16

Privacy Enhancing Techniques on RFID systems[1]

Masataka Suzuki[1] and Kazukuni Kobara[2]
[1]*Bank of Japan*
[2]*National Institute of Advanced Industrial Science and Technology*
Japan

1. Introduction

An RFID system is a tracking and tracing system, and is useful for the management of various items and animals in a supply chain, animal husbandry and so on. According to a Japanese investigation firm, the number of RFID tags in Japan will increase rapidly from 51 million in 2007 to 1.7 billion in 2012 (Yano Research Institute, 2008).

In RFID systems, RFID tags, which have unique IDs, are attached to items, and RFID readers confirm whether something is there and identify what it is by obtaining its ID. It is, however, pointed out that exploiting RFID systems could lead to some privacy issues. One issue is that someone may know what you have by getting the IDs of your items. Another one is that someone may know when and where you were by recording the time and the place at which the IDs were obtained. Many kinds of countermeasures against these issues have been proposed. Some of them have been implemented in RFID products.

This chapter explains the privacy issues concerning RFID systems, their countermeasures and finally compares them from the security point of view.

2. An RFID system and its privacy issues

2.1 A basic RFID system

At first, we explain a basic RFID system in which an RFID tag, hereafter called *a Tag*, emits a plaintext of its ID to *a Reader*. The RFID system consists of the Tags, the Reader and *a Server*. The Server assigns a unique ID to each Tag preliminarily (Fig. 1-1)). This task may be done by manufacturers when shipping. The Server records the IDs and their corresponding information to its database (Fig. 1-2)). In the phase of reading the ID of the Tag, the Reader sends an ID-query to a Tag (Fig. 1-3)) and receives the ID as a response from the Tag (Fig. 1-4)). The Reader forwards the ID to the Server (Fig. 1-5)), and the Server looks up its corresponding information in the database (Fig. 1-6)).

[1] Views expressed in this chapter are those of authors and do not necessarily reflect the official views of the Bank of Japan and National Institute of Advanced Industrial Science and Technology.

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

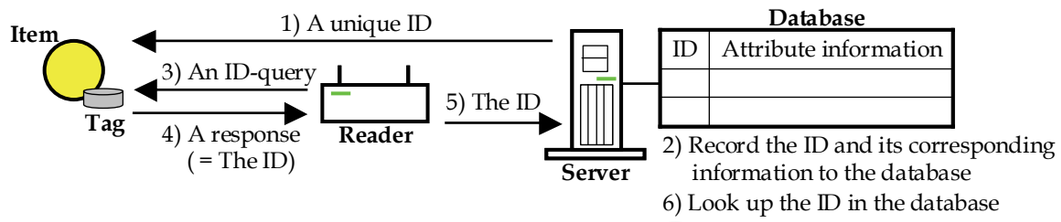

Fig. 1. A basic RFID system

2.2 Privacy issues on the RFID systems

It is worried that usage of RFID systems could lead to privacy violations in the following two senses. One issue is that someone, hereafter called *an Adversary*, may know what you have by obtaining the IDs of your items if the Adversary knows the relationship between the IDs and their corresponding information. The IDs can be obtaining by eavesdropping on the communications between legitimate Readers and Tags or by the Adversary sending an ID-query to your Tags. The Adversary may guess the corresponding information of a new ID from known IDs if the ID format is "an identifier of a company, an identifier of a product, an identifier of an individual product." We call this issue *belongings privacy* in this chapter.

Another issue is that the Adversary may know where you have been. Suppose you go around in a city with Tag-attached items. And the Adversary is supposed to locate many Readers in various places in the city, e.g. a hospital, a supermarket or an apartment, in order to collect IDs from people who pass near the Readers. For example, your ID, to be accurate, an ID of your item, is contained in two sets of IDs. The sets consist of IDs which were collected at the hospital and at your apartment, respectively. The Adversary may guess you are sick by confirming that your ID is contained in the two sets. That is, the Adversary knows where you have been by confirming the link of collected IDs, in other words, whether the IDs are emitted by the same Tag or not. This issue is called *location privacy*.

