Radio-Frequency IDentification (RFID) devices and systems are fast becoming a ubiquitous tool in automatic identification technologies due to their relatively low cost and ease of deployment. These systems are made of three main components, tags, readers, and back-end servers. Common tags have a very simple circuitry, and do not have their own power sources. Tags receive their power through inductive coupling, electromagnetic backscatter and close coupling with readers, and typically engage in authentication and transfer of information once they are powered by any nearby reader. As increasing numbers of RFID devices are used in logistics, consumer applications, and business specific applications, security and user privacy concerns are becoming ever more important. However, the general architecture of these systems and the make-up of their components, in particular resource constrained tags, pose considerable challenges in designing secure, privacy-preserving algorithms for these systems. Any possible solution not only has to be able to counter attacks against any typical computer systems, but also has to be able to address the unique vulnerabilities due to the use and set up of these systems. Any solution must also be extremely efficient and scalable.

This book attempts to bring together comprehensive coverage of security and privacy issues related to RFID systems from the formal definitions and standards used, to security modelling of existing threats and vulnerabilities, while detailing both general and specific solutions and countermeasures to these threats. Each chapter was contributed by expert authors in the field, and best attempts were made to make each chapter self contained. The book also contains all the required background information, and it is meant not only to be of value to those researchers who work in the security domain, but also to be accessible to those researchers and practitioners without any prior background in security and privacy technologies. This book is comprised of four major sections: Background and Preliminaries, Attacks, Existing Solutions and Privacy. Below, you will find a brief description of each chapter in each part, which can also be used as a map of how this book can be read.

SECTION 1: BACKGROUND AND PRELIMINARIES

Devising and implementation of cryptographic algorithms and protocols suitable for RFID systems represent a challenging area of research. This book has two chapters dedicated to covering fundamental cryptographic concepts and notions used in the remainder of the book and in the area as a whole. In the first chapter, titled “Security Terminology” by Li, basic definitions of security service requirements, notions of symmetric and public key cryptosystems, and those of computational security versus information theoretical security are described. This chapter is intended for researchers and practitioners without any background in security, and introduces them to the general necessary concepts and terminology without focusing on any specific algorithms or cryptosystems.
Standards are an essential part of today’s modern manufacturing methods and they regulate product characteristics such as quality, reliability, and safety for consumers. They also enable inter-operability among the same kind of products from different manufacturers and increase competition by providing a wider market share for higher quality and better priced products. In the second chapter, titled “RFID Standards,” Ilker et al. provide an overview of the RFID standardization bodies and their standards. The chapter includes a categorization of RFID systems and describes their operating principles from the standard’s perspective.

SECTION 2: ATTACKS

RFIDs use wireless media, so all of the threats associated with wireless media usage exist in RFID systems. RFID systems are further challenged by these threats because of the tags’ limited hardware and energy capacity for implementing robust security measures. The chapter titled “RFID Wireless Link Threats” by Ilker et al. discusses various different types of attacks that can be launched against low-end, mid-range and high-end RFID systems. These attacks include eavesdropping attacks, tampering, session hijacking, relay and replay attacks. Countermeasures against these types of attacks are also discussed.

Hardware attacks represent another class of important security threats to RFID systems, as they target architecture and the operations of the working components of these systems. Chapter four, “Hardware Attacks” by Kong et al. gives a survey of various kinds of hardware attacks and their countermeasures. Attacks discussed include cloning attacks, direct read attacks, and side channel attacks including power and timing analysis attacks.

Attacks on RFID systems can target different components and layers. In the chapter titled “Computer System Attacks,” Ning gives a detailed account of some of these attacks on tags and readers in middleware, back-end systems, and wired links. These include buffer overflows, data flooding and spurious data, propagation of viruses and worms, application layer attacks and those on Object Naming Services, and network protocol attacks. Different countermeasures proposed in the literature to combat these attacks are also discussed.

SECTION 3: EXISTING SOLUTIONS

Chapter six, titled “An Overview of Cryptography,” by Vahedi et al., discusses some of the related number theoretic preliminaries; details some of key algorithms such as AES, RSA, and Elliptic Curve Cryptography; as well as hash functions, digital signature algorithms and identification and authentication protocols. The chapter concludes by highlighting some of the challenges in designing lightweight cryptographic techniques suitable for RFID applications.

