Review of the book

"Security in RFID and Sensor Networks"

by Yan Zhang, Paris Kitsos

CRC Press, Taylor & Francis, 2009

ISBN: 978-1-4200-6839-9

Maria Cristina Onete
CASED (TU Darmstadt)

1 What the book is about

This book presents various security aspects in RFID and sensor networks. Each chapter represents a self-sufficient, independent paper, and the topics are not formally bound together by means of e.g. an introduction or an overview of the debated topics. The editors have chosen and arranged the discussed topics in such a way, however, as to give a good overview of the security challenges in resource-constrained environments. The general structure of the book is as follows: there are three parts, the first of which covers RFID, the second elaborates on security in wireless sensor networks, whereas the third refers to challenges and solutions which are valid in both cases.

In particular, the book's 24 chapters can be informally grouped as follows:

① Part *I*, RFID: this is the most comprehensive part of the book, containing 13 papers, which I can classify in the following categories:

- How to attack an RFID system. There are three topics describing how to attack an RFID system in practice. Chapter 2 of the book gives a first overview of possible attacks, chapter 3 offers an analysis of RFID Relay attacks, whereas chapter 8 shows how to concretely perform relay attacks on RFID tag standard ISO 14443.
- Overview of existing RFID solutions. This topic includes solutions for authentication (chapter 5), lightweight cryptography primitives (chapter 6), distance bounding (chapter 7), and scalable solutions to attain privacy (in particular solutions for full-synchronisation and delegation) in chapter 10. An overview of more expensive asymmetric security is given in chapter 9, and chapter 11 describes threat modelling in EPC-based information sharing networks.
- Architecture solutions for RFID. Here I include the solutions which enrich RFID security more generally than at the level of the protocol. In this category we have solutions that improve the reliability of RFID reading (chapter 1) and that increase security by means of using PUFs (chapter 4).

- Solutions for expensive tags. These solutions include expensive primitives such as asymmetric encryption and ECC cryptography. In this class, I include chapters 11 (describing access control in an RFID setting) and 13 (presenting an application of RFID to the distribution of media content, mainly DVDs).

② Part *II*, Wireless Sensor Networks contains 8 papers, which I would classify as follows:

- An overview. Chapter 14 gives a general overview of Sensor Networks and its main security challenges.
- Security solutions. There are four main topics of security which this section elaborates on: intrusion detection (chapter 15), malicious node detection (chapter 17), key establishment (chapter 16), and authentication (chapters 20 and 21). The last topic contains two flavours, namely message authentication and authentication in Ad Hoc Networks.
- Security breaches. Finally, this part includes two types of attacks, namely signal jamming (chapter 18) and concealed data aggregation (chapter 19).

③ Part *III* describes topics which are of interest in both RFID and sensor networks, including an overview of security threats in both systems (chapter 22), a description of finite field arithmetic in resource-constrained environments (chapter 23), and a description of how to design secure wireless embedded systems, with reference to both RFID and Sensor Networks.

2 What is the book like (style)?

As previously noted, this book is in fact a disjoint collection of papers. There is no formal introduction, nor any connections between the separate chapters. The style is the usual style of scientific writing, and each chapter includes an extensive bibliography. The chosen topics are interesting and well put-together, giving a good overview of the security notions that are the most relevant in RFID and sensor networks. The general tendency of these papers is inclined more towards implementation and feasibility, and thus the presented topics refer mostly to improvements that are scalable and implementable. On the other hand, topics such as extended definitions and security/privacy models are only referred to in the bibliographies of several chapters. The new notion of pseudonymization due to Visconti et al. also does not appear in this book.

On the other hand, this book serves as a great overview, both for those who are only vaguely familiar with RFID and/or sensor networks, and for those who have spent some time researching either (or both) of the two areas. Each chapter is written in some detail and most constructions also present implementation results. Of the overview chapters, I found chapter 10 the most interesting, as it actually introduces the problem of (re)synchronization between readers and tags as the main challenge in avoiding denial of service (DoS) attacks; throughout this chapter, the authors then give a brief overview of solutions of how to

achieve synchronization. Another very strong point of the book is its diversity, as it covers all the aspects of RFID security and reliability, from the use of multiple tags to distance bounding protocols. The two environments – RFID and sensor networks – are very smoothly bridged, and part III also relates topics that are common to the two.

A disadvantage of this book – and a natural one in my opinion, given the diversity of the topics – is the lack of depth and the somewhat implementation-based approach taken by most chapters. The readers may use this work as a starting point in a deeper research, using also the good amount of bibliographical references that is provided for each chapter, but the book itself does not suffice in trying to obtain a good idea about a specific detail of RFID or sensor network security. I was also surprised to see that very few chapters actually contain any formal definitions or models. Chapter 4 is one of the few chapters introducing some notion of what security is and how it is measured/proved. On the other hand, most other constructions use intuitive notions of security and privacy, which are not standard and which are sometimes not complete.

The general style is concise and to the point. The editors did a great job of putting these chapters together in a more-or-less logical order, and such that the topics share some common ground. There is little or no cross-referencing; on the other hand, the authors tend to use the same style and notations, so that it is easy to follow through from, say, an overview chapter to a constructions' chapter. I particularly liked the good amount of detail regarding RFID hardware and the feasibility of the constructions, as RFID tends to be a domain in which the physical and communications layer cannot be separated from the applications layer. The book also includes clear figures and tables summarising the most important characteristics of the presented topics.

3 Would you recommend this book?

I would certainly recommend this book, particularly to those who are already familiar with theoretical definitions and models related to the cryptographic primitives and security notions that are paramount in RFID and sensor networks. Another possible target group would be those interested in mounting up attacks against RFID systems and sensor networks. It is possible that also adjacent fields such as Ad-Hoc Networks and wireless communications in general may benefit from a brief account of the contents of this book. For all involved audiences, however, it is important to also study of the various references quoted in each chapter, as the authors present only succinctly the topic of other papers or books.

The reviewer is a Ph.D. student at the Center for Advanced Security Research Darmstadt (CASED).