Chapter XLV
Security and Privacy in RFID Based Wireless Networks

Denis Trček
University of Ljubljana, Slovenia

ABSTRACT

Mass deployment of radio-frequency identification (RFID) technology is now becoming feasible for a wide variety of applications ranging from medical to supply chain and retail environments. Its main draw-back until recently was high production costs, which are now becoming lower and acceptable. But due to inherent constraints of RFID technology (in terms of limited power and computational resources) these devices are the subject of intensive research on how to support and improve increasing demands for security and privacy. This chapter therefore focuses on security and privacy issues by giving a general overview of the field, the principles, the current state of the art, and future trends. An improvement in the field of security and privacy solutions for this kind of wireless communications is described as well.

INTRODUCTION

Radio-frequency identification (RFID) has its roots in WWII when it was used for the first time to distinguish British from German aircrafts. An aircraft was challenged to communicate a certain piece of information and on this basis a decision was made on whether to attack it or not.

This principle is the core of contemporary RFID technology, although, of course, the implementation technology is significantly different. It is now based on low-cost integrated circuits (ICs) called *tags*. Due to the ability to currently store up to two kilobytes of data on these tags, they constitute a very attractive technology in many areas. These include manufacturing, supply chain management, inventory management, healthcare applications, air-transportation, and so forth. All items (in containers) can be scanned together, while each item can be uniquely identified and traced. These properties give RFID technology significant advantages over existing bar-code systems that currently serve for low level, operational acquisition of data in the above mentioned business environments.

These appealing properties also have drawbacks, many of them in the area of security and privacy. But as RFID is already finding its place in contemporary information systems (ISs), these issues need to be addressed seriously, which is the goal of this chapter. In the second section, the background of RFID technology is given. In the third section, threats are described and countermeasures are given. In the fourth section anticipated future trends are discussed. There is a conclusion in the fifth section, while the chapter ends with references and key definitions.

BACKGROUND OVERVIEW

Some definitions have to be given first. One basic definition in the area of computer (communications) security states that security means minimization of vulnerabilities of assets and resources (ISO, 1989). *Wireless security* thus means minimization of vulnerabilities of assets and resources when communicating information in electro-magnetic media through a free-space environment. Finally, *RFID technology* will be defined as wireless identification technology which operates on radio frequencies and deploys low-cost ICs.

A model of RFID environment is described in Figure 1. It consists of *tags* (also called responders) and *readers* (also called transceivers). This is the front-end of RFID applications, which have their back-end in database management systems, where they are integrated with the rest of the IS (see Figure 1). It is generally assumed that RFID security and privacy is concerned with the front-end part (the left-hand side of the dashed vertical line in Figure 1). This is actually the part that is covered by the reader's signal; the tag's signal usually falls within its range.

Tags consist of a microchip and an antenna, both encapsulated in polymer material. The microchip has encoded data, called *identification* (ID), which typically include the manufacturer, brand, model, and serial number. Communication takes place on radio-frequencies, for example, from 125 kHz to 134 kHz for security cards and from 800 MHz to 900 MHz for retail applications (Roussos, 2006). However, increasing the frequency means increased accumulation of signal in bodies containing large quantities of water or in metal.

Communication is achieved by electromagnetic coupling between readers and tags. A reader transmits a signal, which induces a voltage in the tag's antenna. This coupling provides sufficient power

Figure 1. A model of the RFID security and privacy environment