Security Issues in RFID

Kai Wang
Research Institute of Information Technology, Tsinghua University, Beijing, China
wang-kai09@mails.tsinghua.edu.cn

Abstract

RFID (Radio Frequency IDentification) are one of the most pervasive computing technologies with technical potential and profitable opportunities in a diverse area of applications. Among their advantages is included their low cost, convenience and their broad applicability. However, they also present a number of inherent vulnerabilities. This article will provide an insight on RFID security issues by developing a simple classification of RFID threats, presenting their important features, and discussing possible countermeasures against them. The aim of the paper is to introduce and categorize the existing security issues of RFID, so that a better understanding of RFID threats can be achieved, and subsequently more efficient and effective algorithms, techniques and approaches to overcome these threats may be developed.

Keywords

RFID; Security; Privacy; Authentication; Eavesdropping

1. Introduction

Radio Frequency Identification, better known as RFID, is fast becoming one of the most popular technologies of our era. It dates from a paper published by a scientist named Harry Stockman in the late 1940s.

As its name implies, RFID is generally used to describe any technology that uses radio signals for automated identification of specific objects and even people. It may be viewed as a means of explicitly labeling objects to facilitate their “perception” by computing devices.

A RFID system consists of a small embedded microchip (RFID tag) attached to an antenna, that communicates with its interrogating device (RFID reader) using electromagnetic signal at one of several standard radio frequencies. Additionally,

there is usually a back-end database that collects information related to the physically tagged objects.

Similar with Internet, the RFID systems can be considered to be constructed based on four layers[1], as Figure 1 shows: physical layer (the physical interface, the radio signals used and the RFID devices), network-transport layer (the way the RFID systems communicate and the way that data are transferred between the entities of an RFID system), application layer (service applications and the binding between back-end database and RFID tags), and strategic layer (organization and business applications).

Cost vs. Utility Tradeoffs	Logistical Factors	Real-world Constraints	Strategic Layer
EPCIS/ONS	Oracle/SAP	Commercial Enterprise Middleware	Application Layer
ISO 15693/14443	EPC 800 Gen-2	Proprietary RFID Protocols	Network-Transport Layer
RF	Reader IC	RFID tags	Physcial Layer

Figure 1 Layers of RFID Communication

RFID systems can be used to improve service quality, thwart product counterfeiting and theft, increase productivity and maintain quality standards in many areas. In other words, RFID systems can make object management easier and more convenient, just like the Library RFID Management System shows.

Figure 2 Library RFID Management System

However, although the innovation and automation potential of RFID systems is large, they also have a number of inherent vulnerabilities. They are susceptible to a

broad range of malicious attacks ranging from passive eavesdropping to active interference.

The rest of paper is organized as follows. In section 2, we give an overview on the threats in RFID nowadays, mainly focusing on the privacy, authentication and confidentiality problems. In section 3, we present a series of prevalent protection approaches against these threats, and explain their pros and cons. Finally, in section 4, we conclude the property of the present security issues and possible approaches in RFID and discuss some future work in section5.

2. Threats in RFID

In this paper, threats in RFID are divided into four aspects: privacy problem, authentication problem, confidentiality problem and other attacks.

2.1 Privacy Problem

RFID raises two main privacy concerns for users: clandestine tracking and inventorying[2].

RFID tags respond to the reader interrogation without alerting their users. Thus, where read range permits, clandestine scanning of tags is a plausible threat. As discussed above, most RFID tags emit unique identifiers, even tags that protect data with cryptographic algorithms. In consequence, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for clandestine physical tracking. Such tracking is possible even if a fixed tag serial number is random and carries no intrinsic data.

In addition to their unique serial numbers, EPC (Electronic Product Code) tags carry information about the items to which they are attached. Thus a person carrying EPC tags is subject to clandestine inventorying. A reader can silently determine what objects the user has on him, and harvest important personal information just as Figure 3 shows. This problem of inventorying is largely particular to RFID.

