



“RFID systems are deployed in many industrial fields, but the security and privacy issues with RFID systems are not well addressed yet. In this article, we will cover three main parts as follows:

- RFID Threats and DREAD Model
- RFID Security and Privacy: Issues and Countermeasures
- EPCglobal Network Security

Firstly, we provide guidance to users and systems designers on potential threats to RFID systems and describe a methodology for assessing the various possible threats in order to determine the relative risk level of a specific RFID application. Secondly, we investigate the security and privacy issues with RFID systems and list a number of possible countermeasures to effectively address those specific issues. Thirdly, we present the potential security problems of EPCglobal network, and identify usable security solutions to make EPCglobal network more secure and cost-effective. Finally, we conclude the article with a vision on secure RFID.”

Mr Tan Jin Soon

Executive Director, EPCglobal Singapore

Chairman of Automatic Data Capture Technical Committee

Dr Li Tieyan

Principal Investigator, Cryptography and Security Department
Institute for Infocomm Research, A*Star

1 INTRODUCTION

Radio Frequency Identification (RFID) technology was developed more than 60 years ago. However, it was only after the successful development of EPCglobal/RFID Gen2 standards [2] in December 2004 and the successful development of EPCIS (EPCglobal Information Service) in April 2007 coupled with the low cost of EPCglobal Gen2 RFID Tags that industries are actively renewing their focus to adopt EPCglobal Gen2 System. We believe that the economies of scale in the demand and production of standard EPCglobal Gen2 tags will further drive the cost of EPCglobal Gen2 Tags lower and stimulate the following industries to adopt EPCglobal RFID System by 2009/2010:

- Manufacturing and production
- Transport and logistics
- Retail and consumer goods

- Public transport
- Healthcare
- Anti-counterfeiting
- Ticketing
- ePayment
- Security
- Recycling

With the wider adoption of RFID applications, it is important to ensure the data security of RFID applications.

This article will provide an insight on RFID Security.

The RFID system is divided into modules, each having their own security elements. These modules are: tag; tag to reader; reader; reader to host; host (back-end enterprise) system. These are illustrated in Figure 1.

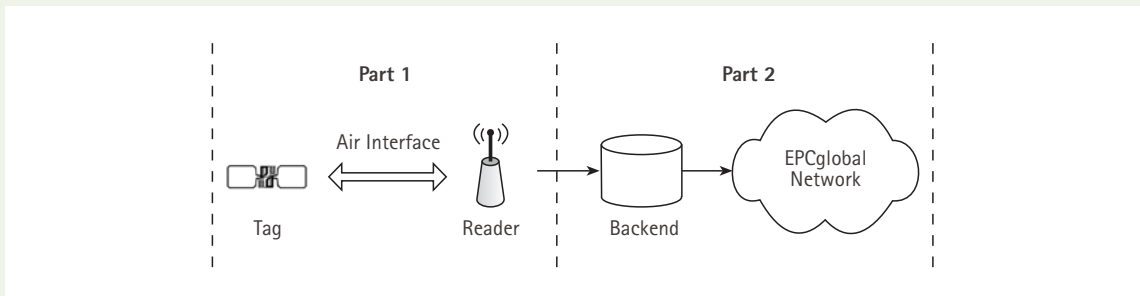


Figure 1: RFID System Architecture

The scope of this article is restricted to the security aspects of the tag and tag-to-reader communication, and EPCglobal network as illustrated in parts (1) to (2) in Figure 1 above. The article will first highlight potential threats and appropriate countermeasures. It will also cover the RFID security and privacy issues. This is because data and personal privacy depend on the use of appropriate security measures. Data access security provides a measure of personal privacy protection by mitigating the potential for unauthorised reading of data on a tag. However, not all data access security countermeasures provide the same level of protection. Part 2 is also important and is addressed in Section 4 in this article.

2 RFID THREATS AND DREAD MODEL

2.1 RFID Threats

The proliferation of RFID tags implies that pervasive RFID technology might bring unintended risks. Unauthorised data collection, where attackers gather illicit information by either actively issuing queries to tags or passively eavesdropping on existing tag-reader communications. RFID threats are categorised as unintentional or intentional.

Unintentional threats are the result of physical or environmental effects, e.g., daily wear and tear on a tag or reader or accidental damage. In this article, we will focus on intentional threats (malicious user abuse - human factors). The threats can be grouped into three primary categories labelled as Mimic, Gather, and Denial of Service (DoS) [1].