2.3 Approaches of countermeasures against privacy issues

Countermeasures against belongings privacy are to prevent an Adversary from obtaining IDs themselves or the relationship between IDs and items. The countermeasures against obtaining IDs are 1) to conceal the existance of Tags by preventing Tags from emitting any IDs and signals, 2) to prevent the Adversary from obtaining IDs by generating jamming and 3) to record not plaintexts of IDs but ciphertexts of the IDs in the Tags. The countermeasures against obtaining the relationships are 4) to make it difficult to guess the product of a new ID from the known relationship and 5) to employ strict access control on a database which records the relationship.

Countermeasures against location privacy are countermeasures 1) and 2) above because they prevent the Adversary from obtaining IDs. Countermeasure 3) above is not effective against location privacy. The Adversary can confirm the link of ciphertexts emitted from Tags by regarding the ciphertexts as new identifiers of the Tags if the ciphertexts are static. Therefore, for solving the location privacy, we need to make it difficult for the Adversary not only to extract IDs from the ciphertexts but also to confirm the link of ciphertexts. We call this countermeasure 6). Of course the Server must resolve the IDs from the recieved ciphertexts.

The countermeasures 4) and 5) above are not specific ones for RFID systems but can be used in general for information systems which use IDs and databases. Therefore we may refer to

operational countermeasures for such kinds of systems. Countermeasures 1) and 2) are effective against both issues. In addition, countermeasure 6) is more sophisticated than countermeasure 3). Consequently, we focus on countermeasures against location privacy, i.e. countermeasures 1), 2) and 6), hereafter. Fig. 2 shows the relation between the three countermeasures.

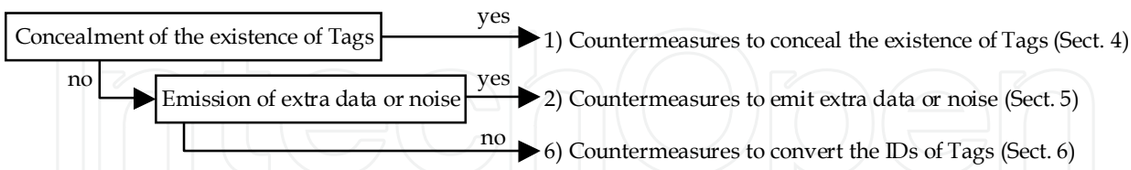

Fig. 2. Approaches of the countermeasures against location privacy

3. Assumptions of an adversary

We assume the following conditions for an Adversary:

- The Adversary cannot eavesdrop upon communications between a legitimate Server and legitimate Tags (Fig. 3-1)) because the ID assignment process is done in a secure area.
- The Adversary cannot obtain IDs and the corresponding information from the Server's database because the database is appropriately managed.
- The Adversary can eavesdrop upon the communication between a legitimate Reader and legitimate Tags (Fig. 3-3), 4)) because they communicate through a public channel.
- The Adversary can send ID-queries to the legitimate Tags (Fig. 3-3′), 4′)).
- The Adversary cannot eavesdrop the communication between the legitimate Reader and the Server (Fig. 3-5)) because they communicate through a secure channel, e.g. Virtual Private Network.
- The Adversary can extract secret information, e.g. an ID and a cryptographic key, from the Tag.

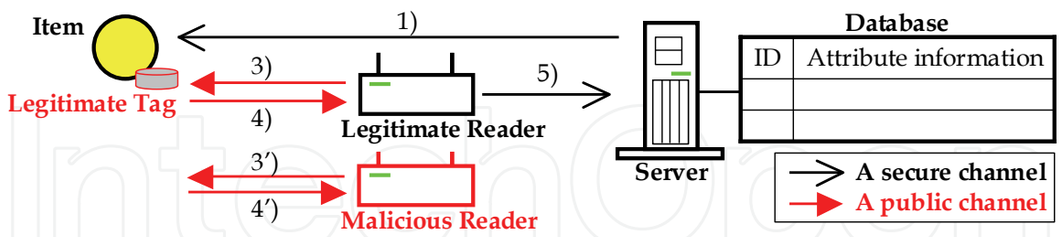

Fig. 3. The secure and public channels in the RFID system

Fig. 3 shows the secure channels and public ones in the RFID system. In order to make descriptions simple after section 4, we assume the Reader has the Server's resources, i.e. the computation power, the memory and the database. In other words, we describe the Server's task as the Reader's one.

