ARRAY Logo

icon

Rethinking Public Key Infrastructures and Digital Certificates and Privacy

---

A Review of *Rethinking Public Key Infrastructures and Digital Certificates and Privacy*, Stefan A. Brands, MIT Press 2000. ISBN 0-262-02491-8.

Reviewed by Martin Nemzow
E-mail: mnemzow@networkperf.com
Web: www.networkperf.com

This is a background book for technical staff and some managers involved in e-commerce or its implementations. Its focus is clearly described by its title and does not wander from that topic. Much of the content is academic and very mathematical. Less-formal discussions, such as on topics of authentication implementation and smart cards, are unparalleled in current security literature because they are balanced but also supported with significant scientific and mathematical documentation. I read the book and ignored the proofs on the first pass, reading only for ideas and content. On the second pass, I still skipped some proofs, but delved into others because of their relevance to some of my actual current implementation and marketing activities.

At some point, in real ecommerce activities, security bypasses the implicit need and becomes an explicit, legal, and fiduciary responsibility. At that stage, when you need to be as well-versed as a professional and aware of foundations in security, this book represents a formal and precise reference. This college-level textbook is not a light reading, nor is it intended to be. Note that much of the book is highly mathematical with elaborate proofs of security, workflow, and implementations. To that degree, it is not a typical security manual or a book to read curled up in front of the fireplace on vacation. However, this book is a good contrast to "Secret and Lies" by Bruce Schneier because it focuses on the scientific path rather than the social engineering one. There is a distinct place for both types of books. With that representation, it is a great reference for any specialist in electronic security because of its scholarly grounding in security theorems and proofs.

This book focuses on the background for public key infrastructures and the mechanisms that create security. Half of this book is driven to the mathematics and the allegation of how certificate verification should work and what can be done to improve it. Do not overlook other parts in the book, which have a tremendous technical overview dealing with privacy, an ill-defined concept that everyone quotes and wants, but has failed to define, measure, or realistically implement. In this context, Mr. Brands defines privacy as the confidence to deliver information without having compromise. Focus in his book is establishing validity and authenticating security certificates in workflow. Relevant and referenced applications include electronic cash, electronic postage, digital rights management (such as copyright protection), protection of health information, and ways to enable electronic voting. The proofs are actually a great litmus test when talking with vendors--if you're into the mathematics and want to validate

technical support or developers with those vendors. However, the overview is actually much more informative than security books aimed at the mass market because of the formal structure and the lack of spurious or unsubstantiated assertions.

For example, Mr. Brands specifically explains how public key infrastructures can be applied for banking activities to authenticate individuals, process, and transactions. This is of relevance to JIBC readers because theft of identity is likely to become increasingly expensive crime in e-commerce and Internet banking. The rewards are great, the risk is low, and the current infrastructure remains so insecure. The burden of making identity theft wrongs right will fail to those with the deep pockets, the banks, brokerages, and businesses. Chapter 6 is specifically geared towards smart card operation. Smart cards will have increasing value in the banking community as a means to limit exposure and extent of losses. The epilogue explains what can go wrong with this technology that is sufficient background for anyone talking to vendors. It is also useful to impress and assess potential security hires and subordinates. It is a shame that the references are the usual security ACM journal articles and commercial press; the academic depth in the book itself outshines the usual stale security assertions. I would have hoped that the references would have opened new doors to security threads, but the book itself does a lot of that.