Review of the book *"Security without Obscurity"* by J. J. Stapleton, CRC Press, 2014

ISBN: 978-1-4665-9214-8

M. Frederic Ezerman

August 10, 2016

This is a review of Stapleton's book on security systems and standards. The book divides its treatment of security controls into three major areas: confidentiality, integrity, and authentication. The subtitle of the book reads *A Guide to Confidentiality, Authentication and Integrity*.

Summary of the book

The book has seven chapters. As the subtitle suggests, the main concerns are confidentiality, authentication, and integrity (henceforth, CIA). Treatments on authentication, non-repudiation, privacy, and key management are all geared towards the above concerns. This work comes from a seasoned practitioner's point of view. The author has extensive working experiences primarily in the financial service industry. He noted that widespread lack of sound technical know-how often led to repeated design and implementation mistakes.

There are various reasons attributable to such a sorry state: limits to one's knowledge, economic reasons, as well as genuine deficiencies in technical expertise even large organizations must deal with. This book was conceived to share compiled knowledge and observations about information security that the author had gathered over years as a practitioner. It emphasizes the importance of security standards by providing a roadmap showing various standards and their applicability to CIA to help stem the tide of LCD (lowest common denominator) security: minimal solution to apply the lowest possible cost and often the least effective security controls.

Chapter 1: Introduction

The first chapter gives the author's motivation, a rough description on the structure of the book, the intended readership, and a brief justification on changing the A in CIA to *authentication* instead of *availability*. The book reorganizes security controls into confidentiality, which protects data from unauthorized access when in transit, in process, as well as in storage, *integrity*, which protects data against modification and or substitution, and *authentication*, which verifies and regulates entity access to various system resources such as data and applications.

Organizations actively involved in establishing standards in various parts of the world and the outline of their modes of operation are listed. The text then focuses on standards in financial services. A brief history of the various work groups involved in managing standards in this business can be found here. This chapter, therefore, is most valuable for existing or would-be financial practitioners.

Stapleton makes a sobering observation that standards tend to depreciate from publication to implementation. There are security gaps between the requirements or recommendations spelled out in standards versus what most end products actually deliver. Most of us who dabble in cryptology understand this point, albeit vaguely at times. Examples of breaches and failures and the staggering cost of repair and recovery in this book serve as a good reminder on how crucial getting things right is.

In risk assessment, assigning costs for various types of risks is difficult. One finds a yardstick given in terms of threat and vulnerability scores here. Some methods to quantify impact of realized threat are

outlined. The chapter also discusses control adjustments to reduce the impacts of security breaches and attacks, to recover well, and to add preventive controls into the system.

Chapter 2: Confidentiality

This chapter is all about data and their treatment. A working definition of *confidentiality* is the set of security controls needed to protect data from unauthorized access during its life cycle. This chapter has three main subtopics. The first one is *data classification*, which discusses how to organize information into categories according to the impact of unauthorized exposure, either because of internal or external threats. The second one treats security controls that can be used to secure data in its various states. The states are *in transit*, *in process*, and *in storage*. The last one discusses encryption methods. Included here are issues in key management, in particular pertaining data in transit.

Chapter 3: Authentication

Methods and protocols to verify any entity that requests access form this chapter. The methods are categorized into authentication factors: single-factor, mutual (at least two entities ascertain sufficient proof of the others' identities), and multifactor (something you know, something you have, and something you are). Comparison and contrast between corporate and government technical guidelines for (electronic) authentication are supplied.

Although cryptography is used to design and deploy the three factors mentioned above, the book defines cryptography as the fourth authentication factor, tagged *something you control*, e.g., MAC, HMAC, and signatures. This is often implicitly understood yet here it is stated explicitly.

Regarding knowledge factors, it is noted that PIN in financial service industry is managed using far more stringent cryptography and key management controls than passwords in other industries. A quick recap of PIN encryption key life cycles is highlighted. Differences in characteristics and management standards between PIN and password are also discussed in considerable length.

Among the something-you-are authentication factors, the chapter allots a significant space to discuss biometric factors. These are measurable behavioural or biological traits that distinctively identify a person and are only applicable for person entities. They include fingerprints, iris scans, voice patterns, facial features, and dynamic signatures.

In terms of cryptography factors, a list of 17 mechanisms that are commonly deployed as authentication schemes is provided for those who would like to dig deeper.

Chapter 4: Integrity

Security controls to detect alteration or substitution of data due to unauthorized access form the backbone of data integrity. They are typically classified according to the data types (in storage, in process, in transit). The focus in this book is on integrity verification procedure called *integrity check value* (ICV). Its generation, storage and validation are detailed. Its roles in data integrity for all states of data are then explained.

The chapter discuss several methods to perform integrity check at length. They are redundancy checks, hash and message digest, (hashed) message authentication code (H)MAC, digital signature, and time-stamp token (TST).

Chapter 5: Nonrepudiation

The focus of this chapter is a set of controls designed to prevent repudiation, i.e., a party's refusal to acknowledge an agreement. There are two main components, namely data integrity and entity authentication. Since a judge or an arbitrator is usually in charge of dispute resolution, data integrity and authenticity must be provable to the judge. The chapter covers how methods such as MAC, HMAC, digital signatures, and TST are used for nonrepudiation. The first two (MAC and HMAC), unlike digital signatures and TST, are insufficient to establish nonrepudiation, yet they play some important roles in the overall approach.

