Review of the book

"RFID Security and Privacy" by Dirk Henrici Springer, 2008

ISBN: 978-3-540-79075-4

Maria Cristina Onete
CASED (TU Darmstadt)

1 What the book is about

This book presents the topic of RFID Security and Privacy in the framework of pervasive computing. Pervasive computing, sometimes known as ubiquitous computing or “ambient intelligence”, is a human-computer interaction model, wherein information processing is integrated in everyday life. The author argues that, as a growing technology, Radio Frequency IDentification (RFID) has many applications which can increase efficiency, comfort, and productivity; however, its technical limitations require solutions that are scalable, flexible, inter-organisational, and durable. The motivation of the author is that the already-existent, negligent solutions compromise security and privacy.

Henrici’s thorough treatment of the topics of RFID security and privacy provides a good foundation for research in this area, a suitable guide into further literature, and raises awareness into the difficulties of first modelling the desired degrees of privacy and security, and then achieving them in useful constructions. These concepts are also analysed from the point of view of implementation and practicality, each chapter containing a detailed perspective into real aspects of RFID security and privacy. However, the structure of the book is not suitable for readers looking for a brief overview in RFID technology, and some degree of academic understanding and intuition are required in order to handle the density of the material.

The book contains seven chapters, which are structured as follows:

- Motivation and Vision. This chapter explains the framework of pervasive computing and describes RFID as a growing technology with great potential in the improvement of the quality of life, a potential which may be difficult to achieve if security and privacy notions are ignored. The author also details possible improvements and applications for RFID.
- Fundamentals. This chapter focuses on the notion of privacy. The author first describes RFID technology, outlining the specific properties and possible consequences of hardware constraints on tags, readers, and the

communication between them. Though the chapter is meant to focus on privacy, the more thoroughly explored topic is that of RFID properties. The author outlines what is generally understood by “security” in the context of RFID, and gives useful ISO definitions of confidentiality, integrity, and availability. He places these definitions in the perspective of practicality and outlines useful properties for practical implementations. Though he gives a thorough motivation of what is generally understood by “privacy”, Henrici does not give in this chapter any technical details of how this is modelled, nor of how it is achieved.

- Analysis and Modelling. This chapter gives concrete, motivated goals for RFID systems and derives challenges for this technology. Henrici also presents an attack model against RFID, describing adversaries from the point of view of their involvement in the RFID communication. There are seven main adversaries, three of which are also reinforced so that their attacks may go both ways, interacting with the reader AND the tags. A significant benefit of this approach is that the author also includes side-channel attacks and practical considerations (such as tag availability) in his models. Relationships are also given between the various models. A very useful analysis of a particular design of tags, i.e. EPC Gen II Tags, shows various approaches that are already in use in RFID technology, their advantages and disadvantages.

- Security and Privacy. This chapter is mainly concerned with security and location privacy. Henrici outlines various facets of security, such as: maintaining data security, denial of service resistance, counterfeiting prevention, illegitimate access prevention, and prevention of unwanted recognition and tracking (this last property requiring also the notion of indistinguishability). An overview of RFID tag functionalities is followed by a discussion of identification and authentication.

- Pseudonymization. One of the most problematic issues in RFID systems is scalability for larger infrastructures of readers and tags. In particular, meeting both (location) privacy and scalability requirements seems to be a nearly unsolvable problem if resources and costs are to be taken into account. Henrici explains the topic of scalability in general, and then applies it to the case of a widespread RFID infrastructure. His proposed solution relies on the tag’s use of so-called pseudonyms: ideally one-time external IDs, which are updated according to the specifications of the manufacturer of each tag. It should be noted that Henrici refers here to a wide RFID infrastructure, containing several manufacturers; he begins by outlining an asymmetric solution — which, though impractical in the context of RFID, provides a good framework for the topic of scalable pseudonymization. His subsequent solutions are hash-based and can be thus applicable to RFID. Both solutions rely on the concept of shared trust, though some entities are more trusted than others. I would recommend the interested reader to also consult the novel work of Visconti et al., which has appeared after the publication of this book.