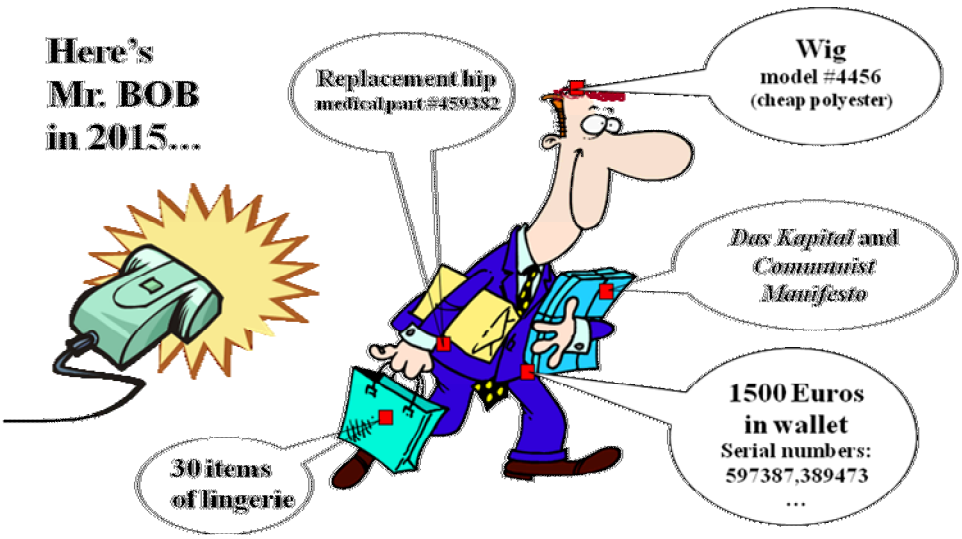

Figure 3 An illustration of potential consumer privacy problem of RFID

2.2 Authentication Problem

To some extent, privacy has overshadowed the equally significant problem of authentication. Generally speaking, RFID privacy concerns the problem of malicious readers harvesting information from good tags. RFID authentication, on the other hand, concerns the problem of good readers harvesting information from malicious tags, particularly counterfeit ones[2].

Basic RFID tags are vulnerable to simple counterfeiting attacks. Scanning and replicating such tags requires little money or expertise. Jonathan Westhues, an undergraduate student, describes how he constructed what is effectively an RF tape-recorder. This device can read commercial proximity cards, even through walls, and simulate their signals to compromise building entry systems.

Figure 4 shows that, the "clone" Mr. BOB can counterfeit the identity of a legitimate tag in order to be authenticated by the reader as the real Mr. BOB, and his things may be also illegitimate or bad, this can cheat the reader as the same. So the real Mr. BOB's rights can be possibly abused or violated.

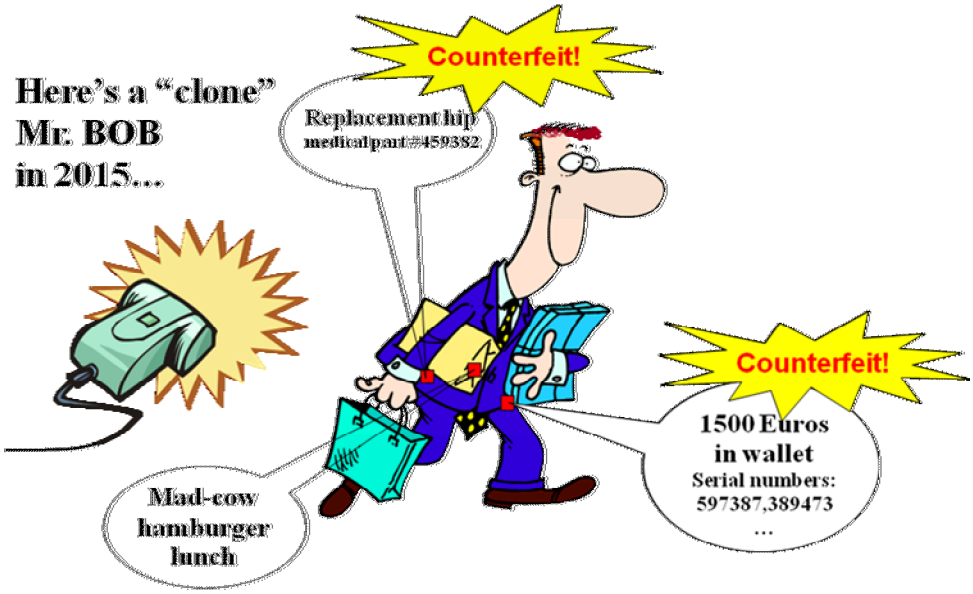

Figure 4 An illustration of potential consumer authentication problem of RFID

2.3 Confidentiality Problem

The wireless nature of RFID makes eavesdropping one of the most serious and widely deployed threats[4], so the confidentiality problem is of great importance.

