Book Review

Hallam-Baker, P. (2008). *The dotCrime Manifesto: How to Stop Internet Crime*. Upper Saddle River, NJ: Addison-Wesley. 415 + xxix pages, ISBN: 0-321-50358-9, US$29.99.

Reviewed by Gary C. Kessler (*gary.kessler@champlain.edu*)

At the beginning of each fall semester, an e-mail routinely circulates around university campuses recounting those technologies that this year's incoming class grew up with and, therefore, for which they have no memory of a time before those technologies existed -- such as a ubiquitously available Internet, GPS satellite technology, CallerID, and karaoke. Most of today's freshmen (in fact, most of today's user community) mistake their familiarity with *using* a technology as actually *understanding* how that technology works; not only do most users not really understand the workings, they also don't know the history, background, and evolution of these technologies. Nevertheless, many of our incoming students consider themselves experts.

I took my first computer programming class as a college sophomore in 1973, early in the Information Age. Even as a 19 year old, I realized that if we were really in an Information Age, then information should have value, we should take steps to protect that information, and, perhaps, violating the integrity of information systems should have consequences. (Yes, even then I complained to my college registrar about social security numbers being used as student identification numbers.)

Phillip Hallam-Baker's *The dotCrime Manifesto* is a wake-up call for all of those who do not yet recognize the threat of crime in cyberspace and how our own actions and lack of understanding enables such an environment. The book describes the problem of criminal activity in cyberspace by providing a historical context with a particular emphasis on the evolution of the security mechanisms employed by Internet protocols and Web applications. This approach is sorely needed. There are many excellent texts describing how to build secure applications, systems, and networks -- often by building from the ground up. There are few treatises, however, on how to secure an existing global network -- sort of akin to repairing an airplane while in-flight. Since we cannot rebuild the Internet, we need to find strategies to strengthen it. But such a fix is not merely technical in nature; the Internet is also largely a social phenomenon (as Licklider predicted more than 45 years ago).

This book has 19 chapters plus an appendix, divided into four sections. Section one is titled "People Not Bits" and is composed of five chapters that provide the background and historical context necessary so that the reader can understand Hallam-Baker's perspective of the problem. More importantly, this history lesson helps the reader appreciate why known e-crime problems on the 'Net continue to persist despite the many solutions that have been proposed, ranging from the Secure Sockets Layer (SSL) to the latest privacy-enhanced version of Internet Explorer. E-crime as a social issue is the main theme here. Technology, Hallam-Baker argues, is not the sole avenue to eliminating cybercrime because technology is not the root cause; the motive is money and the perpetrators are people.

This section starts with chapters discussing the motive for e-crime ("it's the money, stupid") and a look at some of the criminals themselves. Here, Hallam-Baker introduces his premise that accountability is needed on the Web and it is this lack of accountability that enables criminal activity. The remaining chapters discuss how the architecture of the Internet protocols and infrastructure could be changed to create such accountability.

Section two, titled "Stopping the Cycle," comprises four chapters discussing intermediate changes and short-term methods with which to combat spam, phishing, and botnets. Hallam-Baker does not suggest that a global solution to e-crime can be implemented overnight. In this section, he distinguishes between the tactical changes that can slow the pace of cybercriminal activity while gaining time to implement the strategic fixes that he believes will provide a long-term solution to the problem.

"Tools of the Trade" is the third section, two chapters that delve into cryptography and the existent mechanisms for establishing trust relationships on the Internet and in cyberspace. The quote "Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography" (widely attributed by Roger Needham and Butler Lampson to each other) is wholly applicable here. Hallam-Baker does not fall into the trap of suggesting that cryptography is sufficient to solve issues of criminal activity and trust -- but crypto is necessary and, therefore, deserves the reader's understanding.

The fourth section, "The Accountable Web," is composed of the final eight chapters (and final third) of the book. This section describes the technology needed to create an accountable Web, one where individual users can be accurately identified and held accountable for their actions in cyberspace. These chapters cover such issues as next-generation secure infrastructures for transport layer and messaging applications, secure identity and naming mechanisms that will eventually morph into an Identity 2.0 architecture, secure networks and the disappearing network perimeter, secure operating systems, and advanced schemes for code signing. Laws and the legal system also have to better address e-crime, both to provide tools for law enforcement and to send a message to society that cybercrime is real crime.

The last chapter is aptly titled "The dotCrime Manifesto," and it includes a "five-point action plan for reclaiming the Internet." This plan suggests that the design of security proposals and mechanisms should have realistic goals, provide accountability, focus on end-user usability, be an integral part of the Internet infrastructure, and be ones that can be rapidly deployed.

I enjoyed reading this book for several reasons. One is that the history presented here is one that I vividly recall living through albeit more as a user than as the designer that Hallam-Baker is, given his work with the IETF and at VeriSign. Another reason is that Hallam-Baker makes many of the same points that I have tried to make in my own classes and lectures over the years: Internet crime is *crime*; black-hat hackers who attack information systems need to be taken seriously if we take our information seriously; the Internet, Web, and secure e-commerce protocols have totally changed the world-wide economy; Negroponte is right and Internet commerce is about "bits, not atoms"; and as products and money go, so follows crime and criminals.

The book is quite readable and, more importantly, accessible by the non-technical policy-maker by purposely avoiding the use of technical jargon and geek speak. The solutions discussed in this book are within our grasp; we need to demonstrate the will to make it happen. All sectors -- software vendors, Internet service providers, governments, and users -- need to play their part and work together to achieve the ultimate goal of cleaning up the streets of the Information Superhighway.

Will we ever achieve perfect security and eliminate e-crime? Probably not. But we can certainly raise the bar higher than it is today.

Kessler, G.C. (2008). Book Review: "The dotCrime Manifesto: How to Stop Internet Crime" (Hallam-Brown). *Journal of Digital Forensics, Security and Law*, *3*(2), 71-73.