Chapter 84
Security Risks/Vulnerability in a RFID System and Possible Defenses

Morshed U. Chowdhury
Deakin University, Australia

Biplob R. Ray
Melbourne Institute of Technology, Australia

ABSTRACT

Remote technologies are changing our way of life. The radio frequency identification (RFID) system is a new technology which uses the open air to transmit information. This information transmission needs to be protected to provide user safety and privacy. Business will look for a system that has fraud resilience to prevent the misuse of information to take dishonest advantage. The business and the user need to be assured that the transmitted information has no content which is capable of undertaking malicious activities. Public awareness of RFID security will help users and organizations to understand the need for security protection. Publishing a security guideline from the regulating body and monitoring implementation of that guideline in RFID systems will ensure that businesses and users are protected. This chapter explains the importance of security in a RFID system and will outline the protective measures. It also points out the research direction of RFID systems.

INTRODUCTION

RFID is a wireless technology used to identify an object. Generally, it has three main components: a tag, a reader and a back-end. This chapter assumes that the back-end has enough computational power to operate under existing security protection such as cryptography, hash algorithm, etc. It will discuss secure tag data transmission between the back-end and the tag, malware protection from malicious tag content and the infecting of a clean tag by another infected tag. A tag uses the open air to transmit data via radio frequency (RF). It is also weak in computational capability. RFID automates information collection regarding an individual's

DOI: 10.4018/978-1-4666-4707-7.ch084

location and actions which could be abused by hackers, retailers and even the government.

The tag can be "promiscuous," that is, it will communicate with any reader. The reader can query any tag and gather information which makes users vulnerable to information exposure and location privacy threat. The tag might contain different information sets based on its implication. Commonly, a tag might contain a product code or object code, patient identification code, credit card information, passport number, etc. Exposing part or all of this information could put someone into a life threatening situation.

Retailers are initiating processes for collecting customer information to make their business processes more efficient. This opens up the possibility to identify a customer by attaching a tag. The system can use the information to locate the tag bearer. In the supply chain a competitor might use information gathered from various tag fields. The tag contains a very small amount of information but this information might be sufficient to take unfair advantage of competitors. The tag format and the process of reading data from a tag by reader are very important in understanding the security concerns of a RFID system. There are two popular tag formats available for users; an ISO tag format and an EPC Global tag format. These tags contain different fields which relate to the business entity. The EPC tag format is shown in Table 1.

The tag data format shown in Table 1 is a General Identifier (GID-96) 96-bit EPC tag format, and helps an application to identify an object. The EPCglobal Gen 2 tag encodes a header field, EPC manager, object class and serial number. The header field defines the overall length and format of the values of tag fields. The EPC manager identifies the company associated with the EPC. The object class number refers to the exact type of product being identified. The serial number field identifies the serial number of the product itself. There are two different sizes of Tag: the 64-bit scheme and the 96-bit scheme. The data is stored in a tag using a particular binary encoding. The EPC scheme is then translated using a tag data translation technique (TDT), to a uniform resource identifier (URI). The URI is assembled to form a uniform resource name (URN) notation to represent the identity of a tag (EPCglobal, 2011).

The ISO/IEC 15693-3 tag format is shown in Table 2. The 64 bit Unique Identification Number (UID) has four fields: 40 bit unique serial number for products, 8 bits data to specify tag type, 8 bits to store the manufacturer code and the last 8 bits for ISO specific code for a particular tag model. The ISO specific code should be E0 to ISO/IEC 15693-3.

The intruder can use various fields such as the Object Class and the EPC manager for standard database matching. Later, information can be used to take an illegal business advantage from competitors. To protect the data transmission and the tag, we have to protect security properties (Ray, Chowdhury et al, 2010) such as:

- Data Confidentiality
- Anti-Cloning
- Availability
- Indistinguishability
- Forward Security
- Backward Security
- Tag Tempering
- Reader Authenticity

Table 1. EPC-96 bits tag data format

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

Table 2. ISO-64 bits tag data format

Iso Specific Code For Tag Model	Manufacturer Code	Tag Type	Serial Number
8 bits	8 bits	8 bits	40 bits