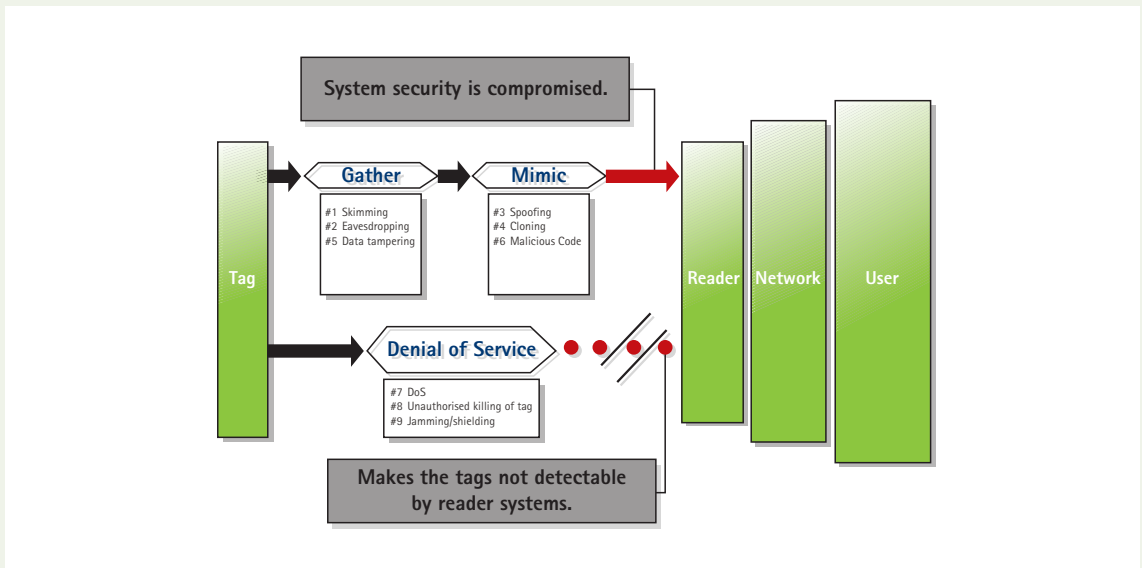


Figure 2: RFID Threat Categories

These categories are shown in Figure 2. The details of those threats are categorised and explained as follows:

- Gather: Skimming, Eavesdropping and Data tampering;
- Mimic: Spoofing, Cloning and Malicious code; and
- Denial of Service.

Skimming data is the unauthorised access of reading of tag data (skimming). Data is read directly from the tag without the knowledge or acknowledgement of the tag holder.

Eavesdropping or "sniffing" on transmission between tag and reader. Eavesdropping (also called passive "man-in-the-middle" reader) is unauthorised listening/intercepting, through the use of radio receiving equipment, of an authorised transmission to monitor or record data between the tag and reader for the purpose(s) of: collecting raw transmissions to determine communications protocols and/or encryption; collecting the tag's data, or determining traffic patterns.

Spoofing is defined as duplicating tag data and transmitting it to a reader. Data acquired from a tag, by whatever means, is transmitted to a reader to mimic a legitimate source. For example, for an electronic seal, a threat that defines spoofing is where the e-seal information is transmitted to the reader from some alternative source that is not the original e-seal.

Cloning is defined as duplicating the data of one tag to another tag. Data acquired from a tag, by whatever means, is written to an equivalent tag. For example, in contrast to spoofing, cloning an e-seal would be the duplication of the e-seal and replacement of the original with a duplicate/cloned version that would then communicate with the reader.

Data tampering is unauthorised erasing of data to render the tag useless or changing of the data. For example data tampering in the consumer goods market could involve changing the price of an item for sale to the detriment of the owner.

Malware insertion of a executable code/virus to corrupt the enterprise systems is hypothetically possible given a tag with sufficient memory and range.

Denial of Service (DoS) occurs when multiple tags or specially-designed tags are used to overwhelm a reader's capacity to differentiate tags, rendering the system inoperative. A type of denial service is a blocker tag that confuses the interrogator so that they are unable to identify the individual tags.

Killing of a tag (electronic or mechanical) is an operational threat in that the physical or electronic destruction of the tag deprives downstream users of the tag of its data.

Jamming/Shielding is the use of an electronic device to disrupt the reader's function. Shielding is the use of mechanical means to prevent reading of a tag.

Utilising a combination of above threats, more serious attacks can be launched on RFID systems including unwanted location tracking of people and objects (by correlating RFID tag sightings from different RFID readers). Beyond these threats, RFID tags suffer from a variety of subtle attacks such as physical invasive attack, where an adversary physically compromises the inlay of a RFID tag and reads the memory for any information; and side channel attack, where an adversary uses timing analysis, power analysis or electromagnetic analysis to extract tag information.

2.2 The DREAD Model

The decision to ensure RFID data access security depends, in part, upon the perceived risks. For RFID data access security, risk is dependent on two variables: probability and the impact upon the individual or organisation. Not all types of data justify high levels of security nor are the costs justified. As security measures increase, cost increases.

Take for example the pharmaceutical chain-of-custody, security breaches could lead to product tampering, counterfeiting, or theft. The impact on the individual could be life-threatening. For dispensing of pharmaceuticals, however, if a pharmacy order number is the only data on the tag, the risk is low because the number itself is non-significant and would not differentiate between Schedule drugs and non-Schedule drugs. Unauthorised access to the pharmacy's database would be required to understand the code's association.

