MORGAN & CLAYPOOL PUBLISHERS

RFID Security and Privacy

Yingjiu Li
Robert H. Deng
Elisa Bertino

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, AND TRUST

Elisa Bertino & Ravi Sandhu, *Series Editors*

RFID Security and Privacy

RFID Security and Privacy

Yingjiu Li, Robert H. Deng, and Elisa Bertino

www.morganclaypool.com

ISBN: 9781627053259 paperback
ISBN: 9781627053266 ebook

DOI 10.2200/S00550ED1V01Y201311SPT007

A Publication in the Morgan & Claypool Publishers series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #7
Series Editors: Elisa Bertino, *Purdue University*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Synthesis Lectures on Information Security, Privacy, & Trust
Print 1945-9742 Electronic 1945-9750

Synthesis Lectures on Information Security, Privacy, & Trust

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

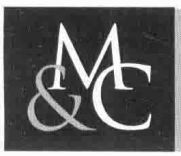
RFID Security and Privacy

Yingjiu Li
Singapore Management University

Robert H. Deng
Singapore Management University

Elisa Bertino
Purdue University

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #7



MORGAN & CLAYPOOL PUBLISHERS

ABSTRACT

As a fast-evolving new area, RFID security and privacy has quickly grown from a hungry infant to an energetic teenager during recent years. Much of the exciting development in this area is summarized in this book with rigorous analyses and insightful comments. In particular, a systematic overview on RFID security and privacy is provided at both the physical and network level. At the physical level, RFID security means that RFID devices should be identified with assurance in the presence of attacks, while RFID privacy requires that RFID devices should be identified without disclosure of any valuable information about the devices. At the network level, RFID security means that RFID information should be shared with authorized parties only, while RFID privacy further requires that RFID information should be shared without disclosure of valuable RFID information to any honest-but-curious server which coordinates information sharing. Not only does this book summarize the past, but it also provides new research results, especially at the network level. Several future directions are envisioned to be promising for advancing the research in this area.

KEYWORDS

RFID technology, RFID system, RFID security, RFID privacy, authentication, access control, EPCglobal Network

Preface

The purpose of this book is to provide a systematic overview on RFID security and privacy which has been rigorously researched over the past decade. A unique feature of this book is that it organizes all material in two dimensions: (i) RFID security and privacy at (ii) physical and network levels. Consequently, the following chapters are covered in this book.

- **Chapter 1: Introduction.** This chapter provides background knowledge about RFID technology as well as the two dimensions by which we organize this book. In one dimension, RFID technology at the physical level is used to identify physical objects with RFID devices, and RFID technology at the network level is used to share RFID information among networked parties. In another dimension, security means that authorized entities can operate correctly in the presence of attacks, and privacy implies that an adversary cannot obtain any unauthorized information from its attacks.

- **Chapter 2: RFID Security at the Physical Level.** The major concern in this chapter is how to identify RFID devices correctly in the presence of attacks. This concern is addressed in RFID tag/reader/mutual authentication, key distribution, path authentication, and clone tag detection. RFID tag/reader/mutual authentication requires that only valid tags or/and valid readers are accepted under certain adversary models. Since most RFID authentication solutions rely on secret keys which are shared between tags and readers, the key distribution problem should be addressed which deals with how to distribute necessary keys to readers in a secure and timely manner. Another security issue at the physical level is path authentication, which accepts only those valid tags that have passed through valid paths. Finally, clone tag detection is used to identify possible clone tags which bear the same IDs as genuine tags in an RFID system.

- **Chapter 3: RFID Privacy at the Physical Level.** RFID privacy at the physical level requires that RFID devices should be identified without disclosure of any valuable information about the devices. While fixed pseudonyms may be used to prevent an adversary from knowing real tag IDs, it is more challenging to ensure that an adversary cannot trace the movement of any target tag from RFID communications. Various privacy notions are defined, analyzed, and compared in a single-reader system, including indistinguishability based privacy (an adversary cannot distinguish between two uncorrupted tags), unpredictability based privacy (an adversary cannot distinguish protocol messages from random numbers), zero knowledge-based privacy (whatever information an adversary can obtain from interacting with a target tag can be derived by any simulator without interacting with the target tag), Vaudenay's privacy framework with eight types of adversaries, and universal composibility-based privacy

framework. In addition, various privacy notions are investigated in a multi-reader system, including tag unlinkability, step unlinkability, and path privacy in path authentication, as well as old owner's privacy and new owner's privacy in ownership transfer.

