Chapter 85
Identification and Authentication for RFID Systems

Behzad Malek
Ryerson University, Canada

Ali Mir
Ryerson University, Canada

ABSTRACT

In this chapter, the author briefly reviews the various attacks on existing identification and authentication schemes and describes the challenges in their design for RFID systems. The chapter categorizes the RFID identification and authentication schemes into two general categories: cryptographic and non-cryptographic solutions. Cryptographic solutions are based on symmetric or asymmetric cryptography systems. Depending on the resources available on the RFID tags, algorithms based on standard cryptography cannot be utilized in an RFID system and new cryptographic algorithms must be designed. However, there remain security challenges in protecting the RFID systems that cannot be solved solely by relying on cryptographic solutions. The chapter also reviews these challenges and looks at the countermeasures based on non-cryptographic solutions that would further protect RFID systems.

BACKGROUND

Advancements in technology have enabled mass production of cheap, miniaturized RFID transponders (tags) that have become rampant in every application ranging from animal/cargo tracking to labeling items in stores and to payment systems. All types of RFID transponders have non-volatile memory storing the identification data and some additional data. The identification data might be equivalent to a Universal Product Code (UPC) code that uniquely identifies the RFID transponder. Additional data can be stored in the tag to carry more information about a product, such as its description, category, manufacturer, expiry date, price and other useful data. The main task of RFID transponders is to securely transmit data from the memory and to confidently identify a

DOI: 10.4018/978-1-4666-4707-7.ch085

tag. In other words, an RFID scanner (reader) should be able to find the RFID transponder in its reading range and recognize its identity, based on the data transmitted from the tag.

RFID transponders are wirelessly activated and usually scanned without being noticed. Every time an RFID transponder is scanned, it (almost always) responds immediately with the same identification number. The tag receives a specific service, depending on its identity. The service varies greatly from one application to another. It can range from simply matching the identity of the transponder to a price in a retail store to granting entrance access through a secured door in a building.

There are many technical challenges facing the designers and researchers in making a robust RFID system. These challenges are mainly due to the physical constraints of the RFID devices and their limitations on sophisticated measures. In this chapter, we review some of the challenges in choosing an RFID technology and designing a suitable identification mechanism.

IDENTIFICATION IN RFID SYSTEMS

RFID systems communicate via electromagnetic waves and are categorized as radio systems. All radio systems operate in a narrow band to avoid signal interference with other radio systems. Therefore, available frequencies and transmitted power in every radio system, including RFID systems, are heavily regulated. These regulations and restrictions directly affect an RFID system in reading range, memory and the applicable standards. In this section, we briefly review each characteristic.

Reading Range

In general, there are three types of transponders: *passive*, *semi-passive* and *active*. Passive tags have no battery in their circuitry, and they rely solely on the reader to provide the power for the tag to operate. Active and semi-passive tags use internal batteries to power their circuitry. An active tag also uses its battery to broadcast radio waves to a reader, whereas the power to broadcast in semi-passive tags is supplied by the reader. Usually, active tags operate in higher frequencies and have a longer reading range than passive and semi-passive tags.

A specific range of frequencies is reserved in every country or region for industrial, scientific or medical applications that are classified as Industrial-Scientific-Medical (ISM) bands. RFID systems operate in the ISM bands as well. Three major frequency ranges are usually defined within ISM bands for RFIDs: Low Frequency (LF), High Frequency (HF) and Ultra High Frequency (UHF).

LF: Frequencies below 135 kHz are in the LF band. They are low frequency, long wavelength signals. The propagation conditions in these frequencies make LF systems preferable for long-distance, low cost transponders for applications such as livestock tracking. Low frequencies have low absorption rate or high penetration depth in non-metallic materials, which is useful for transponders to be implanted in animals (Finkenzeller, 2003). Such transponders have a low power consumption rate due to the low operating frequency.

HF: The 13.553-13.567 MHz range is located in the middle of the short wavelength range and is referred to as the HF band. The propagation conditions in this frequency ranges are suitable for designing low cost and medium speed transponders (Finkenzeller, 2003). Common RFID systems in the HF band operate with a 13.56 MHz frequency, which is suitable for fast data transmission (typically 106 kbits/s) and high speed operations used in implementing cryptographic functions (Finkenzeller, 2003).

UHF: Frequencies in the range between 888-889 MHz and 902-928 MHz (in the USA and Australia) or 2.400-2.4835 GHz (in Europe) are categorized as the UHF band (Finkenzeller, 2003). This range is suitable for applications that demand