In eavesdropping, an unauthorized individual can use an antenna to record communications between legitimate RFID tags and readers. This type of attack can be performed in both directions, tag-to-reader and reader-to-tag.

Since readers transmit information at much higher power than tags, the former are susceptible to this type of attacks at much greater distances and consequently to a greater degree. The signal that will be eavesdropped is also subject to the location of the eavesdropper regarding the RFID tag and reader as well as the possible countermeasures employed for deteriorating the radio signal. The feasibility of this attack depends on many factors, such as the distance of the attacker from the legitimate RFID devices.

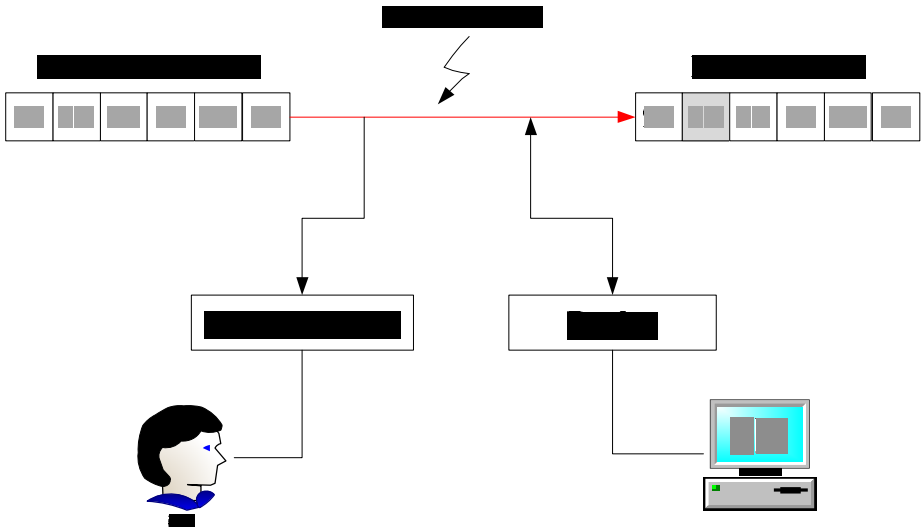

Figure 5 Attempted attacks on a data transmission

As Figure 5 shows, the motivation of this attack is to collect raw transmissions to collect the tag's data, determine the traffic pattern, or figure out the communication protocol and/or encryption. So, this behavior can also bring in cloning, tracking, replay and problems so on.

2.4 Other Attacks

Other attacks focus on intentional threats, which can be grouped into three primary categories labeled as Mimic, Gather, and Denial of Service (DoS). These categories are shown in Figure 6.

