Security Aspects in Radio Frequency Identification Networks

Győző Gódor
Budapest University of Technology and Economics, Hungary

Sándor Imre
Budapest University of Technology and Economics, Hungary

INTRODUCTION

During the last decade RFID (Radio Frequency Identification) technology became ubiquitous; it can be used in almost every fields of our life. RFID solutions are dated back to World War II. Axis fighter pilots made special movements to modify the radar signals reflected from the surface of their planes, thus differentiated the Axis and Allied planes on the radar screen. On the other hand Allied planes were equipped with a so-called Friend or Foe identification system, which worked on the basis of a rudimentary challenge-response identification protocol over radio transmission.

Nowadays, a general RFID system consists of three main parts (Figure 1); a reader, which transmits RF signals; tags that are small integrated circuits with antennae, which use the energy gathered from the RF field to backscatter the data stored on them; and the back-end server, which verifies the tags and executes certain functions. This technology can be used in various applications, e.g., personal identification, payment system, access control, animal tracking, supply-chain management, and many more.

Many kinds of RFID tags are available on the market, which vary in storage and computational capacity. From the cheapest one having very limited computational capacity and low memory, to the more expensive ones, which has its own battery, and has high computational capacity, the most suitable RFID tags for a given application might be found. However, all the tags have low computational capacity; hence the security mechanisms which are in use in computer networks are not suitable in this environment. For expensive tags with relatively large computational capacity many secure communication protocols were developed, for cheap low-end tags, only a few lightweight protocols exist.

Upon implementation of an RFID based management system many questions emerge concerning the security of sensitive business information as well as customer privacy. Let us consider a scenario in a typical commercial setup. A customer enters a shopping center to buy some clothes, books, etc. Since each product has a unique RFID tag, which is situated inside them, a malicious attacker with a portable RFID reader could check the customer's bag in order to decide there is some valuable product inside or not.

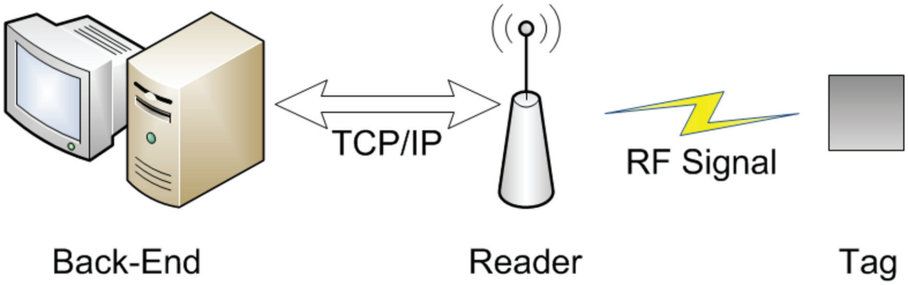
This is just a simple scenario, where some pieces of information about a person or product can be obtained easily; unfortunately more serious problems have to be faced. Since more and more credit cards are supplied with RFID tags, in addition passports and ID cards contain RFID tags, rather sensitive information related to our bank account, or medical record can be accessed. Hence, the security issues of RFID systems are very important; authentication protocols, encryption methods are needed in order to guarantee the secure communication, moreover our privacy.

BACKGROUND

Similar to other wireless networks, in RFID systems the communication between a reader and tags uses the air interface, which is an insecure media and could be eavesdropped easily. Unprotected communication between readers and tags via the radio channel may unfold sensitive information about a tag, e.g., its location, and indirectly the location of the user who possesses the tag. First, we introduce the attacker model in this section, and in possession of it the relevant security and privacy threats in RFID environment are discussed.

DOI: 10.4018/978-1-4666-5888-2.ch433

Figure 1. Common RFID system architecture



Attacker Model

An attacker is anyone who could influence the authentication process or simply monitor the radio channel in such a way that sensitive data could be gained or modified. Two different types of attackers could be differentiated: active and passive attackers.

In case of an active attacker, the malicious entity possesses tools and knowledge by which the communication can be observed and manipulated, e.g., intercepting messages and later replay them, modifying messages or impersonating the parties. Because attackers take part the communication actively, this kind of attacks could be realized easily. However, in case of an appropriately designed authentication protocol where an attacker tries to modify a given message the used cryptographic functions permit the detection of them. For instance, if the messages are not sent in plain but hashed, the receiver could identify any modifications of the message, thus the attack can be detected.

Passive attacker can only monitor the radio channel and can eavesdrop and store the messages of the communication for further processing. Since this attacker does not take part actively in the communication process and thus does not modify the messages, none of the parties could detect the presence of them.

Security Vulnerabilities

As the communication between tags and readers operates via an unprotected media, RFID related concerns are classified into two categories: security and privacy related problems. In case of security a legitimate reader gets information from illegitimate tags, whilst privacy issues deal with illegitimate readers gathering information from legitimate tags. As it was mentioned before, from a consumer's point of view, privacy related problems are typically more important than the security issues.

Although, plenty of RFID based applications have been implemented, and the technology is significantly improved, the security and privacy issues remain potential risks for the proliferation of this technology. The security vulnerabilities should be solved to achieve admirable usage of RFID.

Security Issues

Several security threats occur in RFID systems obstructing RFID to become more popular, familiar, and widespread than before (Thompson, Chaudhry, & Thompson, 2006). In this section the major security goals in RFID systems are introduced.

Protection against eavesdropping: Malicious reader can receive the response from tags without any knowledge of the owner of the tags. In order to guarantee that an attacker could not gain any sensitive information about the tags (or the owner of the tag), messages should be encrypted to be recognizable only for authorized ones. By eavesdropping, an adversary may catch secret information and perform replay attack. Subsequently, the RFID system must be designed in such a way that attackers cannot acquire any secret information from the eavesdropped message and it should resist against the replay attack.

Protection against replay attacks: This kind of attacks belongs to integrity attacks. In order to impersonate a tag the attacker uses a tag's response to answer the reader's challenge.

Protection against tracking: This is one of the most important goals from consumers' point of view of. Since the adversary is able to collect the responses from all the tags, the trackers can reveal when, from where and how much information is transmitted by a given tag.