Remote identification is one of the main tasks for RFID tags, and secure, practical authentication schemes represent the first line of defence against (wireless) attacks on RFID systems. In the seventh chapter, titled “Identification and Authentication for RFID Systems,” Malek et al. first discuss the physical characteristics of typical RFID systems such as reading range, memory, and timing and their impact on any practical authentication scheme. The chapter also discusses different types of attacks such as eavesdropping, relay and replay attacks, and tampering against two general types of authentication that may be required: unilateral and mutual authentication. The chapter then gives a detailed treatment...
of both symmetric authentication solutions such as MAC/hash- and AES-based protocols, as well as asymmetric ones such as RabinXs, NTRU and ECC. The chapter concludes by providing coverage of some specially designed authentication schemes such as HB and HB# and non-cryptographic solutions.

SECTION 4: PRIVACY

In typical RFID systems, tags have unique identifiers that are readable without line-of-sight contact. Although this is one the key features that makes these systems usable in many different types of applications, it also can lead to serious breaches of privacy as it creates the possibility of user information leakage and location tracking. In the chapter titled “Privacy Issues in RFID,” Song describes in detail some of the privacy requirements in terms of tag information and location, and introduces the Avoine, the Juels-Weis, and the Vaudenay formal models that have been proposed to study and measure privacy of these systems.

A common technique for dealing with privacy issues discussed in Chapter Eight is to use pseudonyms for RFID tags instead of their true identifiers. This technique, however, can pose challenges for readers and back-end servers trying to identify and authenticate tags in the system. Malicious attackers can also exploit such a set up in many of current protocols by exhausting back-end servers’ computational resources. In Chapter nine, titled “DoS Attacks on RFID Systems: Privacy vs. Performance,” Duc et al. highlight the key issues with regard to these type of Denial-of-Service (DoS) attacks, and discuss the DoS vulnerabilities of several privacy-preserving RFID authentication protocols including O-FRAP, Ryu-Takagi, and Burmester-Medeiros-Motta protocols. The chapter also includes a proposed countermeasure technique that takes advantage of a two-phase authentication protocol.

The scale and widespread use of RFID systems in various applications pose serious concerns about the effects of malware propagation and the impact on many systems that use RFIDs. The chapter “Malware Protection on RFID-Enabled Supply Chain Management Systems in the EPCglobal Network” by Yan et al. uses RFID-enabled supply chain management systems in the EPCglobal network as a case study to demonstrate the basic characteristics of RFID malware and key issues in RFID malware protection. The chapter introduces a demo security system, RFscreen and shows how it can be used to protect a given system at the tag, the reader and the back-end system layers. Countermeasures used in different phases of malware life cycle are also discussed in detail.

RFID technology plays an important role in automation and optimization of organizations’ supply chains. However, it can enable adversaries to infer both spatial and temporal information about a given supply chain if they can create a covert channel by using tag tracking, tag duplication or modification and possible reader compromises. In the chapter “Addressing Covert Channel Attacks in RFID-Enabled Supply Chains,” Chawla et al. model supply chains as network flow graphs, and introduce taint checking and verification algorithms that can be used as countermeasures against supply chain-based covert channels. Evaluation results based on a case study and other possible mitigating techniques including the use of authentication, pseudonym, re-encryption, and Physically Unclonable Functions (PUFs) are also discussed.

Chapter twelve, titled “Building Scalable, Private RFID Systems,” by Lu, focuses on privacy-preservation for large scale RFID systems. After an overview of some of the existing protocols and highlighting some of their security vulnerabilities or lack of scalability, strong and weak formal security models are defined for this problem and it is argued that strong security models may not be acceptable
for large scale RFID systems due to the lack of authentication efficiency. A weak formal privacy model called Refresh is introduced, which has looser constraints on the output of tags, such as randomization and unpredictability, while allowing RFID systems to achieve acceptable privacy protection as well as highly efficient authentication.

I hope that you find the content of this book beneficial to you, and that it helps all those who are interested and working in this very explosive area to make more secure and private systems.

Ali Miri  
*Ryerson University, Canada*