To assess the risk of security threats, the Open Web Application Security Project (OWASP) identifies other factors to security threat levels that include Damage Potential, Reproducibility, Exploitability, Affected users, and Discoverability

(DREAD). Although the DREAD model is targeted towards software security threats, it can be applicable for RFID security. For instance, the definition of RFID DREAD model is:

- Damage Potential: How much damage will be caused if a threat occurs?
- Reproducibility: How easy is it to reproduce the threat exploit?
- Exploitability: What is needed to exploit this threat?
- Affected Users: How many users will be adversely affected?
- Discoverability: How easy is it to discover this threat?

The risk evaluation algorithm of DREAD model is defined as:

$$\text{Risk}_{\text{DREAD}} = (\underline{D} + \underline{R} + \underline{E} + \underline{A} + \underline{D}) / 5$$

and is used to compute a risk value, which is an average of all five categories. The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk. Refer to [1] for more details on RFID risk evaluation.

It is theoretically or actually possible to adversely affect a RFID system's security. Such breaches might depend on: Access to a remote, secure database; Unusual or contrived circumstances to enable reading or data manipulation; Expensive or sophisticated equipment; or Unusually specialised knowledge of the target system. The probability of such an attack is low and may not require significant security measures. However, in other scenarios, the probability may be determined to be high because of the value of data accessed or action enabled by the breach. These scenarios may require more significant security measures.

3 RFID SECURITY AND PRIVACY: ISSUES AND COUNTERMEASURES

3.1 RFID Security Issues

RFID security is the prevention of unauthorised reading and changing of RFID data. RFID data security means protecting the data on the tag and the data transmitted between the tag and reader (or tag to tag in more advanced systems) to ensure it is accurate and safe from unauthorised access. In addition, security includes unauthorised access to the reader from the air interface. RFID systems must employ mechanisms to achieve one or more of the security objectives such as confidentiality, integrity, availability, authentication and access control, to alleviate various security concerns. While security cannot be solely accomplished by security mechanisms, it should be mentioned that proper legislation, procedural techniques and enforcement of laws is also required. In the following, we describe the security objectives in detail and show that meeting these security objectives eliminates the security threats posed by inherent weaknesses in low cost RFID systems.

Confidentiality: The term 'confidentiality' can be used to describe a mechanism to keep information from all but those that are authorised to see it. In a RFID system, the information exchanged between a reader and a tag needs to be confidential when sensitive data such as secret keys, which must not be collected by an eavesdropper, is transferred between a reader and a tag. The confidentiality of any secret information stored on a tag is also at risk

and needs to be secured. Confidentiality may be achieved by having the communication link between tags and readers encrypted, and thus by establishing a secure communication link. Confidentiality of tag contents may be achieved by tamper proofing the tag to prevent physical access to tag contents.

Integrity: Providing data integrity involves a method by which it is ensured that information has not been altered by unauthorised or unknown means. Alteration in a RFID context may involve the capture, substitution, deletion or insertion of information and the retransmission of that altered information to a reader or a tag. Ensuring data integrity will somehow prevent man-in-the-middle attacks. Integrity of a RFID system applies to the integrity of the devices, such as the reader and the tags where it implies that a reader or a tag has not been malevolently changed. A reader receiving data from a tag needs to be able to trust that the information received from a tag is correct, while a tag needs to be able to trust that the information it receives from a seemingly authentic reader is trustworthy. Ensuring the integrity of a system is an important consideration in addressing physical attacks, too.

Availability: Ensuring availability in RFID systems is important since readers need to be ready to detect tags that may enter their reading range at certain intervals of time. In a RFID context, availability applies to ensuring that the services offered by a reader to a RFID tag or the services offered by a tag to a RFID reader are available when expected. RFID systems meeting the availability criteria will ensure that there are services in place to thwart or prevent a DoS attack.

Authentication: The objective of authentication in RFID context can be expressed as authenticating the devices involved (the tags and the reader) or in a supply chain application where the tags are used to label products, as product authentication. In some applications where perhaps the tag is an integral part of the tagged object, authentication of the tag may be adequate to guarantee the authenticity of the object to which it is associated, in other application where tags are placed as an external label to a high value item, authentication of the tag may not be adequate. The objectives of tag and reader authentication and product authentication are discussed below.

- **Tag/Reader Authentication:** In the RFID context, authentication proves the claimed identity of a tag or a reader. It is an important RFID security measure for preventing counterfeiting behaviours. It is also important for controlling access to label contents. The use of authentication may also be required in other applications of RFID technology such as baggage reconciliation or secure entry systems. Authentication of a tag is useful in addressing vulnerabilities posed as a result of cloning.
- **Product Authentication:** In certain use cases, authentication of the tag is not sufficient to guarantee the authenticity of the product to which the tag is attached. These tagged goods are subject to some specific attacks such as the "remove and reapply" attack. Hence in the case of using a low cost RFID tags to label a product, product authentication refers to the establishment of the authenticity of a product by the secure binding of the identity of a tag and the legitimacy of the product with an irrefutable link between the product and the tag that can be verified by a third party.

Access Control: In the interaction between RFID readers and tags, access control implies a mechanism by which a tag or a reader grants access or revokes the right to access some data or perform some operation. Generally tags will require access control mechanisms to prevent unauthorised access to tag contents.