Given the multi parties involved in nonrepudiation, the chapter discusses various technical, cryptographic, as well as operational and legal considerations, seen from each of the participating parties.

Chapter 6: Privacy

Privacy is said to have a broader scope than confidentiality. The former includes authentication, authorization, and accountability. The chapter begins with how aspects of privacy have been treated in Chapters 2 to 4 and how the topics in the said chapters contribute to controls to ensure privacy.

In many legal jurisdictions, the laws spell out privacy policies on data elements. Diversity in legal frameworks greatly affects data attributes across national or regional borders. Moving data across borders triggers various interpretations regarding the attributes assigned to data. This chapter touches briefly on cross-border jurisdictions (when exist) and provides brief guidelines on the movement of data across jurisdictions. Cryptographic keys are also subject to jurisdictional rules. Hence, compliance is a significant consideration in an organization's cryptographic architecture.

Perhaps the most instructive part of this chapter is the brief discussion on the eleven topics to consider when establishing and maintaining a security policy adopted in several standards. The discussion aids the thinking that should go inside the mind of policy makers.

In the last subsection, a comparison of the laws in several jurisdictions is given, with the EU privacy directive as the common reference point. There are interesting details that may appeal to people from diverse professional backgrounds who work with personal data in manners specific to their respective professions.

Chapter 7: Key Management

This chapter brings the book to end. Its contents have been referred to in preceding chapters that had promised to treat the technical details in this very chapter. Key management is at the center of the stage since data are protected by cryptographic keys which are in turn protected by yet other keys.

A review of symmetric and asymmetric cryptographic algorithms opens the chapter. This is intended to provide a minimum knowledge requirements for encryption and other basic protocols such as key transport and key agreement methods. How the protocols help to certify and construct modules for cryptographic software and hardware is discussed next.

Several terminologies are defined formally. *Key transport* is a key-establishment method to encrypt and then distribute cryptographic keys for eventual decryption and deployment. *Cryptographic modules* are engines that execute cryptographic algorithms. Various certifying bodies are mentioned and the relevant standards and security requirements are pointed out with some historical notes added. *Life cycle* refers to the secure handling of material, including keys, from creation to destruction or archival, i.e. throughout the material's so-called *crypto period*. Commonly used life cycle and its corresponding standard(s) are explained with differences among standards pointed out. Determining factors are the type(s) of key and the operational environment.

Cryptographic architecture consists of characteristics that describe the details of the operational environment and associated controls. Major components are listed with brief explanation. They include security policies, practice, and procedures, key inventory, and (sequential) diagrams detailing the network, data flow, and key deployment.

Public Key Infrastructure or PKI contains formal cryptographic architectures regarding the management and governance of public-key cryptography. Standards identifying crucial entities and giving frameworks of practices and policy requirements in PKI are given. Aside from technical concerns, the standards also incorporate legal and commercial considerations.

A nice feature of this chapter is the numerous tables that summarize the discussion. Often, glancing through them gives enough details to understand the main points the author raises without going through the text.

What is the book like?

This book is not an easy read. At least not in the usual sense. It can be an essential reference to keep in the arsenal of practitioners as well as researchers who advise practitioners and organizations.

This book is not suitable for a continuous reading. It is not a textbook either. It is a handy reference when one wants to orient oneself into the various standards. The flow is uneven, containing lists upon lists upon more lists. Perhaps the materials are collated from various sources or write-ups (abstracts of important documents and position papers on standards) that the author had prepared for different

occasions and audiences over an extended period of times. An example of the many overlaps is the instances where SHA-3 (Keccak) is mentioned alongside its creators and its formal adoption in FIPS 180 in adjoining subsections (7.1.3 and 7.1.4). There is also a rather unusual term, *alternation*, used in several places. The meaning is clear from the context, yet this choice of term is rather baffling.

Having said how disjointed the book can be, it is a treasure trove, full of useful details and insightful observations. Coming from a seasoned practitioner, it offers valuable lessons not usually spelled out in more theoretical works. The approach is unlike that of many other books available to our community. This one focuses on how to understand and implement various cryptography primitives in actual situations to satisfy evolving business and compliance requirements.

Would you recommend this book?

I would recommend this book to the following audiences:

- Anyone who needs an on-hand reference to specific standard(s). It is very likely that this book can point you to the exact document(s). For examples, if one wants to see standard for PKC in the financial services industry using discrete log, then X9.42 is the document to get. If ECDSA is what you want, check out X9.62. For biometric information management and security, get X9.84.
- People in the legal and compliance department of any business or agency with significant cryptography portfolios. In this era, this means basically almost any organization pass some size's threshold.
- Information security professionals for reference and refresher materials.
- Business analysts who want to understand relevant security issues for risk management purposes.

The reviewer is a Researcher affiliated with the Cryptology and Coding Theory Research Group, Division of Mathematical Sciences, Nanyang Technological University, Singapore.