4. Countermeasures to conceal the existence of Tags

This section introduces countermeasures which prevent Tags from emitting responses and signals against ID-queries. These countermeasures can conceal the existence of a Tag though we cannot receive the services of the RFID system.

4.1 Destroying / detaching Tag

This countermeasure is to destroy or to detach a Tag from an item. After destroying or detaching, we cannot permanently use the Tag. The means of destruction are, for example, to cut the antenna of the Tag by scissors, to burn off the logical circuits in the Tag by a high voltage electrical current and so on.

4.2 Faraday cage

This countermeasure is to wrap a Tag with some material, e.g. foil, which intercepts electromagnetic waves, i.e. ID-queries, in order to prevent the Tag from emitting responses. It is, however, difficult to apply the countermeasure to some items, such as large things, pets and domestic animals.

4.3 Kill command

This countermeasure is to implement a specific command on a Tag, which prevents the Tag from emitting responses. The Tag does not respond permanently after the Tag executes the command. Compared with the destroying/detaching of the Tag, this countermeasure disables the Tag only by executing the command. Therefore in order to protect against its misuse, we need to authenticate the Reader which directs the Tag to execute the command.
The command is implemented as *a Kill command* in a Tag, conforming to EPCglobal specification. The Tag has an authentication mechanism in which the Tag verifies a password sent by a Reader. The bit lengths of the password are 8 bits in EPCglobal Class 1 in frequency range of 860 MHz – 930 MHz (Auto-ID Center, 2002), 24 bits in Class 0 in that of 900 MHz (Auto-ID Center, 2003a) and Class 1 in that of 13.56 MHz (Auto-ID Center, 2003b), and 32 bits in Class 1 Generation 2 (ISO 18000-6 Type C, EPCglobal Inc., 2005), respectively. However, the number of the variation of the password is 256 at most in the case of an 8-bit password, it is not secure from the viewpoint of cryptography, that is, the Adversary may cause the Tag to execute the command.

4.4 Access password schemes

This countermeasure, hereafter called *an access password scheme*, is to respond an ID of a Tag when the Tag receives a correct password from a Reader. The countermeasure is relatively easy to implement and can conceal the existence of the Tag from an Adversary. However, the Adversary can obtain the password and the ID by eavesdropping upon the communication between the legitimate Reader and the Tag. The countermeasure is adopted in EPCglobal Class 1 Generation 2 (ISO 18000-6 Type C) and the bit length of password is 32 (EPCglobal Inc., 2005).

4.5 Hash Lock scheme

This countermeasure, called *Hash Lock scheme*, involves a Tag authenticating a Reader before sending its ID as a response (Weis et al., 2003). This scheme is executed with the following procedures:

1. A Reader generates a password for each Tag and calculates a hash value for each password. The Reader assigns a unique ID and the hash value to each Tag. In addition, the Reader stores the IDs, the corresponding hash values and passwords in the database.
2. Upon receiving an ID-query from the Reader, the Tag sends its hash value to the Reader.

3. The Reader looks up the corresponding password in the database and sends the password to the Tag.
4. The Tag calculates the hash value of the password and compares it with the stored one. The Tag sends its ID if it matches.

The advantage of Hash Lock scheme over the access password scheme is that a lot of time is required in order to guess the password from the secret information in the Tag. An Adversary must analyze the hash value in the Hash Lock scheme but need not analyze it in the access password scheme. The Adversary, however, can obtain the password against both schemes only by eavesdropping upon communications between a legitimate Reader and the Tags. The Adversary can confirm the links between the responses, i.e. the hash values, because the responses are static in Hash Lock scheme.