- Extending the RFID System Model. This chapter presents global RFID systems, stressing the difficulties that arise in an inter-organisational and truly open RFID infrastructure, specifically with respect to sharing symmetric data and allowing for different levels of trust in the interaction between legitimate entities and tags. Henrici shows the insufficiencies of the classical RFID model in which trust is either set to 1 or to 0: trusted or untrusted, and argues for full trust to be shared between the current tag bearer and the tag owner. Furthermore, detailed user policies, managed by a personal manager, will decide whether an entity is considered to be trusted with respect to a data request from the RFID tag or not. The key points in the extension of the model are: the addition of the tag bearer as a key entity in the system; the definition and use of a personal manager; and the so-called push principle, which assumes all readers to be untrusted and nevertheless ensures tag data transfer to legitimate querying identities. The architecture proposed by Henrici uses a pseudonymization infrastructure in order to ensure that no sensitive information is given to the reader; the author also explains several disadvantages of the architecture, such as the high trust placed in personal managers, and also suggests ways to make personal managers as little cumbersome as possible particularly for tag bearers.

- Current Research. The final chapter of this book attempts to translate the theoretical concepts and models presented in the previous chapters into a concrete, practically implementable so-called ID-Zone Architecture. This architecture combines the pseudonymization strategy of the previous section with a structured, zone-based identifier update. In particular, the threat model is adjusted to identify areas where updates are necessary, and areas where the identifiers need not be changed on a regular basis. This chapter also describes useful tools, such as the use of triggered hash chains and of pre-computed challenge-response pairs which can be based on PUFs.

2 What is the book like (style)?

Written in a dense style, which requires careful digestion and analysis, this book presents a novel and very useful picture of an outspread RFID system with many tag owners and tags, interacting in a standardised infrastructure. This represents a good frame of reference for designers of RFID architectures and a starting point towards understanding the challenges related to optimising the process of authentication with RFID. The chapters are long and dense, and there is a strong inter-dependence, which does not allow readers to skip to and fro between them. The style is very formal, although the sections do not represent self-contained papers. The approach is top-down, and a motivation is given before the challenges in each of the seven topics is outlined. The solutions build on each other and are evaluated against the framework that is established in that chapter. Moreover, each construction and each chapter end with a succinct summary, outlining the topic at hand.

One of the best traits of this book is that it builds an intuition into the reader by analysing various solutions to the presented problems and explaining the shortcomings and advantages of each. Intermediate building blocks and solutions are also presented, thus providing the reader with a deeper understanding of how various issues of RFID authentication may be addressed. The author gives a thorough documentation both of implementation- and protocol-related literature, and of RFID security and privacy models. His style is persuasive, as he identifies real problems that appear in a large-scale RFID system implementation, and he clearly distinguishes between ideal security and privacy and realistic security and privacy. The constructions showed in this book are complete in the sense that they satisfactorily answer the challenges presented in each chapter.

It is notable, however, that while Henrici classifies adversaries depending on their attack abilities, he does not give formal definitions, nor proofs of security for any of his constructions. One important drawback, in my opinion, is that no complexity analysis is given for the large-scale models presented throughout the book: considering that RFID tags are resource-constrained devices, such an analysis is paramount. Another point where this book may be improved is in my opinion the content of the illustrations. While Henrici very well depicts and outlines the main architectural points of his constructions, more concrete illustrations of the protocols he suggests would be useful. I missed the works of Serge Vaudenay amongst the references of this book, particularly from the point of view of privacy and security models. Amongst useful references for a second edition of this book, I would mention Visconti's work.

3 Would you recommend this book?

I would strongly recommend this book to anyone interested in an in-depth study of the potential uses and constraints of large-scale RFID authentication. Although the style is dense and the inter-dependency between the chapters makes this work unsuitable in obtaining a general overview of the topic of RFID, the book is a thorough study of the most important challenges related to this subject. Not only does it present constructions which may be valuable in practice, but it also builds a strong intuition related to the main issues in security, privacy, performance, reliability, and scalability of large-scale RFID infrastructures. A preferred target would be academic researchers in this field, although the practical considerations included in this work may interest industry research labs as well.

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