

## BOOK REVIEWS

### WIRELESS SECURITY AND CRYPTOGRAPHY: SPECIFICATIONS AND IMPLEMENTATIONS

EDITED BY: NICOLAS SKLAVOS AND XINMIAO ZHANG, CRC PRESS / TAYLOR & FRANCIS GROUP 2007, ISBN 10: 0-8493-8771-X, ISBN 13: 978-0-8493-8771-5, HARDCOVER, 400 PAGES

REVIEWER: MARCIN NIEMIEC

This book is a collection of independent texts gathered by Nicolas Sklavos and Xinmiao Zhang. The authors present in detail many specifications of algorithms, such as Advanced Encryption Standard (AES), elliptic curves, and the hash function Whirlpool, as well as the implementations of security solutions in Bluetooth, WLAN, and Universal Mobile Telecommunication System (UMTS). The book is well organized and readable as a whole. Although some chapters describe the same security basics and algorithms, this is not a disadvantage because it allows each chapter to be read independently.

This book can be recommended for university researchers and graduate students in computer science and information systems. Also, engineers, wireless system architects, and developers will find in it interesting and useful content. For professionals each chapter includes extensive bibliographic notes.

The book consists of 13 chapters that cover most of the main security issues in wireless networks. The first chapter, "Overview of Cryptographic Primitives for Secure Communication" by Palash Sarkar, is an introduction to cryptographic solutions that are able to ensure confidentiality and integrity of data in wireless communications: block and stream ciphers, hash functions, key agreement, asymmetric cryptography, digital signatures, and identity-based encryption (IBE).

"Introduction to Communication Security," by Vesna Hassler, is a short chapter that includes a lot of basic terms involved in security and is recommended for security beginners. The author explains security basics (threats, security services, mechanisms, and techniques), and also considers some issues connected with key management, security evaluation, and audit.

Chapter 3, "Efficient VLSI Architectures for the Advanced Encryption Standard Algorithm" by Xinmiao Zhang, is devoted to the symmetric-key cipher AES. First, an accurate description of the algorithm is pre-

sented. Later, the author presents architectural and algorithmic optimization approaches to efficient hardware implementations of the AES, as well as resource sharing between encryptors and decryptors. Some algorithmic modifications of the AES are also presented.

The next two chapters, "Hardware Design Issues in Elliptic Curve Cryptography for Wireless Systems" by Apostolos P. Fournaris and O. Koufopavlou, and "Efficient Elliptic Curve Cryptographic Hardware Design for Wireless Security" by Lo'ai A. Tawalbeh and Cetin Kaya Koc, are dedicated to elliptic curve cryptographic (ECC) hardware design for wireless systems. Both chapters, besides the issues of efficient hardware design, include the basics of ECC: group theory and elliptic curves theory.

In Chapter 6, "Cryptographic Algorithms in Constrained Environments" by Vincent Rijmen and Norbert Pramstaller, the authors present some issues described in the three first chapters of the book: cryptographic primitives, hardware implementation issues, and the AES algorithm. In addition, the hash function Whirlpool is presented in detail.

Chapter 7, "Side-Channel Analysis Attacks on Hardware Implementations of Cryptographic Algorithms" by Siddika Berna Ors, Bart Preneel, and Ingrid Verbauwhede, describes many passive attacks on hardware implementations: differential attacks, timing attacks, power attacks, electromagnetic attacks, and acoustic attacks. Beside the summarization of previous side-channel attacks, the chapter presents passive attacks the authors have conducted on the hardware implementation of Data Encryption Standard (DES), AES, and ECC.

The next three chapters (8 to 10) describe security architectures in the wireless communication network and their hardware implementations, presented in order of the range achieved. "Security Enhancement Layer for Bluetooth," by Panu Hamalainen, Marko Hannikainen, and Timo D. Hamalainen, presents a novel enhanced security layer (ESL) for Bluetooth. This chapter describes standard Bluetooth security and the proposed ESL architecture (authentication, encryption, and data integrity services) as well as implementation of the ESL. The next chapter, "WLAN Security Processing Architectures" by Neil Smyth, Maire McLoone,

and John V. McCanny, considers two architectures that can be used to ensure efficient WLAN security. An improvement in WLAN cryptographic processing is achieved by means of cryptographic instructions contained in the instruction set architecture (ISA) of a microprocessor and implementation of the hardware accelerator block. "Security Architecture and Implementation of the Universal Mobile Telecommunication System" by Paris Kitsos and Nicolas Sklavos is the final chapter of the three. The authors present hardware implementation of the UMTS security architecture as well as an evaluation of it.

Chapter 11, "Wireless Application Protocol Security Processor: Privacy, Authentication, and Data Integrity" by Nicolas Sklavos, deals with a security processor for the Wireless Application Protocol (WAP). The author presents a novel wireless transport layer security (WTLS) architecture supporting authentication, privacy, and data integrity. The hardware implementation of the proposed WTLS architecture, as well as verification, testing, and evaluation issues are covered in this chapter.

Chapter 12, "Binary Algorithms for Multiplicative Inversion" by Erkay Savas, consists of two parts. The first part describes binary inversion algorithms for prime fields  $GF(p)$ , and the second includes inversion algorithms for binary extension fields  $GF(2^n)$ . The chapter also includes discussions about the performance of the algorithms from software and hardware implementation points of view.

Chapter 13, "Smart Card Technology" by Martin Manninger, is dedicated to smart card technology. The first parts of the chapter present a general overview of smart cards: classification, applications, operating system, and file system. The rest describe smart cards from a security point of view: cryptographic abilities, access control, authentication, secure messaging, and an example of mobile payment secured by a SIM card.

The fact that many security aspects are widely discussed is the great advantage of this book. It allows one not only to acquire general knowledge about security specifications and implementations, but also to find out particular security solutions in different environments. In my opinion this book is worth recommendation because it presents the current status of wireless security and describes future directions.