4.6 Change of operation modes

This countermeasure is to flexibly select whether to conceal the existence of the Tag or not by changing the operation modes of the Tag. Many schemes related to this countermeasure are proposed. We introduce two of these schemes in this section: EPCglobal Class 1 in frequency range of 860 MHz – 930 MHz (Auto-ID Center, 2002) and *LKI scheme* (Liu et al., 2004).

In EPCglobal Class 1 at 860 MHz – 930 MHz, the operation mode in which the Tag sends its ID is called *an Active mode* and the operation mode in which the Tag dose not emit its ID and signal is called *a Quiet mode*. And two commands are also implemented. The command, called *a Talk command*, changes the Tag to Active mode. Another one, called *a Quiet command*, changes the Tag to the Quiet mode. This scheme should keep supplying electric power to the Tag in order to maintain the Tag in each mode. Therefore, an Adversary may notice the existence of the Tag by detecting the supply source. Moreover, it needs an authentication mechanism that prevents the Adversary from executing the commands.

In LKI scheme, the operation mode in which the Tag does not emit its ID and signal is called *a Silent mode*. LKI scheme assumes that the Tag has a non-volatile memory to record the operation mode. Then the Tag maintains its operation mode without electric power. This scheme also needs the authentication mechanism. According to Liu et al., the password-based authentication may be enough if the password is managed appropriately and legitimate Readers pay appropriate attention to eavesdropping upon communication of authentication (Liu et al., 2004).

5. Countermeasures to emit extra data or noise

This section introduces countermeasures using extra devices which emit extra data or noise. The countermeasures can prevent an Adversary from obtaining a Tag's ID even if the Tag emits its ID as it is. The countermeasures cannot conceal the existence of the Tag, or to be accurate the extra device, but require no changes or only small changes to the Tag.

5.1 Jamming

An extra device in this countermeasure emits jamming to prevent a Reader from obtaining a Tag's ID. This countermeasure requires no changes in the Tag. Moreover, a legitimate Reader cannot obtain the ID if the device emits jamming. Its disadvantages are follows:

- Some countries restrict the emission of jamming. Moreover, the emission of electromagnetic waves is restricted in some areas, e.g. hospitals. This countermeasure cannot be employed in such situations.

- This countermeasure may prevent Readers in other RFID systems from communicating with Tags.
- An Adversary may be able to trace the Tag by continuously observing the source of the jamming.

5.2 Blocker Tag

Readers use anti-collision protocols for obtaining multi Tags' IDs sequentially in RFID systems. An extra device, called *a Blocker Tag*, emits many dummy IDs in order to obstruct the execution of *a Binary Tree protocol* which is one of the anti-collision protocols (Juels et al., 2003). We introduce a Blocker Tag.

At first, we explain the mechanism of the Binary Tree protocol. Suppose each Tag has a 2-bit ID and there are two Tags, whose IDs are 00 and 10 respectively, in the range where a Reader can communicate with them. The Reader using the protocol obtains the IDs with the following procedures (Fig. 4):

