Review of the book

"Networked RFID Systems and Lightweight Cryptography"

by Peter H. Cole, Damith C. Ranasinghe

Springer, 2008

ISBN: 978-3-540-71640-2

Maria Cristina Onete
CASED (TU Darmstadt)

1 What the book is about

This book is a comprehensive guide to networks of Radio Frequency Identification (RFID) based Electronic Product Codes (EPCs) in supply chains, and its topics range from standardised hardware designs through known vulnerabilities, security and privacy models, and to concrete proposals for RFID authentication in various scenarios: machine readable documents, one- and two-way authentication in supply chains, and the pharmaceutical industry. Though a better insight into several discussion points requires additional reading, the book nevertheless provides both a good overview of the general challenges and opportunities in the area of supply chain RFID, and a comprehensive guide to further literature.

The book's eighteen chapters are structured into four parts:

① Part 1 is roughly concerned with the basics of RFID technology, including: hardware designs, standards, an overview of RF technology, and EPCs in perspective (networks of EPCs).

② Part 2 describes security and privacy issues that arise in RFID-based EPC networks, and provides a framework against which solutions may be evaluated; this part also shows several primitives that may be used in RFID authentication.

③ Part 3 crops together a few network based solutions (with the concrete applications of RFID and Near-Field-Communication—NFC—technologies in anti-counterfeiting, and improving the security of the pharmaceutical supply chain) to the problems identified in part 2, and using design notions already specified in part 1. The solutions are presented in a top-down fashion.

④ Part 4 describes—also in a top-down, but structured manner—smaller-scale problems and solutions, specifically: authentication relying on product specific information (this requires the existence of some easily-distinguishable distinctive feature for a product or class of products), authentication with machine-readable documents (such as ID cards, passports, etc.), synchronization-based authentication of Class I Generation 2 RFID, truly random number generators, PUFs, and a solution for lightweight cryptography for low-cost RFID devices.

2 What is the book like (style)?

Written in a fluent, but not overworded fashion, this work represents both a good starting point for students beginning to work in the area of RFID, and a reference for those who are rather more advanced in this field. It is not particularly suitable for the industry, but rather meant for researchers and research groups. It should also be noted that, while several tag standards are considered, the authors focus on the lowest-cost RFID labels on the market; the solutions they propose, therefore, can be improved in terms of efficiency, security, and privacy if the characteristics and limitations of the considered technology improve.

One of the book's best qualities is that it presents several facets of the RFID industry in the same place, thus making it easier for higher-level (for example protocol layer) researchers to understand lower-level (hardware) concepts, or vice versa. Each chapter also provides numerous references for further reading. A particularly good review of previous results is given in chapter 9, which describes several solutions to the challenge of RFID authentication. For those used to research and to what it entails, this book will constitute an ideal starting point towards studying any of the many facets of RFID authentication; further reading of one or several of the referenced papers indicated at the end of each chapter is meant to add further depth to the reader's background.

A disadvantage of this book in my opinion is that it concerns in greater detail cheaper RFID devices, namely those used in supply chains. Though the scenario for example of machine-readable documents is considered, this scenario does not take into consideration the possibility of a greater investment in the RFID hardware development for such documents. This is not so much a fault of the book as a limitation derived from the subject area chosen by the authors. However, for the readers who are interested in a global overview of RFID technology, this book will only provide a single sub-area, and not the entire view. Another downside—which might be addressed perhaps in a second edition of the book—is that it lacks references to the rather important work of Serge Vaudenay, who has modelled privacy for RFID. Additionally, I felt that the denial of service attacks against the YA-TRAP protocol in particular were not very broadly referenced, nor were they mentioned in great detail. In all fairness, however, one must acknowledge the fact that these last two observations rely on relatively new studies and very recent work; hence, it is possible that the book would have already been in the printing press by the time these papers were presented.

The general style is concise and to the point. Each chapter is written as a self-standing paper, but with connecting elements to previous and subsequent chapters. A great effort has gone into synthesizing problems, approaches, and solutions pertaining to RFID systems. The book describes very concisely, for example, the objectives of security and privacy that have been identified by previous literature. In the literature, it is often the case that a single author focuses on a single—or a few closely related—such security objectives. The terminology used by individual authors to express the same concept is often different, and can therefore be confusing. By giving an overview of all security and privacy objectives, fine separations between various objectives can be made, and the literature may then be better put into perspective.

Another very good trait of this book is that it lists some very helpful references to related work. Moreover, the authors try to give—in the text of the chapter—a very succinct overview of what the reader may expect to find in each of the references (they do not simply say: solutions can be found in such and such previous work, but rather: a distance-bounding solution for RFID can be found in such and such work; it has the following advantages and disadvantages).

In everything they do, the authors try to give a full picture of Networked RFID Systems. A very important feature of their style is that they describe hardware and protocol-related security and privacy for RFID, thus allowing the reader to build a structured and complete background. The general view is top-down: a general overview is always given before the authors plunge into details. Even when details are being discussed, this is done in several steps and layers. As an example: when discussing the evaluation framework, the authors first present an overview—a table—containing the criteria they consider important for the evaluation of the security mechanisms pertaining to networked RFID systems. These criteria can be divided in three categories: security, privacy, and cost/performance characteristics. The authors first elaborate on each of these topics, explaining what they consist of and of what significance they may be towards the evaluation of security mechanisms. Only after an overview has been given for each of these criteria are security models presented, and only after the authors are finished explaining the notion of a security model and the particular characteristics of security models in the RFID setting do they show an adversarial model. This top-down style ensures that each sub-layer of knowledge is complete before another one is begun.

3 Would you recommend this book?

I would certainly recommend this book. It provides a great background for those interested in the topic of RFID in general and supply-chain-RFID in particular. A preferred target audience would be researchers in this field, rather than those working in the industry. Further study of the various references quoted in the book is not only recommendable, but necessary, 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).