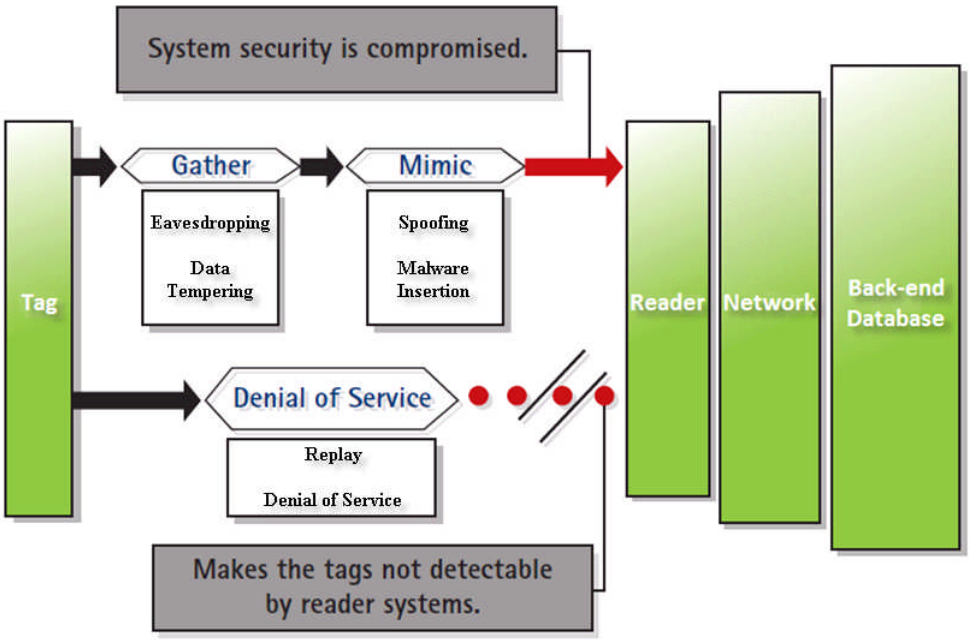

Figure 6 RFID attacks categories

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.

Malware Insertion is defined as having a tag carry malicious code/virus rather than valid data in its data storage area, such as SQL Injection or worms.

Replay is defined as that valid RFID signal is intercepted and its data is recorded, this data is later transmitted to a reader where it is "play back".

Data Tampering is defined as unauthorized erasing of data to render the tag useless or changing of the data.

Denial of service occurs when multiple tags or specially designed tags are used to overwhelm a reader's capacity to identify individual tags, in order to make the system inoperative.

All above are important security issues in RFID systems, but not issues specific to RFID.

3. Protection Approaches in RFID

Now that the RFID is vulnerable, some protection approaches must be developed for its security.

3.1 Protection against Privacy

There are several approaches to solve the privacy problems, here we give some common ones[2].

"Killing" and "Sleeping"

When an EPC tag receives a "kill" command from a reader, it renders itself permanently inoperative. To prevent wanton deactivation of tags, this kill command is PIN protected. To kill a tag, a reader must also transmit a tag-specific PIN (32 bits long in the EPC Class-1 Gen-2 standard). As "dead tags tell no tales," killing is a highly effective privacy measure.

Killing or discarding tags enforces consumer privacy effectively, but it eliminates all of the post-purchase benefits of RFID for the consumer. Rather than killing tags at the point of sale, then, why not put them to "sleep", i.e., render them only temporarily inactive? This concept is simple, but would be difficult to manage in practice. Clearly, sleeping tags would confer no real privacy protection if any reader at all could "wake" them. Therefore, some form of access control would be needed for the waking of tags.

This access control might take the form of passwords, specific PINs, or biometrics, much like those used for tag killing. To wake a sleeping tag, a reader could transmit this information.

Re-encryption

To prevent RFID-tag tracking, it is necessary that tag identifiers be suppressed, or that they change over time. Juels and Pappu (JP) consider the special problem of consumer privacy-protection for RFID-enabled banknotes. Their scheme employs a public-key cryptosystem with a single key pair: A public key P_K, and a private key S_K held by an appropriate law enforcement agency. An RFID tag in the system carries a unique identifier S, the banknote serial number. S is encrypted under P_K as a ciphertext C; the RFID tag emits C. Only the law enforcement agency, as possessor of the private key S_K, can decrypt C and thus learn the serial number S.

To address the threat of tracking, Juels and Pappu propose that the ciphertext C be periodically re-encrypted. They envisage a system in which shops and banks possess re-encrypting readers programmed with P_K. The algebraic properties of the El Gamal cryptosystem permit a ciphertext C to be transformed into a new, unlinkable ciphertext C' using the public key P_K alone, and with no change to the underlying plaintext S. In order to prevent wanton re-encryption by, e.g., malicious passersby, JP propose that banknotes carry optical write-access keys; to re-encrypt a ciphertext, a reader must scan this key.

Blocker tags

The blocker tag is a proposal by Juels, Rivest, and Szydlo for protecting consumer privacy. A blocker tag is a simple, passive RFID device, similar in cost and form to an ordinary RFID tag, however, it performs a special function.

A blocker RFID tag possess a special bit designating them either “public” or “private”: a ‘0’ privacy bit marks a tag as subject to unrestricted public scanning; a ‘1’ bit marks a tag as “private”. When a reader attempts to scan RFID tags that are marked as “private”, a blocker tag jams the reader. More precisely, the blocker tag cheats the tag-to-reader communications protocol in such a way that the reader perceives many billions of nonexistent tags and therefore stalls.