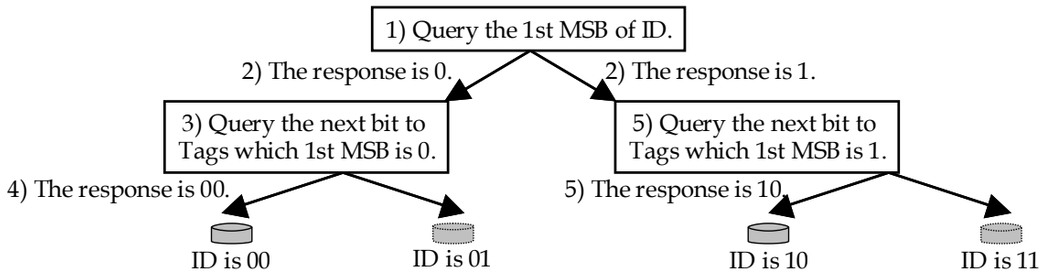

Fig. 4. Binary Tree protocol

1. The Reader asks Tags their most significant bits (MSBs) of their IDs.
2. Each Tag sends 0 or 1, and the Reader detects MSBs of the Tags in the area where the Reader can communicate.
3. The Reader asks the Tags for the next bit of the IDs whose MSBs are 0.
4. The Tag sends 00 and the Reader detects the Tag with 00.
5. The Reader asks the Tags for the next bit of the IDs whose MSBs are 1 in the same way. And it also detects the Tag with 10.

A Blocker Tag behaves as if there were every ID in the range. That is, the Blocker Tag emits "00 and 01" and "10 and 11" in the 4th and 5th steps of the above, respectively. Therefore, the Reader obtains all of the IDs, i.e. 00, 01, 10 and 11. The bit length is only 2 bits in the above case, but the length is longer, e.g. 128 bits, in practical systems. Then the Reader fails to obtain the all of the IDs.

This scheme needs no change to the Tag. Moreover, the Blocker Tag is not more sever than jamming from the viewpoint of the restriction of the emission of electromagnetic waves because the Blocker Tag reacts only when receiving queries[2]. The disadvantages of the Blocker Tag are a) a user must carry it, b) it may obstruct Readers communicating with Tags in other RFID systems, c) an Adversary with a smart Reader, which can accurately identify the location of a Tag sending its ID, may obtain the ID.

[2] The restriction of the emission is not completely solved because the Blocker Tag reacts when receiving the queries.

A more sophisticated Blocker Tag, called *a Selective/Partial Blocker Tag*, is proposed (Juels et al., 2003). A Selective/Partial Blocker Tag obstructs the read of only pre-defined IDs, e.g. the MSB of the IDs is 1, though the original Blocker Tag obstructs the read of every ID.

6. Countermeasures to convert the IDs of Tags

This section introduces countermeasures which make it difficult for an Adversary to confirm the link of responses sent by Tags. Of course legitimate Readers can identify their IDs from the responses. Receiving ID-queries, the Tags always send the response. Therefore the countermeasures cannot conceal the existence of the Tags.

6.1 Randomized Hash Lock scheme

Randomized Hash Lock scheme assumes Tags are implemented with a pseudo-random generator and a one-way hash function H()[3] (Weis et al., 2003). The Tags emit the hash value of their IDs and random numbers. The security of this scheme is based on the difficulty of inversion of the one-way hash function. A concrete procedure is as follows:

1. Upon receiving an ID-query, a Tag generates random number r and calculates hash value h of its ID and r, i.e. $h = H(ID||r)$, where $ID||r$ denotes concatenation between ID and r. And the Tag sends h and r as its response to the Reader.
2. Upon receiving h and r, the Reader calculates the hash value $H(x||r)$, where x denotes each ID of the Tags managed by the Reader. And the Reader exhaustively searches for x such that $H(x||r)$ matches h. The Reader regards the corresponding x as the Tag's ID if it matches.

It is difficult for an Adversary to identify the Tag's ID by comparing the responses mutually because the responses sent by the Tag change at each ID-query. However, this scheme may have two problems: a) the Adversary may be able to identify the ID from the response by exhaustively searching, like the Reader, if the number of candidate IDs is small, b) the computational complexity for the Reader identifying the ID is proportional to the product of the following two factors: the number of the Tags that the Reader manages and the number of the Tags in the area where the Reader can communicate.