- **Chapter 4: RFID Security at the Network Level.** RFID security at the network level requires that RFID information should be shared with authorized parties only. In EPCglobal Network, which is a standard architecture for sharing RFID information, a new type of access control (namely List-Chain-BAC) policies is defined for each EPCIS to specify who can access its event data in EPCIS and who can query its event indexing data in EPCDS. A unique feature of such access control policies is that they are defined based on partner relationship with respect to certain RFID tags. This chapter also presents efficient new algorithms for (i) EPCDS to enforce all policies defined by participating EPCISes and (ii) EPCIS to enforce its policy when its event data are queried by users.

- **Chapter 5: RFID Privacy at the Network Level.** At the network level, RFID privacy requires that RFID information should be shared without disclosure of valuable information to any honest-but-curious server which coordinates information sharing. In EPCglobal Network, it is crucial to protect the information registered by each EPCIS at EPCDS if EPCDS is not fully trusted. This chapter discusses how to achieve anonymity of tag ID and anti-tracing of tag ID in EPCDS.

- **Chapter 6: Summary and Future Directions.** After summarizing the major content of this book, this chapter provides a list of promising directions for advancing the research in RFID security and privacy.

FOCUS AND AUDIENCE OF THIS BOOK

In this book, we focus on providing a big picture with easy-to-understand descriptions and necessary technical details, while leaving out some formal proofs which can be found in the references. This book does not intend to be historical, as the material presented is out of historical order. It is not encyclopedic either, in a sense that some sub-areas are omitted. For example, we do not cover the whole sub-area of hardware design of crypto-tags.

This book is suitable for both academic researchers and RFID practitioners to explore the fast-growing world of RFID security and privacy. Academic researchers may find it useful in identifying interesting research problems, understanding the challenges of solving such problems, and inspiring new ideas from existing solutions. RFID practitioners can find available solutions to address security and privacy challenges in RFID applications, understand the tradeoffs to be made in choosing among various available solutions, and recognize the state of the art in RFID security and privacy research.

The authors welcome any comments and discussions on this book. Since the development in some of the research areas in RFID security and privacy is still in an early stage, more interesting material would be added in possible future editions of this book.

Yingjiu Li, Robert H. Deng, and Elisa Bertino
December 2013

Acknowledgments

The authors would like to thank their collaborators, postdocs, and students, especially Dr. Tieyan Li, Professor Yunlei Zhao, Professor Changshe Ma, Dr. Eng Wah Lee, Wei He, Dr. Guilin Wang, Dr. Junzhuo Lai, Dr. Kuo-Hui Yeh, Dr. Kevin Chiew, Dr. Chunhua Su, Dr. Jie Shi, Dr. Qiang Yan, Dr. Zhongyang Zhang, Hongbing Wang, Shaoying Cai, Su Mon Kywe, Bing Liang, and Ge Fu for their valuable contributions in research on RFID security and privacy.

The authors are also grateful to Diane D. Cerra and her colleagues at Morgan & Claypool Publishers for their help and support in preparing this book for publication.

Yingjiu Li, Robert H. Deng, and Elisa Bertino
December 2013

Contents

CHAPTER 1

Introduction

1.1 RFID TECHNOLOGY

Radio-Frequency IDentification (RFID) is a technology for an automated identification of objects using radio waves. RFID technology is widely envisioned to replace barcode technology in the near future. Currently, RFID technology has been increasingly diffused in many applications and industries, including supply chain management, manufacturing, logistics, supermarket, pharmaceutical, hospital, library, airport, transportation, passport, bank notes, smartphone, payment, asset management, and many more. In an emerging world of *Internet of Things (IoT)*, RFID technology enables almost everything in the real world to be connected to a virtual cyber world so that people can interact with the things remotely and conveniently. In this sense, RFID technology would revolutionize network and IT technology, improve productivity, and change human life significantly.

RFID technology can be investigated and applied at both the physical and network levels. *RFID technology at a physical level* is mainly used to identify physical objects with RFID devices, while *RFID technology at a network level* is mainly used to share the RFID related information among networked parties.

