Review of the book

"Handbook of Financial Cryptography and Security"

edited by Burton Rosenberg

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4200-5981-6

S. V. Nagaraj

2014-11-22

1 Summary of the review

Cryptography is an interesting subject that has many applications in the real world. This review is about a handbook on financial cryptography and security. The handbook offers a good introduction to the usage of cryptography for financial applications.

2 Summary of the book

In today's world, computers and Internet have become ubiquitous. Cryptography which was used earlier primarily for military applications has now become indispensable for making our financial systems secure. This handbook on financial cryptography and security covers many aspects essential for modern applications. The handbook is made up of five parts and has nineteen chapters. It has been published in the series "Cryptography and Network Security" of Chapman and Hall / CRC Press.

The first part deals with protocols and theory. It has six chapters.

Chapter 1 (E-Cash) looks at electronic cash protocols and security concepts. Chaum's e-cash, Brands' e-cash, and compact e-cash are discussed. Extensions of compact e-cash are also studied.

Chapter 2 (Auctions) offers a short introduction to auction theory and cryptographic auction protocols. Unconditional privacy and computational privacy are also discussed.

Chapter 3 (Electronic Voting) looks at the basic properties of systems for elections. On-site and online voting are compared.

Chapter 4 (Non-repudiation) describes the basics of non-repudiation. Mechanisms for securing digital signatures for non-repudiation is also looked at. Fair non-repudiation protocols and multi-party non-repudiation protocols are also discussed.

Chapter 5 (Fair exchange) explains the concepts of fairness in electronic exchanges and solvability of fair exchange. A selective literature review is done and fair exchange in the Dolev-Yao model is scrutinized.

Chapter 6 (Broadcast and content distribution) provides a brief overview of broadcast encryption and security mechanisms for encrypting broadcasts.

The second part is on systems, device, banking, and commerce. It has five chapters.

Chapter 7 (Micro-payment systems) introduces the concept of micro-payment systems and looks at their characteristics. A historical overview is given and two generations of micro-payment systems are described.

Chapter 8 (Digital rights management) familiarizes the reader with the digital rights management model, standardization and interpretability issues, applications, implementation aspects and miscellaneous issues.

Chapter 9 (Trusted computing) discusses the trusted computing approach, compliance and security, security architectures, and further extensions.

Chapter 10 (Hardware security modules) explains the use of hardware security modules. Their realization is discussed and future trends are given.

Chapter 11 (Portfolio trading) looks at the cryptographic building blocks, communicating risks in portfolio holdings, the risk-characteristic protocol and its applications, cryptographic securities exchange, and crossing networks with liquidity providers.

The third part is on risks, threats, countermeasures, and trust. It has five chapters.

Chapter 12 (Phishing) discusses the risks due to phishing which involves luring an internet user to reveal personal details such as passwords and credit card information on fake web pages or email forms that pretend to come from a legitimate source. This chapter looks at the state of phishing and related attacks. Device-centric attacks and data mining concepts related to phishing are also studied.

Chapter 13 (Anonymous communications) discusses anonymous communications, trusted and semi-trusted relays, mix systems, robust and verifiable mix communications, and onion routing.

Chapter 14 (Digital watermarking) introduces the concept of digital watermarking and studies mechanisms for embedding and recovering watermarks, perceptual aspects, attacks, fingerprinting, embedding watermarks securely, and other concepts.

Chapter 15 (Identity management) describes what is meant by identity, other meanings of identity, and notions in addition to enterprise identity management.

Chapter 16 (Public key infrastructure) describes security decisions, X.509 certificates, other certificate semantics, complex decision algorithms, fundamentals, and miscellaneous concepts.

The fourth part is on perspectives. It has three chapters.

Chapter 17 (Human factors) looks at trust and perception of security, use of deception, the psychology of risk, and usability.

Chapter 18 (Legal issues) discusses legal issues related to financial cryptography, unauthorized access to personal information, legal obligations and liabilities.

Chapter 19 (Regulatory compliance) is the final chapter of the book. It looks at the challenges in ensuring regulatory compliance.

All the chapters of the book include references to the literature. The book includes a helpful index.

3 What is the book like (style)?

The handbook offers a good introduction to major issues related to financial cryptography and security. It includes contributions from 29 experts from around the world. They come from academia, industry and research labs. The chapters of the handbook are well written and may be read independently. Despite contributions from several experts, the presentation in the handbook is uniform. A basic background in number theory and the theory of computation will be helpful for the readers of this handbook for understanding the topics discussed. The handbook will be useful for researchers in information security. It will also be useful for teaching courses related to financial cryptography. The handbook offers answers to many questions related to financial cryptography. It also provides solutions to many real-world security problems in the field of financial cryptography. However, it should be emphasized that the handbook offers only a snapshot of financial cryptography and security as entire volumes have been written on topics discussed in the book. There are many topics that are related to the financial cryptography and security for which the reader must look elsewhere. These include for example, access control, audits, biometrics, bitcoins and other cryptographic currencies, cloud computing, fraud detection and forensics, insider threats, prevention of financial crimes, privacy, secure banking and financial services, secure hardware and secure tokens, security of mobile systems, social engineering, smartcard security, and Web security,

4 Would you recommend this book?

The handbook offers an excellent introduction to many issues related to financial cryptography. I strongly recommend it for those interested in learning the techniques and challenges in financial cryptography and security.

The reviewer is a freelancer in Chennai, India