6.2 Symmetric Key Cryptography based schemes

It is possible to solve problems a) and b) of Randomized Hash Lock scheme if Tags are implemented with a pseudo-random generator, a symmetric key encryption function and a non-volatile memory. The scheme with the symmetric key cryptography, hereafter called *an SKC-based scheme*, is as follows:

1. A Reader preliminarily records symmetric key k, which is common to the RFID system, to each Tag.
2. Upon receiving an ID-query, the Tag generates random number r and encrypts r and its ID with k and SE(), where SE() denotes a symmetric key encryption function. And it sends ciphertext $c = SE(k, r||ID)$ as its response to the Reader.
3. Upon receiving c, the Reader obtains $r||ID$ by decrypting c with k and extracts the ID.

[3] A one-way function transforms an arbitrary length bit string into a fixed-length one. It is easy to calculate its output from the bit string and is difficult to calculate the string from the output.

The responses sent by the same Tag are different because the Tag generates random numbers at each ID query. Moreover, an Adversary needs to break the symmetric key cryptography for extracting IDs from the responses. Therefore, it is difficult for the Adversary to guess the IDs and to confirm the links between the responses if the symmetric key cryptography adopted is secure.

6.3 Hash Chain scheme

An Adversary may record ID-queries, the corresponding responses and dates/places when recording, and store them for a long time. The Adversary will have the opportunity to confirm the link of the responses if the secret information, e.g. a secret key, is leaked in the future. Therefore, a new security feature, called *forward security*, is proposed. In this feature, it is difficult for the Adversary who obtains the leaked secret information to confirm the link of the responses. We introduce *Hash Chain scheme* which is a typical scheme to fulfill the role of this feature (Ohkubo et al., 2003). This scheme assumes that Tags are implemented with two one-way functions H() and G(). Its procedure is as follows:

1. A Reader preliminarily assigns a different key to each Tag and stores each ID and the corresponding key in the Reader's database. We describe the initial key of Tag-i as $k_{i,0}$ ($1 \le i \le n$), where n is the number of Tags managed by the Reader.
2. Upon receiving an ID-query, Tag-i calculates hash value $h_{i,0} = H(k_{i,0})$ and sends $h_{i,0}$ as its response to the Reader. And Tag-i updates $k_{i,0}$ with G() and replaces $k_{i,0}$ by $k_{i,1} = G(k_{i,0})$. The key of Tag-i is updated when receiving the queries.
3. Upon receiving the response h, the Reader calculates $h_{i,t+j} = H(G^j(k_{i,t}))$ and searches for i and j such that $h = h_{i,t+j}$, where $G^j() = G(G^{j-1}())$, $0 \le j \le s$. s denotes a range where the Reader searches for the hash value. And $k_{i,t}$ denotes the Tag-i's key recorded in the database at that time.
4. The Reader considers the sender of the response as Tag-i if matching. The key of Tag-i is $k_{i,t+j}$ at this time. The Reader replace $k_{i,t+j}$ in the database by $k_{i,t+j+1} = G(k_{i,t+j})$.

The security of this scheme is based on the difficulty of inversion of the hash functions. It is difficult for the Adversary to guess the former keys from the key obtained by the Adversary at a certain time because the keys are updated with G(). Then the scheme satisfies forward security if G() is sufficiently secure. Moreover, it is also difficult for the Adversary to confirm the link of the responses because the responses are generated by calculating the hash value of the keys with H(). However, the computational complexity for the Reader identifying the ID is proportional to the product of the following three factors: the number of the Tags managed by the Reader, the number of the Tags in the area where the Reader can communicate, and the number of the key updates which are not comprehended by the Reader. Moreover, the Tag updates its key even if a malicious Reader sends an ID-query to the Tag. The Tag's key goes out of the range in which the Reader searches if the malicious Reader sends ID-queries s times. That is, the legitimate Reader cannot identify the ID in this case.

6.4 Public Key Cryptography based schemes

We can construct a scheme which contains the following two features if Tags are implemented with a pseudo-random generator and a public key encrypting function: a) the scheme satisfies forward security, b) the Reader need not search for IDs exhaustively. The procedure of the scheme, hereafter called *a PKC-based scheme*, is as follows:

1. The Reader preliminarily writes its public key and a Tag's ID into the Tag.
2. Upon receiving an ID-query, the Tag generates a random number and encrypts the number and its ID with the public key. And the Tag sends the ciphertext as its response to the Reader.
3. Upon receiving the ciphertext, the Reader decrypts it with the Reader's secret key and extracts the ID.

