Lecture Notes Electrical Engineering

Volume 17

Dirk Henrici

RFID Security and Privacy

Concepts, Protocols, and Architectures

Springer

Dr. Dirk Henrici
University of Kaiserslautern
67653 Kaiserslautern
Germany
henrici@informatik.uni-kl.de

ISBN: 978-3-540-79075-4 e-ISBN: 978-3-540-79076-1

Library of Congress Control Number: 2008924615

Cover design: eStudio Calamar S.L.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Dedicated to all dear people
accompanying me on the journey of life

Preface

In the beginning of 2003, I found a short article about the privacy implications of RFID technology in a newspaper. It raised my interest, and after reading some early research papers on the topic, I thought: "There must exist better solutions." I concerned myself with the topic in my spare time. After having developed my first solutions, I asked my supervisor, Prof. Dr. Paul Müller, whether I could write a paper about my results. As the topic did not fit into any running project or at least the overall research directions of his group, he could have answered no. But instead, he encouraged me to do it. The paper became a success, and many other papers about new concepts and solutions followed. Now the answer is obvious: There exist better solutions.

I have dealt with the topic over the past years. Now I want to share the basics as well as current research results with the reader. This book is surely not a bedside reading. But with all the presented concepts, it can broaden the mind of the reader concerning security, privacy, and RFID systems. I wish the reader many new insights.

There are many people I would like to thank. First of all, my thanks go to my supervisor, Prof. Dr. Paul Müller. He gave me room for creativity and plenty of rope to work on my own. Thereby, he always trusted in my skills, gave helpful hints, and his door stood open for me at all times. He also suggested the publication of this book. Thanks also go to various persons that supported me in finishing this work. As representatives for all of them, I'd like to mention Prof. Dr. Friedemann Mattern for spending his rare available time on rating my research and encouraging me to go on working, Prof. Dr. Karsten Berns for the valuable discussion about his experiences, and Dr. habil. Bernd Schürmann for answering all my legal and administrative questions. I also want to thank the Springer publishing company for the pleasant cooperation and for publishing this book.

Many thanks go to my present and former colleagues for the pleasant and productive atmosphere as well as the lively discussions on scientific and other topics. I am glad that we had so much fun despite of the high workload. I also want to thank our courteous secretaries who disburden us from much administrative work.

My thanks also go to my friends, Michaela Keßler, Sascha Paulus, Nadine Sumser, and the many others, for their long lasting friendship and their understanding that I was not as available as usual in the recent months.

I am deeply grateful to my parents, Doris and Franz-Josef Henrici, for their enduring support and all the other gifts that I received from them. I thank my sister Carina for distracting me from my work every now and then and for always giving me a hearty welcome each time I visited her.

Very special thanks go to Annika Kohlhaas for her love and patience. She did not only show understanding for all the evenings and weekends that I spent sitting in front of my notebook but also did the proofreading of papers and this book. She is very special, and I am glad that she came into my life.

Kaiserslautern, February 2008 *Dirk Henrici*

Contents

Outline

In the first chapter, the topic of this book is classified into the area of pervasive computing. Further, security and privacy in the scope of RFID technology is motivated and the vision that guides the remainder of this book is introduced.

Chapter 2 begins with an overview of RFID technology. It gives required background information for understanding RFID system components, their interplay, and their relevant characteristics. After a short subchapter regarding security, the core topic of the chapter is addressed: privacy. An introduction to privacy with respect to RFID systems is given with the goal to derive design guidelines. The chapter closes with an introduction to important cryptographic primitives. The focus is laid on one-way hash functions and random number generation since these are the most important primitives within this book.

The successive chapter 3 introduces into the security and privacy issues regarding RFID systems. After motivating the topic using some examples, the variety of threats that the systems is exposed to is identified. Based on these threats, goals for secure and privacy-respecting RFID systems are derived. Reaching these goals has many challenges, which are presented in the next subchapter. Afterwards, security and privacy in RFID systems is considered from an attacker's point of view: Classes of attacker capabilities are introduced and possible attacks on RFID systems presented. The chapter concludes with a presentation and an assessment of the current situation in today's application of RFID.

In chapter 4, concepts for addressing the identified issues are presented. Following the current state-of-the-art in the literature, the presentation focuses on securing the communication between RFID tags and readers and on protecting location privacy despite eavesdropped or unauthorized tag queries. The different concepts are presented along a scheme for classification. As a comprehensive example of an RFID protocol that implements all tasks that are required for secure, privacy respecting RFID systems, the "Hash-based ID variation" protocol is presented and discussed. An evaluation of this protocol is performed based on evaluation criteria that have been proposed before in this chapter.

Chapter 5 addresses a deficiency that has been found in RFID protocols that implement identifier modification based on message exchanges: For these protocols to operate, a central entity is required which limits scalability of the approaches. The problem is addressed using "pseudonymization infrastructures" that enable the building of distributed, inter-organizational systems that have the required security and privacy properties. After motivating the use of such infrastructures in RFID systems, the use of classic concepts for pseudonymization infrastructures in RFID systems is presented. Afterwards, pseudonymization infrastructures based on hash functions as cryptographic primitives are developed.

In chapter 6, the necessity to extend the classic RFID system model that is presumed in current RFID literature and that is also used in chapter 4 is explained. After a discussion of the deficiencies of the classic model, that model is extended step by step: First, readers are regarded as untrusted entities. This leads to a push concept. RFID systems using this new model adhere much better to the practical requirements in inter-organizational systems than ones using the classic model. In a second step, the tag bearer is introduced as separate entity and the concept of a "personal manager" for managing tagged items is presented. The chapter concludes with an evaluation of the complete architecture with the presented protocols and concepts as building blocks.

As the result are RFID systems that fulfill the requirements regarding security and privacy perfectly but that cannot be implemented economically, chapter 7 aims at more practical solutions and presents current research results. At first, a more elegant replacement for the "Hash-based ID variation" protocol is considered. It is called "Triggered hash chain" protocol. Second, a partial solution for securing supply-chains against counterfeited products is presented. The main part of the chapter is the development of the "ID-Zone architecture". It is an RFID system architecture that follows the practical requirements identified in chapter 2 instead of providing privacy in a perfect manner. In return, the architecture can be implemented much more economically. The chapter closes with some research directions.