Review of the book

"La Fracture Cryptographique"

by Serge Vaudenay

Focus Science, 2011

ISBN: 978-2-88074-830-2

Olivier Blazy, XLim, France

2014-07-15

1 What the book is about

As explained by the author, Serge Vaudenay, the books aims to explain network security. Instead of considering networks as a media of communication, he focuses on them as a source of security and insecurity. This book tries to highlight the main issues with networks where security was not part of the design process.

This book is divided into 10 chapters covering basic everyday cryptographic notions, and how they impact our privacy. In the first part the author focuses on basic introduction to cryptography like what is a ciphertext, how to define confidentiality, what are the standard primitives, and basic weaknessess. Then in another part, he presents advanced concepts like blind signatures,trust concepts, and finally authentication strategy (wireless, mobiles) but also bluetooth, and biometric passports. The last chapters shows the shortcomings of such technologies and how they reduce our liberty, and propose reflexion on how to use cryptography correctly.

- The first 4 chapters (Encryption, Third party insurance or comprehensive insurance? Digital Confidentiality, Cryptologic bestiary, Warning: Security Loss) are here to explain basic notions surrounding cryptography. First chapter contains explanations of Kerckhoffs principle, the idea of secret key cryptography, an example with Vernam encryption, and then public key cryptography with an example using ElGamal encryption, RSA, so basically the basic Crypto 101 ideas, explained is a didactic way with clear example and a logical approach. In the second chapter, you can find explanations on key recovery, lunch time attacks, adaptive attacks with various examples. Chapter 3 goes a little more into details, and give proper definition of more sophisticated primitive Message Authentication Code, Key Exchange, Quantum Cryptography, Hash Functions, Secret Sharing, ZKPK, Oblivious Transfer. This gives the reader a good overview of classical techniques in Cryptography, with ideas to when they appear. The last chapter of the first part, is about security loss, with Moore's Law, Cryptanalysis ideas, Factorisation, Discrete Logarithm, and then why quantum computing can change everything, side-channel attacks are also evoked. This chapter shows why security is at stake, and the importance of valid models.

- The next 4 chapters are more in touch with Today's world, where we do not need to meet in person any more, and life can be orchestrated from behind a computer screen. First he shows how to do a fair head or tail protocol via telephone to explain basic of secure multi-party computation, then focus on the various kinds of signatures (blind, ring, fail-stop), and then fair exchange, overall this chapters allows to see various mechanisms to build trust in communication between two entities, which is the heart of the next chapter. In this new chapter he presents the differences between the *MAC and encrypt* and the *encrypt and MAC* approaches, the idea of Third Party, the SSL model, SSH, PGP, ID-based cryptography. The third chapter of this corpus is about access control, and explains the classical tryptic using what we know (password), what we possess (key-card, chip-card,...), who we are (speech recognition, facial recognition, finger prints, ...), he then concludes the part with a chapter on wireless communication by speaking about GSM, 3G, DECT, WiFi, Bluetooth, biometric passport.

- The third part is more here an invitation to reflect on what kind of security we want, the first chapter is about the paradox with anonymous identification, where the author explains that in the end we have various spheres of privacy and we want to stay anonymous between those spheres, and so recall general principles like be careful with who you are interacting, who you trust, he explains how to identity anonymously in the middle of the crowd or how to anonymously target someone in the middle of a crowd. The final chapter considers the transition from digital threat to real life consequences by considering everything that can lead to invasion of our privacy so cookies, spams, phishing and techniques that can be dangerous is badly used like biometry, universal identification, electronic voting.

2 What the book is like

In the book, the author tries to explain to everyone how cryptography works, and what are its modern goal, and why those goals do matter in our modern communication world. The whole book is self sufficient to have a rough understanding of what is the current problem, and why finding a good solution can cause problem. Each chapter tries to give a good overview of a specific concept with more practical examples.

After the first chapters the reader should have a decent understanding of what an encryption is, what signatures are, why both are useful and how they might complement each other. The next chapters are more interested in practical applications, and gives primitives that are used in real world scenario. The end chapters, ask several question, which make the reader consider the future.

Lots of figures are present throughout the book, making it easy to read and follow.

A, rather long, bibliography at the end of book, refer to papers either classical or coming from the EPFL, allowing a (scientific) reader to obtain more details on specific concepts.

Overall the book is written in a light hearted way, with jokes, pun and other things are distilled through the reading to keep things interesting. However under this humor, there is a deeply cynical approach, that says that anyway in spite of all the efforts researchers could put in the area, industrials and global policies will always take the easiest approach, and not favor users privacy, even when it's reachable.

3 Recommendation

The book could / should be read by three kinds of audience:

1. I guess, the book is targeted mostly for person new in the global area of cryptography / security and want to have a good overview of the real questions. In fact, it could be a very interesting introduction reading for students in Computer Science / Network Security. Students can easily understand how things work thanks to the different figures / definitions and if they need some precision they can read the corresponding section with the support of the previous figure, and if they continue on this field, the bibliography in the end gives them a really nice set of references to have extra precisions.

2. The final chapters are asking very important questions, that every professional / politicians should have in mind. Modern technology, and modern techniques allow a lot of things, and instead of going to hasty in one direction, people should really take time to reflect on those questions and tries to conceive protocols trying to answer them.

3. The book might also interest industrial, and politicians, it would allow on hand to remind them some basic notions of cryptography, and then it might help conceive security policy that take into account users privacy, or at least have to conscientiously forget to take care of it.

There is however a small, insignificant little twist to those recommendations, the book is written in French, so a decent understanding of the language is required.

The reviewer is a Maître de Conférence at the University of Limoges, France.