How does a blocker actually prevent undesired scanning? It exploits the anti-collision protocol that RFID readers use to communicate with tags. This protocol is known as singulation. Singulation enables RFID readers to scan multiple tags simultaneously. To ensure that tag signals do not interfere with one another during the scanning process, the reader first ascertains what tags are present, and then addresses tags individually.

One type of RFID singulation protocol is known as treewalking. In this protocol, as Figure 7 shows, l-bit tag identifiers are treated as the leaves of a binary tree of depth l, labeled as follows. The root has a null label.

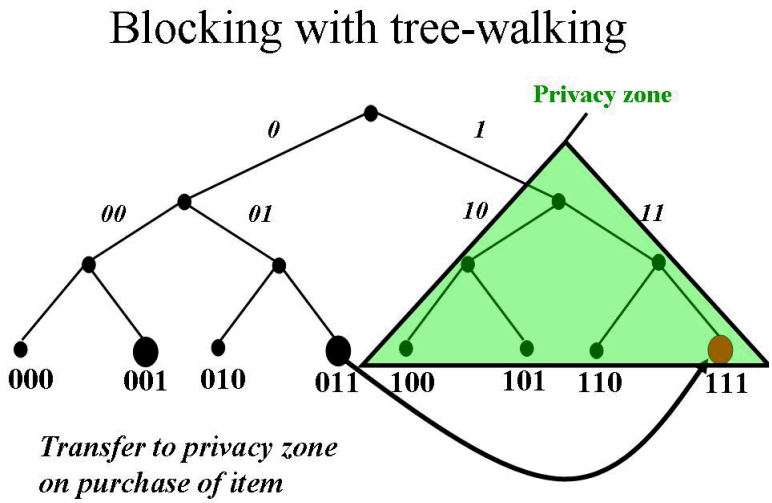

Figure 7 How a blocker tag works

The reader effectively performs a depth first search of this tree to identify individual tags. Starting with the root of the tree, the reader interrogates all tags. Each tag responds with the first bit of its identifier. If the only response received by the reader is a '0' bit, then it concludes that all tag identifiers lie in the left half of the tree; in this case the reader recourses on the left half of the tree. Conversely, a concordant response of '1' causes the reader to recurse on the right half of the tree. If the tag signals collide, that is, some tags emit '0' bits and others emit '1' bits, then the reader recurses on both halves of the tree. The reader continues recursing in this manner on sub-trees; it restricts its interrogation to tags in the current subtree. This procedure eventually yields the leaves – and thus the l-bit identifiers – of responding tags.

3.2 Protection against Authentication

Authentication problem can be solved by incorporation of cryptological procedures.

Mutual Symmetrical Authentication

For authentication and to determine the parties' legitimacy, the reader and tag in the communication need to check the other party's knowledge of a secret cryptological key. The following authentication approach, called Mutual Symmetrical Authentication[6], is based on the principle of three-pass mutual authentication in accordance with ISO 9798-2, in which the procedure above is necessary.

In the mutual symmetrical authentication, the tags and readers of an application are in possession of the same secret crytological key *K*. When a tag first enters the interrogation zone of a reader, it cannot be assumed that the two participants in the communication belong to the same application.

From the point of view of the reader, there is a need to protect the application from manipulation using falsified data. Likewise, on the part of the tag, there is a need to protect the stored data from unauthorized reading or overwriting.

The procedure begins with the reader sending a GET_CHALLENGE command to the tag. When the tag receives this command, it generates a random number R_A and send it back to the reader (This is called Challenge-Response procedure). The reader now generates a random number R_B. Using the common secret key K and a common key algorithm e_K, the reader calculates an encrypted data block called token 1, it contains both the random number R_A and R_B, and additional control data Text1, then sends this data block to the tag.

$$\text{Token 1} = e_K(R_B||R_A||ID_A||\text{Text1})$$

The tag decrypts the received token 1, and compares the received R_A with the previously transmitted R_A. If the two figures correspond, then the tag could confirm that the two common keys correspond.