An Adversary needs a Tag's ID, the Reader's public key, the responses and the random numbers used for generating the responses in order to confirm the link between the responses. The Adversary can obtain the ID and the public key by analysing the Tag, and can obtain the responses by eavesdropping upon the communication between the Reader and the Tag. The Adversary, however, cannot obtain the random numbers because the numbers are deleted when the responses are generated. Therefore, this scheme satisfies forward security if the pseudo-random generator adopted is secure. Moreover, the Reader need not search for IDs exhaustively because the Reader can obtain the IDs only by decrypting the responses. However, general public key cryptosystems (PKCs), e.g. RSA and elliptic curve cryptography, are not suitable for low performance RFID tags because of the computational complexities of such cryptosystems. Then, Suzuki et al. focus on Niederreiter PKC which is a lightweight PKC and is suitable for Tags because its encryption can be performed only with exclusive-OR in the parallel processing (Niederreiter, 1986). In addition, Suzuki et al. propose a new scheme in which the PKC is optimised suitably for the Tag (Suzuki et al., 2006).

6.5 Re-encryption schemes

Some PKCs in a specific class can update ciphertexts only with their public keys, the ciphertexts and random numbers. Of course the plaintexts of the updated ciphertexts are the same as the plaintexts of the original ciphertexts. ElGamal PKC is known as one of such PKCs (ElGamal, 1985).

A scheme, called *a Re-encryption scheme*, using such a PKC has been proposed (Juels & Pappu, 2003). This scheme assumes a Tag is implemented with a pseudo-random generator and the PKC. A Reader preliminarily writes a ciphertext of a Tag's ID and the public key of the Reader into the Tag. Upon receiving an ID-query, the Tag sends its ciphertext as its response and updates the ciphertext. The Reader can identify the ID in the same way as a Reader in a PKC-based scheme does.

The advantage of the Re-encryption scheme over the PKC-based scheme is that it does not store the plaintext of the ID in the Tag. On the other hand, the Tag cannot flexibly execute the reactions which correspond with its ID because the Tag does not know its ID. Moreover, the computational complexity of the updating is not low because the complexity is equal to that of encryption with ElGamal PKC. As a result, Juels and Pappu proposed a scheme in which the Reader updates the Tag's ciphertext and writes the ciphertext in the Tag in order to reduce the computational complexity of the Tag (Juels & Pappu, 2003). However, the Tag in the scheme needs to authenticate the Reader in order to prevent a malicious Reader from forging it.

7. Comparisons

This section compares the above schemes from the viewpoints of four security features: 1) concealment existence of Tags from an Adversary, 2) secrecy of IDs, which is the feature that

the Adversary cannot identify the IDs, 3) unlinkability, which is the feature that the Adversary cannot confirm the link between responses, 4) foward security. Table 1 shows the results of the comparisons.

"o" and "x" in Table 1 denote that the countermeasure satisfies the corresponding feature and that the countermeasure does not, respectively. The schemes with "o" concering feature 1) are some of the schemes based on the approach of not emitting the ID and signals. The majority of schemes introduced in this chapter can be represented as the mark of "o" concering features 2) and 3). The schemes with "o" concering feature 4) are a part of the schemes based on the approach of converting the Tag's ID.

The Adversary may confirm the link by sending ID-queries frequently and by tracing the source of the responses continuously if the schemes cannot conceal the existence of the Tag. It is preferable to adopt the schemes with "o" concering feature 1) for protecting against this attack. On the other hand, it may be preferable to adopt the schemes with "o" concerning feature 4) if the attack is not assumed. For example, Hash Chain scheme, PKC-based schemes and Re-encryption schemes correspond to such schemes. However, these schemes assume a Tag whose performance is middle or more.

