Review of the book

"Secure Smart Embedded Devices, Platforms and Applications"

by Konstantinos Markantonakis, and Keith Mayes (Eds.)

Springer 2014

ISBN: 978-1-4614-7914-7

S. V. Nagaraj

2015-10-24

1 Summary of the review

Embedded systems have become very important for routine day to day activities. This book provides an overview of the security and practical issues related to embedded systems, platforms, and applications. The emphasis is on real world applications.

2 Summary of the book

The book discusses secure smart embedded devices, platforms and applications. It is divided into four parts and comprises twenty four chapters.

The first part of the book focuses on embedded devices. It has five chapters.

Chapter 1 (An Introduction to Smart Cards and RFIDs) describes the application requirements. It acquaints the reader with contact and contactless smart cards and devices based on Radio Frequency Identification (RFID). The availability of a wide range of smart card devices is emphasized.

Chapter 2 (Embedded DSP Devices) gives a brief introduction to Digital Signal Processing (DSP) and then describes the architecture, implementation, security, and applications of embedded DSP systems.

Chapter 3 (Microprocessors and Microcontrollers Security) discusses the security design of embedded Central Processing Unit (CPU) architectures.

Chapter 4 (An Introduction to the Trusted Platform Module and Mobile Trusted Module) looks at the Trusted Platform Module (TPM) - a tamper resistant component that provides trust in secure computing and remote attestation frameworks. The architecture, operations and services of the TPM are looked at and the treatment is widened to the mobile trusted module.

Chapter 5 (Hardware and VLSI Designs) discusses security in the context of hardware implementations.

The second part of the book is on generic security and processing platforms. It has four chapters.

Chapter 6 (Information Security Best Practices) stresses the importance of securing IT systems and includes a treatment of algorithms, key sizes, and trust management along with a case study.

Chapter 7 (Smart Card Security) describes attacks and countermeasures as applicable to smart cards. The focus is on attacks that could affect cryptographic algorithms.

Chapter 8 (Graphics Processing Units) introduces Graphics Processing Units (GPUs) for general purpose computations and then studies their use in cryptography and cryptanalysis.

Chapter 9 (A Survey of Recent Results in FPGA Security and Intellectual Property Protection) describes the recent structure of Field Programmable Gate Arrays (FPGAs). It then discusses security intellectual properties in FPGAs and ways of improving the security.

The third part of the book is on applications and platform embedded security requirements. It has eleven chapters.

Chapter 10 (Mobile Communication Security Controllers) discusses the possibility of using software Subscriber Identity Modules (SIMs) instead of smart card-based solutions.

Chapter 11 (Security of Embedded Location Systems) looks at basic approaches for determining location information in embedded systems. The resilience of these methods against sophisticated attacks is discussed and proposals are made for securely verifying physical location estimates. The security of Global Navigation Space Systems (GNSS) is also briefly reported.

Chapter 12 (Automotive Embedded Systems Applications and Platform Embedded Security Requirements) presents motivation for security in embedded automotive platforms and highlights the need for automotive security.

Chapter 13 (Analysis of Potential Vulnerabilities in Payment Terminals) focuses on the security of payment terminals. The aim of the chapter is to provide an understanding of the potential attacks mentioned in the literature.

Chapter 14 (Wireless Sensor Nodes) looks at applications, constraints, architecture, operating systems, and security concerns of wireless sensor nodes. It provides key references to the literature on these topics but it is not exhaustive.

Chapter 15 (Near Field Communication) deals with different operating modes and use cases that can be implemented with Near Field Communication (NFC) technology with focus on mobile phones.

Chapter 16 (The BIOS and Rootkits) focuses on the Basic Input Output System (BIOS). It describes the main functions of the BIOS and studies attacks and countermeasures. The installation of a rootkit is often the next stage of attack once the BIOS has been compromised. Hence rootkits are also discussed in this chapter.

Chapter 17 (Hardware Security Modules) elaborates on Hardware Security Modules. These are devices for performing cryptographic functions such as data encryption / decryption, certificate management, and calculation of specific values such as Card Verification Values (CVVs) or Personal Identification Numbers (PINs). The chapter studies the usage, physical security, security evaluation, and management of hardware security modules.

Chapter 18 (Security Evaluation and Common Criteria) discusses security evaluation issues and the Common Criteria evaluation scheme for embedded devices.

Chapter 19 (Physical Security Primitives) is a survey on Physically Unclonable Functions (PUFs) and PUF-based security solutions.

Chapter 20 (SCADA System Cyber Security) offers an overview of the cyber threats and vulnerabilities affecting System Control and Data Acquisition (SCADA) systems. These systems are used in monitoring and controlling industrial processes.

The fourth part of the book provides practical examples and tools. It has four chapters.

Chapter 21 (An Overview of PIC Microcontrollers and Their Suitability for Cryptographic Algorithms) gives an overview of Peripheral Interface Controller (PIC) microcontrollers and their suitability for cryptography. It describes means of investigating their strength against side channel analysis.

Chapter 22 (An Introduction to Java Card Programming) provides an introduction to programming smart cards using Java Card. The nuances of working within a restricted environment and its implications on application design are mentioned.

Chapter 23 (A Practical Example of Mobile Phone Application Using SATSA (JSR177) API) provides a practical example of a mobile phone application implementing the Security and Trust Services Application Programming Interface (SATSA API). Freely available tools were used for the demonstration.

Chapter 24 (Wireless Sensors (Languages/Programming/Developments Tools/Examples) is the last chapter of the book. This chapter concentrates on three major wireless sensor node technologies viz. Sun Small Programmable Object Technology (Sun SPOT), Arduino, and TinyOS to help the implementer choose the best option for the application in hand.

3 What is the book like (style)?

This book consists of chapters that may be read individually or as a whole. The chapters have been authored by 36 experts largely from Europe specializing mainly in information security. The chapters are packed with information about specific topics and contain adequate references for further study. Many chapters have been authored by the editors themselves. The book can serve as a textbook on secure embedded devices, however, it does not include exercises and questions. The book unfortunately contains a large number of typographical errors and some grammatical errors. Many abbreviations are used in the preface without their expansions, so it is hard for readers to figure out what they represent, in the absence of a list of abbreviations. It should be emphasized that the book is introductory in nature as whole books are available for some of the topics in the book such as RFID security, smart card security, security of embedded devices / systems, hardware security, information security best practices, FPGA security, security of payment terminals, NFC security, security of wireless sensor networks, rootkits, hardware security modules, security evaluation, common criteria, physically unclonable functions, SCADA security, and Java card programming. The book is essentially an updated extension of an earlier book, Smart Cards Tokens, Security and Applications, Springer, 2008, ISBN 978-0-387-72197-2 by the editors. The reader may refer `https://www.iacr.org/books/2009_sp_MayesMarkantonakis_SmartCards.pdf` for a review of that book.

4 Would you recommend this book?

This book offers an introduction to secure and smart embedded devices, platforms and applications. I recommend this book for students, researchers, and practitioners.

The reviewer is a Professor of Computer Science and Engg. at VIT University, Chennai campus, India