1.2 RFID TECHNOLOGY AT THE PHYSICAL LEVEL

At the physical level, RFID technology is used to identify physical objects with RFID devices. A particular universal identifier for physical objects is *electronic product code (EPC)*. EPC Tag Data Standard [1] includes various coding schemes such as General Identifier (GID), a serialized version of the GS1 Global Trade Item Number (GTIN), GS1 Serial Shipping Container Code (SSCC), GS1 Global Location Number (GLN), GS1 Global Returnable Asset Identifier (GRAI), GS1, Global Individual Asset Identifier (GIAI), DOD Construct, Global Service Relation Number (GSRN), and Global Document Type Identifier (GDTI). In particular, an EPC consists of a header (8 bits), an EPC manager (28 bits), an object class (24 bits), and a serial number (36 bits), which is illustrated in Fig. 1.1. To be specific, we introduce EPC as a typical case of physical object identifiers in this book, though any other physical object identifiers can be used in practice.

Physical objects can be identified using unique IDs such as EPC numbers in an *RFID system*. An RFID system typically consists of a set of RFID tags and RFID readers, as well as a back-end server. RFID tags, usually attached to or embedded in physical objects, are small RFID devices, which can be used to store physical object IDs (e.g., EPC numbers) and related

Header	EPC Manager	Object Class	Serial Number
8 bits	28 bits	24 bits	36 bits

Figure 1.1: EPC code structure.

information. RFID readers are more powerful RFID devices which interact with nearby RFID tags via a wireless radio wave channel, and interact with a back-end server via the traditional network connections (e.g., bluetooth, LAN, or internet). An *RFID communication protocol* is executed by an RFID reader, its nearby tags, and a back-end server so as to identify the IDs associated with the tags and to obtain more information about corresponding physical objects.

RFID technology is different from a traditional barcode technology in the following aspects. First, an RFID reader can interact with multiple RFID tags automatically and speedily (certain RFID tags can be read at a speed of 1000 tags per second), while a barcode reader must scan barcodes one by one manually. Second, an RFID reader can interact with RFID tags at a distance (which may range from several centimeters to over 100 meters) without a line of sight, while a barcode must be scanned with a line of sight in close proximity. Third, compared to a barcode, an RFID tag can store much more information regarding physical objects such as ID and access password. Lastly, the information stored in an RFID tag can be updated easily while the information contained in a barcode is static. With all these differences, RFID technology has triggered tremendous interests in replacing a barcode technology and developing numerous innovative applications.

RFID tags can be active, passive, or battery-assisted passive. An active tag has a battery on board and it can transmit electronic signals periodically. A passive tag has no battery, which harvests power from the electronic signals of nearby RFID readers. A battery-assisted passive tag has a small battery on board but it is activated only when receiving signals of nearby RFID readers.

The electronic signals between RFID readers and tags may operate in different frequency bands, such as standard near field communication (NFC) band 13.56 MHz (HF), and standard EPC Gen 2 band 860-960 MHz (UHF). Usually, the higher the frequency, the longer the operating distance between RFID reader and RFID tag, and the higher the data transmission rate. NFC may operate in a range of centimeters, while EPC Gen 2 in a range of meters.

The nominal distances specified in RFID standards represent the maximal distances at which a normal reader can reliably interact with a tag. An adversary equipped with sensitive readers may interact with a tag from a distance longer than the nominal distance. In addition, an adversary may eavesdrop on existing tag-to-reader communications and reader-to-tag communications at increasingly longer distances.

A major concern in RFID applications is the cost of RFID tags, especially in a large-scale deployment. Passive tags may cost a few U.S. cents each, while battery-assisted tags and active tags are more expensive, at a cost of a few U.S. dollars or even higher. With the Moore's Law, the

cost of RFID tags drops fast. A wide adoption of RFID technology is unstoppable when the cost is low enough as compared to the various benefits it brings in.

Several organizations, including EPCglobal and ISO, have set up standards for RFID technology. In particular, EPCglobal, a joint venture between GS1 and GS1 US, leads the development of industry wide global standards for the use of mostly passive RFID tags and EPC in today's global trading networks. It defines a UHF Class 1 Generation 2 (EPC Gen 2) air interface for communication between RFID reader and EPC Gen 2 tags [2]. EPC Gen 2 tags are widely adopted low-cost passive tags with a memory structure illustrated in Fig. 1.2. An EPC Gen 2 tag consists four memory banks, including 96 bit EPC number, 32-64 bit tag identifier (TID) indicating the manufacturer of the tag, 64 bit reserved bank consisting of 32 bit kill password and 32 bit access password, and a user memory bank which may vary from 0–2048 bits or even more depending on the manufacturer. EPC Gen 2 tags can be read at a speed of 1000 tags per second and written at 7 tags per second given correct access passwords. EPC Gen 2 tags support on-chip Cyclic Redundancy Code (CRC) computation, 16-bit Pseudo-Random Number Generator (PRNG), and other lightweight operations such as XOR, MOD, and string concatenation.

