspect of the EPUB 3 format. While there is a progression, and you can read the book cover to cover, you can also dive into any one of the chapters without missing anything.

EPUB 3 documents are composed using other current standards. The content must be XHTML5 or SVG. Note that this refers to the document as a whole. HTML documents can refer to images in formats other than SVG.

The rest of the glue is XML or CSS. There are a set of standard fonts, and you can embed additional fonts in a document with the OTF or WOFF formats (there are translators for others). While the HTML5 audio and video codec discussions continue, the EPUB 3 specification requires reader software to support MP3 and AAC (MP4) audio. Video is another matter, and the authors stick to describing the implications of the ongoing ambiguities on EPUB 3 documents and reader software.

Interactivity is provided by a required JavaScript engine, which allows the inclusion of dynamic graphics and forms. There is a chapter on language support, another on accessibility, and a third on providing text-to-speech capabilities. Including external resources through standard HTML links is possible, and there are provisions for alternate media if a network is not available.

I like the fact that the authors address several non-technical issues with EPUB production. There is a fairly detailed discussion of the need and means to acquire the rights for proprietary fonts before embedding them. As noted above, the authors devote a portion of the chapter on fonts to their proper use. I think there are a number of instances in which a judiciously placed structure graphic might have helped illuminate how the parts fit together.

As with *Vintage Tomorrows*, I read this book in paper, EPUB, and PDF. In the case of books with code samples, I find the ebooks difficult on small and medium-sized tablet devices. Code often has been laid out carefully in a typeset book, and the otherwise laudable ability of an ebook reader to re-flow the text based on the font size and the device becomes a problem.

I don't expect ever to have the need to create an EPUB 3 document from scratch and by hand. If I do, or if I ever find myself needing to look inside one, I'll keep this book handy. This is a great book for the curious, and I suspect it could be required reading for people meaning to write an EPUB 3 editor, compiler, or reader.