Review of the book

”Smart Cards, Tokens, Security and Applications”

by Keith Mayes and Konstantinos Markantonakis (editors),
SPRINGER
2008

ISBN: 978-0-387-72197-2

Eric Diehl
Security Competence Center, Thomson

2009-10-10

What the book is about

This book provides an overview of secure chips and their applications. It mainly focuses on two types of tokens: contact and contactless. Except a brief introduction to Trusted Platform Modules (TPM), the book does not detail embedded IC or Hardware Secure Modules (HSM). The book depicts the major operating systems and environments (Java Card, Global Platform, MultOS, …) and describes in details the application development environments for Java and SIM toolkit. The book explores different fields of application: mobile, banking, Pay TV and ID cards. A special focus is given to the mobile applications.

What the book is like

Chapter 1: “*An introduction to smart cards*” introduces smart cards. The author provides his definition of smart cards with five characteristics. This definition is rather good. Then, he benchmarks existing solutions (magnetic stripe cards, chip cards, microprocessor chip cards, contactless smart cards, and smart tokens) with his definition. The author introduces different notions that will be explored later in the book (tamper resistance, issuer control, …) and highlights potential application fields. It would have been interesting that this section points to the relevant chapters of the book.

Chapter 2: *“Smart Card Production Environment”* is an extensive description of the manufacturing process of a card. It starts from how to build a plastic card to end up in the shipment. At the end of the chapter, you guess that the key word is diversity. The chapter lacks pictures of tools for the reader to have an idea of the size or shapes, ... A diagram describing the different steps of the complete process would have been extremely useful. From my perspective, the sub-section describing security is too small. For instance, why not tackle the different steps that avoid leakage or theft of “virgin” products?

Chapter 3: *"Multi application Smart Card Platforms and Operating Systems"* gives a tour of current OSes. The description of Java Card is good and provides a basic view. I would have appreciated a more detailed description of Java Card's security model. Then it describes the Global Platform Card Specification and MultOS. Unfortunately, there is no consistency between all the descriptions. For instance, each architecture uses a different formalism. The illustrations use different styles. Thus, it is difficult to compare. The remaining OS: smartcard.net , Basic card, or WfSC are just mentioned.

Chapter 4: *"Smart Cards for Mobile Communications"* attempts to describe how SIM/USIM allows a new world of communication and powerful applications. I must confess that I do still not have a clear understanding of the system. A presentation of the overall security architecture is lacking. The authors do not find the right level of description. Most of the descriptions are at very high level (missing some flesh) whereas some descriptions are going at the bit level confusing even more the reader (or at least me). Chapter 11 does a better job on this.

Chapter 5: *"Smart cards for Banking and Finance"* I really enjoyed reading this chapter. The authors explain why EMV was created to limit the fraud. The presentation on how the users' cards and the banks securely exchange the data allows better understanding the mechanisms. Then the chapter focuses on the Non Present Card (NPC) problem. It clearly highlights the threats. It concludes with the description of new systems (such as 3D secure) that may partly solve this issue. The brief analysis on why a mobile phone cannot be an acceptable authentication token for Internet EMV transaction is excellent. The authors are extremely pragmatic and do not underestimate issues such as deployment costs, and users' acceptance. A small regret is the absence of e-purse experience such as French Moneo.

Chapter 6: *"Security For Video Broadcasting"* I was waiting eagerly for this chapter. The chapter gives a reasonable description of DVB system. Nevertheless, there is a serious mistake. The chapter never explains the role of the smart card without associating it with the DVB Common Interface (Why using this incredible acronym CIM when the usage is to use DVB-CI?). DVB can work without DVB-CI directly communicating with the smart card. I am not sure that the casual reader will be able to explain clearly what the role of the smart card is. Unfortunately, the chapter is fully DVB centric. It never speaks about US Open cable or US OCAP… It would have been interesting to make a generic description of smart card based Pay TV and then specialize it.

Chapter 7: "*Introduction to TPM"* describes the expected features of the TPM as published by TCG. It briefly describes how these features may be implemented. The sub-section that explains the services and how to use them (root of trust, secure boot, secure storage, attestation) is not detailed enough. At least, it would have been interesting to explain the behavior of the PCRs and how they are used to check the integrity of an environment. Let's consider this chapter as a good teaser for TPM. The hungry reader will have to look elsewhere.

Chapter 8: *"Common Criteria"* is an excellent introduction to CC. It clearly explains the rationales. It describes the different elements of a Target Of Evaluation. The author also gives a very pragmatic view on the associated cost and efforts.

Chapter 9: *"Smart Card Security"* gives a very good introduction of the different types of attacks that may apply to smart cards. It briefly describes invasive attacks. The focus is on semi-invasive and non-invasive attacks. He presents the different categories of side channel attacks. The author clearly likes the more esoteric but lethal fault injection attacks. He illustrates the fault injection by two simple to understand examples. A large bibliography allows the hungry reader to dive in more technically oriented descriptions.

Chapter 10: "*Application Development Environments for Java and SIM Toolkit*" provides a first lecture to Java card. Once more, the chapter oscillates between a lot of details and a very high view. The section on the tools is very useful to get an idea of what you'll need. The section "A word on testing" should have been a "large section on testing". The problem of testing a product before releasing it and leaving out all the tricks used for debug deserves more. The section on Dongle is surprising.

Chapter 11: *"OTA and Secure SIM Lifecycle Management"* At last, I understand better SIM/USIM. This chapter clarifies how a SIM card works in its environment. The Lifecycle management is very interesting. We should have had a lifecycle management for each explored domain.

Chapter 12: "*Smart Card Reader APIs"* is an excellent introduction to OpenCard Framework and PC/SC. Concise and clear.

Chapter 13: "*RFID and Contactless Technology"* The UFO chapter; compared to previous chapters which were mostly at very high level, this chapter dives into the details. You will learn the equations that rule electromagnetic fields. You will learn the details on how the protocol of communication handles collisions. And you may enjoy it because it is well written. I must confess that I did not read too much the electromagnetic equations but I never thought how to create a return channel with an antenna that powers the chip.

Chapter 14: *"ID Cards and Passports"* gives a hint of the physical security inside this type of plastic cards. Of course, it cannot go into details. These are secrets, as for printing bank notes. I suppose there are many similarities and common techniques.

Chapter 15: *"Smart Card Technology Trends"* draws the history of smart cards. Nevertheless, it is funny that in a book about smart cards you never encounter the name of Moreno. The chapter clearly explains that there are four trends: more power (SIM), more storage, more security and cheaper (banking, transport). These trends are not necessarily aligned. I would have appreciated to have an idea of what the smart card may look in 2020.

Recommendation

As for many books that are a collection of articles, there is a strong lack of consistency, and many redundancies. A small twist is the special focus on UK, forgetting many other countries were applications are widely deployed. Nevertheless, the book is rather easy to read.

Should you read it? If you are looking for a basic introduction to smart cards, this may be one of the references to read. Thus, it may interest non-security students, people who want to have a first level of understanding, journalists… If you are looking for a good understanding of one of the domains of use of smart cards, then look for a more specialized book. If you are a security expert, definitively this book is not for you.

In my mind, smart cards are strongly associated to security. Security is mainly absent one from this book (except in chapter 9). The book never speaks about the hacks. In the contactless field, often the transport cards are cited. Nowhere the recent hacks have been cited. For ID cards, nowhere the recent problems of passports have been disclosed. Hence, the book may give an idealistic view of smart cards.

The reviewer is the head of Thomson's security competence center,
Rennes, France.