Afterwards, another random number R_{A2} is generated in the tag, and this is used to calculate an encrypted token 2, which also contains R_B and control data Text2. Token 2 is sent from the tag to the reader.

$$\text{Token 2} = e_K(R_{A2}||\ R_B\ ||\text{Text2})$$

At last, the reader decrypts token 2 and checks whether the received R_B is equal to the previous one. If the two figures correspond, then the reader could confirm the key too. Now, the tag and reader have authenticated each other, and further data communication is thus legitimized, as Figure 8 shows.

Figure 8 Mutual symmetrical authentication procedure

The mutual symmetrical authentication procedure has following advantages.

First, there is no need for the secret key to be transmitted on the air, only encrypted random numbers are transmitted.

Second, two random numbers are always encrypted simultaneously, this rules out the possibility of performing an inverse transformation using R_A to obtain token 1, with the aim of calculating the secret key.

Third, the token can be encrypted using any algorithm.

Fourth, the strict use of random numbers from two independent sources means that recording an authentication sequence for replay attack would fail.

Fifth, a random session key can be calculated from the random numbers generated, this can be used to secure the subsequent data transmission.

However, all tags belonging to an application are secured using an identical cryptological key. For applications that involve vast quantities of tags, this represents a potential source of danger. Because such tags accessible to everyone in uncontrolled numbers, the small probability that the key for a tag will be discovered must be taken into account. If this occurred, the procedure described above would be totally open to manipulation.

Derived Key Authentication

An improved idea is making the key of each tag derived independently. So, the Derived Key Authentication is put forward[6].

In derived key authentication, unique ID number of each tag is read out during its production, and a individual key K_X is calculated using certain cryptological algorithm and a master key K_M, so the tag is thus initialized. Each tag thus receives a key linked to its own ID number and the master key K_M.

Then the authentication begins with the reader requesting the ID number of the tag. In a Security Authentication Module (SAM) in the reader, the tag's specific key K_X is calculated using the master key K_M, so that this can be used to initiate the mutual symmetrical authentication procedure, as we describe before. Figure 9 shows the procedure of Derived key authentication.

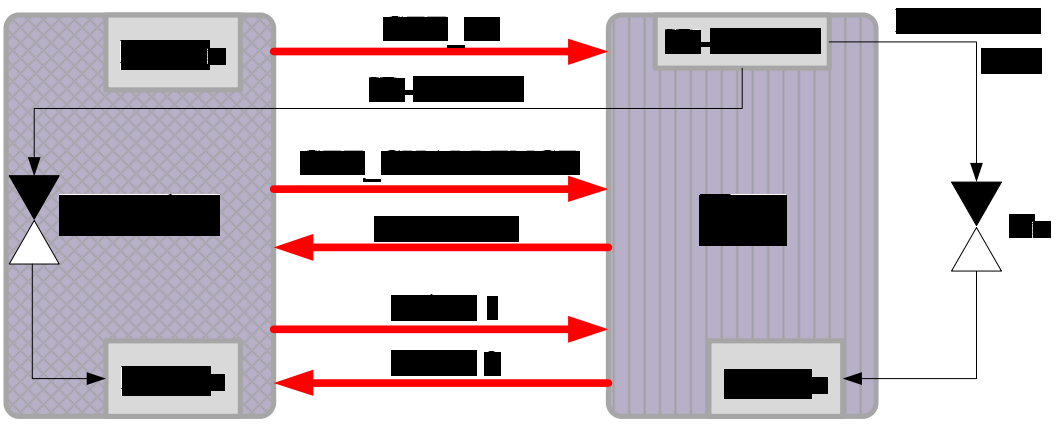

Figure 9 Derived key authentication procedure

3.3 Protection against Confidentiality

As for the confidentiality, the common solution is using encryption.

As Figure 10 shows, the pseudorandom generator can achieve our aim[6]. The Internal state *M* is changed after every encryption step by the state transformation function g(*K*), The pseudorandom generator is made up of the components *M* and g(*K*). The security of the cipher depends principally on the number of internal states *M* and the complexity of the transformation function g(*K*). The encryption function f(*K*) itself, on the other hand, can be generally very simple and can only comprise an addition or XOR logic gating.