Countermeasures \ Security features		Concealment of existence of Tags	Secrecy of IDs	Unlinkability	Forward security
No countermeasures		x	x	x	x
Destroying/detaching Tags	(Sect. 4.1)	o	o	o	x
Faraday cage	(Sect. 4.2)	o	o	o	x
Kill command	(Sect. 4.3)	o	o	o	x
Access password schemes	(Sect. 4.4)	x *a	x *a	x *a	x
Hash Lock scheme	(Sect. 4.5)	x *a	x *a	x *a	x
EPCglobal Class 1 (Quiet mode)	(Sect. 4.6)	x *b	o	o	x
LKI scheme (Silent mode)	(Sect. 4.6)	o	o	o	x
Jamming	(Sect. 5.1)	x	o	o	x
Blocker Tag	(Sect. 5.2)	x	o	o	x
Randomized Hash Lock scheme	(Sect. 6.1)	x	o	o	x
SKC-based schemes	(Sect. 6.2)	x	o	o	x
Hash Chain scheme	(Sect. 6.3)	x	o	o	o
PKC-based schemes	(Sect. 6.4)	x	o	o	o
Re-encryption schemes	(Sect. 6.5)	x	o	o	o

Table 1. Security features of each countermeasure. Grey cells show the negative features. "*a" denotes the fact that the Adversary can obtain IDs and passwords, if the Adversary eavesdrops upon communications between a legitimate Reader and the Tags. After obtaining them, the Adversary can detect the Tags, can identify the IDs and can confirm the link. "*b" denotes the fact that the Adversary may notice the existence of the Tags due to detecting the power sources.

8. Conclusions

We explained two privacy issues on RFID systems in this chapter. One is an adversary may know the items you have and the other is your locations might be traced by linking RFID responses. In addition, we explained known approaches against these issues with concrete schemes. Finally, we compared them from the viewpoint of the four security features. Some of the schemes, which do not require heavy burden on tags, have already been implemented in some current RFID products. The other schemes, however, require certain technical break through to reduce the cost for implementing them and leave themes to study.

9. References

Auto-ID Center. (2002). 860 MHz – 930 MHz Class I Radio-Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1

Auto-ID Center. (2003a). Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag

Auto-ID Center. (2003b). 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0

ElGamal, T. (1985). A public key cryptosystem and signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, IT-31, pp. 469-472

EPCglobal Inc. (2005). EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.1.0

Juels, A., Rivest, R., & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, *the 10th ACM conference on Computer and Communications Security (CCS 2003),* USA, October 2003

Juels, A. & Pappu, R. (2003). Squealing Euros: Privacy protection in RFID-enabled banknotes, *Financial Cryptography 2003*, January 2003

Liu, D., Kobara, K. & Imai, H. (2004). Pretty-Simple Privacy Enhanced RFID and Its Application, *The Seventh International Symposium on Wireless Personal Multimedia Communications (WPMC 2004)*, Italy, September 2004

Niederreiter, N. (1986). Knapsack-type Cryptosystems and Algebraic Coding Theory, *Problems of Control and Information Theory*, Vol. 15, No. 2, pp. 159-166

Ohkubo, M., Suzuki, K. & Kinoshita, S. (2003). Cryptographic Approach to a 'Privacy Friendly' Tags, *RFID Privacy Workshop*, USA, November 2003

Suzuki, M., Kobara, K. & Imai, H. (2006). Privacy Enhanced and Light Weight RFID System without Tag Synchronization and Exhaustive Search, *IEEE International Conference on Systems, Man, and Cybernetics (SMC 2006)*, Taipei, October 2006

Weis, S. A. (2003). Security and Privacy in Radio-frequency Identification Devices. *Master's thesis of Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology*

Weis, S. A., Sarma, S. E., Rivest, R. L. & Engels, D. W. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *In First International Conference on Security in Pervasive Computing*, Germany, March 2003

Yano Research Institute. (2008). Result of the survey on RF-ID market. Research Express (in Japanese)

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen