Review of the book

"Paiements électroniques sécurisés"
by Mostafa Hashem Sherif
Presses polytechniques et universitaires romandes, 2007

ISBN: 2-88074-694-0

Olivier Blazy, Xlim, Université de Limoges, France

2016-08-28

1 Summary of the review

This book gives an overview of e-commerce technologies in French as of 2007. The book is nicely written, and nearly self-sufficient. However the decade gap since the publication makes most of the chapter obsolete, and readers interesting into developing solutions should really read additional material before doing so.

2 Summary of the book

The author, Mostafa Hashem Sherif, a research engineer at AT&T, describes this book as presenting the state of the art around electronic cash, and electronic transactions. He does a broad presentation, mixing formal part coming from conferences, and other more accessible inspired by the Financial Times. This book is divided into three main parts.

- The first three chapters are dedicated to the general context of electronic transactions (as of 2007).
  - The first chapter "What is electronic commerce" explains the general context, what categories of electronic commerce exist, what is the impact of electronic transactions and in particular what was the effect of the emergence of the Internet, and where they happen in every day use and what are they consequences.
  - The second chapter "Currencies and other means of payment" is about currency and how it is handled in various countries, to show the various habits and that the users expectations are really diverse throughout the world. So it presents arious means of payments (cash, cheques, wire-transfers, recurring payments, cards,...). It then consider virtual currency, and the various possibilites it brings, and compares those to real life "physical" money. It then focus on banking system in the United States, the United Kingdom and France, to underline the specifity some region can expect.
  - The third chapter "Architecture and securisation algorithm" starts to get technical, and explain the OSI system, and some basic cryptographic notion. This is there, to lay the foundations for the other chapter and be sure, that every one starts on a solid ground. It explains symmetric and assymetric cryptography, data integrity, identification and athentification of users, access control, denial of service, Public Key Infrastructure.
- In the second part, chapters 4 to 12 the author gives an overview of the main available solutions to secure transactions.
  - In chapter 4 and 5, the author starts by Speaking about SSL and TLS. It explains its architecture, the various subprotocols, its performance, and some of its implementations. he then widen the spectrum to the wireless exchanges, in particular with WTLS.

  - Chapter 6 is dedicated to the SET (Secure Electronic Transaction) protocol, used for bank card transaction. Once again, the author explains its architecture, and security. He then gives a more detailed approached on how sales are handled, and how efficient the instantiations are.
  - Chapter 7 follows the same idea but for online payments, via C-SET of Cyber-COMM. He then shows how it can be improved with TLS, and how 3D-Secure can further improve the global security. Anecdotically it also mentions secured payments via CD-ROM...
  - Chapter 8 and 9 are dedicated to micropayments. It follows the same structure as before, this time for CEPS, ECML, Advantis, Chipper, FeliCa, GeldKarte, Mondex, Proton and then proceed to compares those solutions. It then consider remotes solutions, First Virtual, NetBill, KLELine, Odysseo, . . .
  - The next two chapters are dedicated to dematerialized currency. First it explains the general principal of non-traceability of both ends of the transaction, and then consider two solutions digicash and netcash. Then it considers dematerialized cheques, first by explaining how they work in the physical world, and then by considering Netchaque, BIPS (Bank Internet Payment System) and eCheck.
  - The final chapter is dedicated to Chip Cards. It first desses a little history and present various applications. It then reminds the various ISO norms, and the EMV specifications. It finishes with some possible attacks either logic, or invasive.

- In the third and final part, is more focused on norms (like X12, EDIFACT) or new ones, at the time, (ebXML, SEMPER, Web services). The author proposes various examples, like bank wire-transfers, bill dematerializations, and others all coming from real-life scenarios.

  - Chapter 13 is devoted to Intercorporation e-commerce. It presented an overview of what is hidden behind this term, some history of what has already been done, and the various norms linked to this (ANSI X12, EDIFACT, X 400, . . .)It continues by having a closer look at XML and ebXML and various web services (WSDL, UDDI, SOAP).
  - Chapter 14 goes a little more in depth, and focuses on e-commerce systems like SEMPER, CAFE, JEPI, PICS and P3P. It then considers analysis of user behavior, how fidelity cards works in the context
  - The last chapter tries to give an overview of e-commerce in society. First by considering the linked infrastructure, then how to generate e-cash, how intellectual property is limiting the developement of solutions, how surveillance may not collaborate well with e-cash, but still how one can manage fraud.

The parts are designed so that both technicians, engeneers and marketers can make the best out of them. When a chapter gets to technical, there is an abstract at the end dedicated to summarize the notions presented.

3 What the book is like

In the book the author tries to be very pedagogical, and explains clearly what the various problematics / solutions are. He does so using his industry experience, and proposes convincing real-life scenarios.
For each notion, you can find a detailed litterature on the topic, clear figures explaining how things works, and several references to obtain more details.
The whole book tries to be self sufficient, the first part tries to introduce the global problematics around e-commerce, and the necessary building blocks to understand the notions involved. The second considers the various existing solutions (as of 2007) and place them into context to better explain how they are used in the real world. The final part surrounds the norms used to articulate those protocols, and wraps up neatly the presentation of e-commerce solutions.
At the end of the book, there are some appendices. The first one is a collection of links to give even more details on the various notions seen throughout the book Encryption Kerberos, Certification, Biometry, Standardisation, various e-commerce solutuons, SSL/TLS/WTLS, Online purse, Online payments solutions, Chip Cards, XML/EDI intergration, various norms, SEMPER, Labelisation organisms, and some

legal aspect. The author then presents an extensive (35 pages long) bibliography, allowing the reader to see the source of all the information provided.

An index is present at the end of the book, and which let the reader uses it as a reference manual if needed.

4 Recommendation

It's not so easy to determine who is the best target for this book, considering the last version was published in 2007, and starts to be a little outdated. In addition to that, one should not forget that this book is written in French; which reduces even further the number of potential readers.

Overall, I guess this book can still work for two different audiences: on one hand students in Computer Science / Network Security might be interested, on the other hand security professionals can use it as a convenient reference book to understand what was done in the past.

Students can easily understand how things work thanks to the various figures / definitions and if they need some precision they can read the corresponding section with the support of the previous figure. This book is going to give them a lot of context, and will allow them to see what was happening, and how and why some of the current protocols / norms were adopted.

On the contrary, professionals will probably focus on specific subsections, while maybe using the figures only to summarize some of the notions. (Or to explain a notion to a neophyte). The different applied examples can give direct solutions to some problems. However for real-life deployments they need to be carefull, and read more up to date material to avoid some modern security flaws, or to learn more about modern solutions. (There is no mention of bitcoin and blockchain-based technology for example)

This book was an interesting read, but while it is nicely written, it should more be seen as a time-machine to travel 10 years back, than as a valid book giving modern state of the art. I would recommend it to "crypto-historian" who wants to understand how we arrived to present day solutions, but people wanting ready to use solutions, should not use it.

The reviewer is a Maitre de Conférence in Cryptography at the University of Limoges.