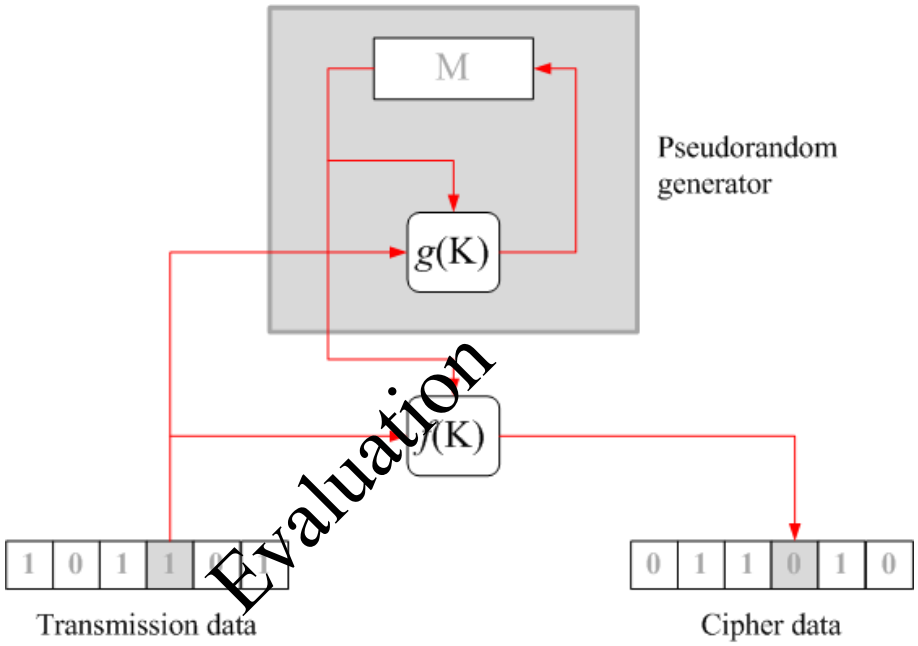

Figure 10 Encryption using a pseudorandom generator

Thus, the security study of sequential ciphers and encryption/decryption is primarily concerned with the analysis of pseudorandom generators.

3.4 Protection against Other Attacks

For other attacks such as Spoofing, Malware Insertion, Replay, Data Tampering, and Denial of Service, there are several countermeasures as Table 1 shows.

Table 1 Protection Techniques against different attacks

Category	Techniques
Spoofing	Appropriate authentication Protect secrets Don't store secrets
Malware Insertion	Middleware Detection

Replay	Appropriate authentication Timestamps
Data Tampering	Appropriate authentication Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Denial of service	Appropriate authentication Appropriate authorization Filtering Throttling Quality of Service

4. Conclusion

For the applications in bank, should be more secure than those in supermarket. So, the design and use of security approaches, should depend on the security requirements. Because, although the performance is not a problem, the cost and the complexity of RFID system is necessary to be considered. And the more complicated the system is, the more secure it could be. What we need to do, is to figure out the way with less cost and better security.

Nowadays, the security issues in RFID are not so serious as Internet, but they have much similarity to some extent. We may consider the security issues in RFID according to the experience in Internet.

Figure 11 is the classification of RFID attacks according to the layer structure in RFID systems as we previously describe[1]. It indicates that the attacks in RFID can be deployed in different layers.