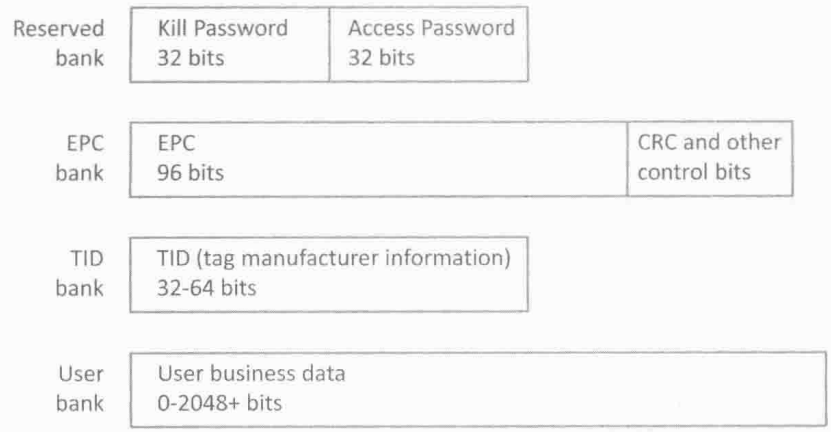


Figure 1.2: EPC Gen2 tag memory structure.

1.3 RFID TECHNOLOGY AT THE NETWORK LEVEL

At the network level, RFID technology is used to share RFID information among networked parties. EPCglobal Network is a standard architecture of computer networks created by EPCglobal for sharing RFID information. Fig. 1.3 illustrates the architecture of EPCglobal Network [3], which consists of the following components: EPC Information Services (EPCIS), EPC Discovery Services (EPCDS), and Object Naming Services (ONS).

EPCIS is essentially a database management system which is used by a networked party to manage its own RFID-related information in a repository and share with other parties via a

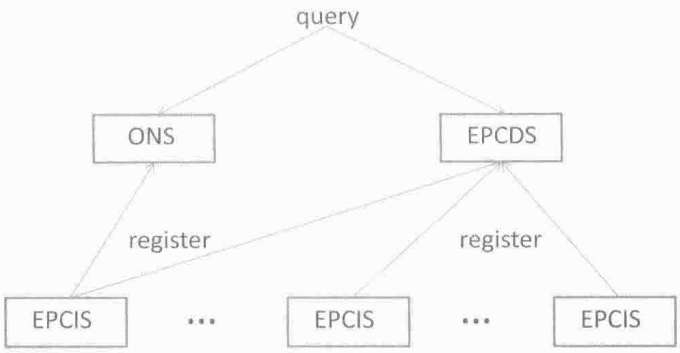


Figure 1.3: EPCglobal network architecture.

query interface. The RFID-related information is called RFID events in EPCglobal Network, which consist of EPC numbers and application information such as time, location, and business step for processing the physical objects indexed by the EPC numbers.

EPCDS is designed to discover all EPCIS systems which hold events about certain EPC. It can be compared to a search engine in the Internet which returns a series of URL links given a keyword. EPCDS enables networked parties to discover physical objects and to share RFID events about the objects.

ONS is a simplified version of EPCDS. Given an EPC, ONS returns the address of a single party which originally assigns the EPC code. In comparison, EPCDS returns the pointers to all parties which hold event information about an EPC. ONS can be compared to DNS in the Internet which translates URL names to IP addresses. Since ONS is a simplified version of EPCDS, we focus on EPCDS instead of ONS in this book.

1.4 RFID SECURITY AND PRIVACY

We address the security and privacy issues in RFID technology at both the physical and network levels. Roughly speaking, security means authorized entities can operate correctly in the presence of attacks, while privacy implies that an adversary cannot obtain any un-authorized information from its attacks. At the physical level, an authorized entity, which could be RFID reader, RFID tag, or backend server, operates according to an RFID communication protocol for the purpose of identifying physical objects. At the network level, an authorized entity, which could be any networked party, makes queries to EPCDS and EPCISes for the purpose of sharing RFID information.

Considering that RFID technology may be used in a hostile and competitive environment, the security and privacy issues in RFID technology should be addressed appropriately in the presence of attacks such as industry espionage and hacking. Various *adversary models* can be used to model an adversary's capability of launching attacks. An adversary may control the communi-