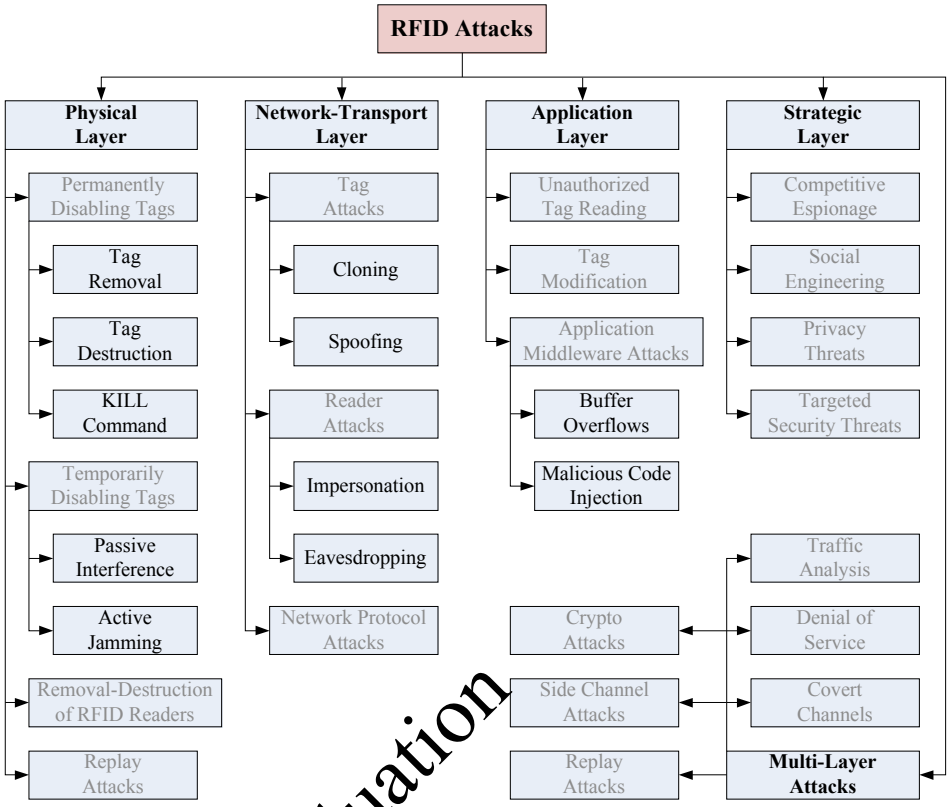

Figure 1. Classification of RFID attacks

According to the classification, what can be considered is that, IPSec, SSL or TLS, S/MINE or PGP is applied in IP layer, TCP layer, application layer respectively, to supply protective security in Internet. So, to deal with the security issues in RFID, a thought is design a kind of countermeasure against certain layer.

From my point of view, We can focus our attention on the network-transport layer, because no matter what the attack is, the network-transport layer must be the weakest and initial point to intrude.

From this point, we may consider that dividing the system into two parts, one is from the tag to the reader, the other is from the reader to the database. We can try to guarantee the security of the former part to make wireless data transmission secure without caring the latter one. In this way, if the attacks can be blocked at source, the affect of the threats will be decreased greatly.

5. Future work

In the future, it is not possible for people to take diverse RFID tags with them, the trend is that, one tag can have many integrated functions to support many readers which can supply various services, such as CPU card. So the symmetrical authentication described in this paper will be not as valid as we expect because of its

symmetrical key for single application. So the key distribution problem has to be concerned.

We will call the secret data a key, and the message data that has been encrypted with the secret data, authentication data. We will also call a "key" the data that a recipient will use to validate the authentication data. Let's say two parties want to communicate: How does the sender securely transfer the validating key to the recipient when the sender and recipient don't already have a secure way of communication? This is called the key distribution problem.

The point is that, distributing the key for validating authentication data that has been algorithmically combined with a user's key is an outstanding problem in all authentication systems, not only in RFID systems. Solutions to the Key Distribution Problem exist, but all solutions to date carry high costs for the infrastructure and administration needed to support them. Therefore, distributing validation keys is definitely a security issue in RIFD, and it is significant for us to consider it.

Reference

[1] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, *Classfying RFID Attacks and Defenses*, Information Systems Frontiers Special Issue on RFID, 2009.

[2] A. Juels, *RFID Security and Privacy: A Research Survey*, IEEE Journal on Selected Areas in Communications, 24(2): 381–394, Feb. 2006.

[3] F. Thornton, *RFID Security*, Rockland MA: Syngress Publishing, 2006.

[4] S. Garfinkel and B. Rosenberg, Eds., *RFID: Applications, Security, and Privacy*, Upper Saddle River, NJ: Addison-Wesley, 2006.

[5] H. Y. Chien and C. H. Chen. *Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards*, Computer Standards and Interfaces, Elsevier Science Publishers, 29(2):254–259, February 2007.

[6] S. Ahson and M. Ilyas, Eds., *RFID handbook: applications, technology, security, and privacy*, Boca Raton: CRC Press, 2008.

[7] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, In 1st International Conference on Security in Pervasive Computing, 2003.