EPC Tag Authentication with Randomized Characteristics for Strong Privacy

Soohyun Oh,† and Jin Kwak††,

†Department of Information Security, Hoseo University, Korea
†† Faculty of Information Science and Electrical Engineering, Kyushu University, Japan

Summary
Recently, RFID systems have been studied actively in ubiquitous computing as main technology. While RFID systems have much advantage, however it may create new problems to the user privacy. In this paper, we present a description of previously proposed mechanisms for protecting user's privacy and these problems. Then, we propose RFID system providing privacy protection in ubiquitous computing. The proposed system provides a way of protecting user's privacy from unwanted scanning and tracking by an adversary.

Key words:
RFID, privacy, tracking, hash function

1. Introduction

RFID(Radio Frequency Identification) system is a common and useful technology in manufacturing, such as supply chain management and inventory control. It is auto identification technology that uses RF signal and under active research as the appropriate recognition system in the ubiquitous environment. The low-cost RFID tag is capable of reading or writing information of an entity without the physical contact, while it possesses a fast recognition speed, and has a relatively greater storing ability compared with bar-code. Thus, it is expected to replace bar-code in the material handling and distribution system [4, 11, 14].

However, RFID system creates new privacy problem that expose excessive information such as credit information and a purchase pattern, without them knowing. Accordingly, in order to utilize the RFID technology extensively in the industrial fields, including the material handling and distribution system, solving the relevant security problems is definitely necessary. Several method of protecting the user's privacy have been proposed, including "Kill command"[12, 13], "Blocker Tag"[7], "Hash-lock"[15], "Randomized Hash-lock"[16], "Re-encryption" [6] and "Hash-chain based protocol"[9].

Firstly, in this paper, we present a description of previously proposed mechanisms and analysis of these. Then, we propose RFID system providing privacy protection in ubiquitous computing. The proposed system

provides a way of protecting user's privacy from unwanted scanning and tracking by an adversary.

2. Related works

2.1 Introduction to RFID System

RFID system is composed of three main elements : RFID tag, RFID reader and back-end database[3, 5].

- **RFID tag or transponder** : It includes object-identifying data. Tags are generally composed of an IC chip and an antenna. The IC chip in the tag is used for data storage and logical operations, whereas the coiled antenna is used for communication between readers. Tags are divided into active tag and passive tag according to the supply of electronic power.

- **RFID reader or transceiver** : It is a device that sends an RF signal to the tag, receives the information from the tag, and sends such information to the back-end database. The reader may read and write data to the tag. In general, readers are composed of the RF module, a control unit and a coupling element to interrogate electronic tags via RF communication.

- **Back-end database** : It is the data-processing system that stores related information (e.g., product information, tracking logs, reader location, etc) with a particular tag.

The following are the general operations of the passive RFID system(see Fig. 1).

* Corresponding Author: Jin Kwak , He was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD). (KRF-2006-214-D00152).

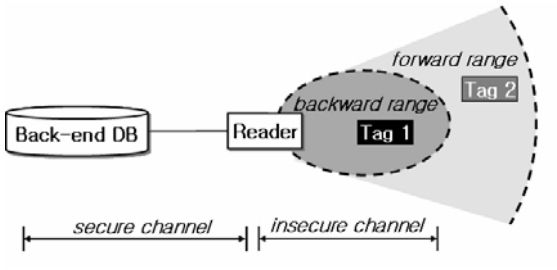

Fig. 1 RFID system

2.2 Previous RFID systems with privacy protection

In this subsection, we discuss previously suggested approaches for protecting consumer's privacy threatened by RFID Tags.

(1) Physical methods

- ***"Kill" command*** : The most straightforward approach to the protection of users' privacy is to "kill" RFID tags before it moves to the user. It is proposed by Auto-ID center in MIT and the user can deactivate a tag using "kill command"'. But a killed tag cannot be re-activated.[12,13]

- ***Faraday Cage*** : The RFID tag may be shielded using what is known as a Faraday Cage - a container made of metal mesh or foil that cannot be penetrated by RF signals.[7] But, it is inadequate for many applications because it has some limitations of size, shape and mobility.

- ***Active jamming*** : The user uses a device that actively broadcasts RF signals to block or disturb the operation of the RFID reader.[7] If the broadcast power is too high, however, this method may be illegal because it can bring about fatal consequences to all nearby RFID systems including legitimate systems where privacy is not a concern.

- ***Blocker tag*** : It is a way of protecting users from unwanted scanning of RFID tags attached to items they be carrying or wearing.[7] A Blocker tag is a cheap passive RFID device that can simulate many ordinary RFID tag simultaneously. When carried by a user, a blocker tag thus "block" RFID readers. It can do so universally by simulating all possible RFID tags.

(2) Cryptographic methods

- ***Hash-lock protocol*** : Weis et al. proposed in a tag that may be locked, such that it reject to disclose its ID until it is unlocked.[15] When the tag is locked, it is given meta-ID, and it is only unlocked by the presentation of key k such that meta-ID = h(key) for hash function h(). The tag receives a query to find the ID and sends meta-ID to the reader, and the reader sends the key k related to meta-ID. The tag then computes the hash value using received k and checks whether it is same to stored meta-ID. Only if two values are equal, the tag sends its own actual ID to the reader. But, this protocol may allow the tracking of tags, since meta-ID is static information.

- ***Randomized hash-lock protocol*** : To solve the problem of hash-lock protocol, Weis et al. proposed a randomized method of the hash function.[16] It is called Randomized Hash-Lock scheme. It requires the tag to have an additional pseudo random number generator aside from the hash function. Since the tag output data is changed in every communication, this scheme blocks tracking by unauthorized entities. Nonetheless, this scheme has a security problem, i.e., the ID is revealed in the last forward channel between the reader and the tag.

- ***Re-encryption method*** : Juels and Pappu proposed new scheme using Fujisaki-Okamoto's public key encryption to solve the privacy problem of the tag embedded in euro banknotes.[6] The serial numbers of a tag are encrypted and embedded in a euro banknote and stored data in the tag is rewritten (called "re-encryption"). Re-encryption is usually performed by an external agent because it requires heavy computation. This method prevents the tracking of tags, but it has some disadvantages such as many computational workloads and high costs.

- ***Hash-chain based protocol*** : This method is proposed by Ohkubo et al. and it is a secure authentication scheme between the reader and the tag using two different hash functions.[9] When the reader sends a query, the tag responds with a hash value. In the next communication, the tag updates the secret that is used as seed in order to generate a different response for the reader's next query. When the reader sends the tag's response to the back-end database, the back-end

database authenticates the tag by computing all tag's IDs and comparing them with the tag's response.

3. Security Requirements of RFID system

In RFID system, an attacker can capture all communications since the tag and the reader communicate through insecure channel using RF signal. Also, the reader can obtain the information stored in the tag without any physical contact. So, to widespread a RFID system, some security requirements must be satisfied.

- ***Eavesdropping*** : Even if an attacker can eavesdrop all communications of the reader and the tag, he cannot obtain the any secret information stored in a tag.

- ***Replay attack*** : Even if an attacker can eavesdrop and record all communication data of the previous session, he cannot be authenticated the legal tag to the reader using replay or modification of obtained information.

- ***Impersonation attack*** : Even if an attacker impersonates the legal reader and sends a query, he cannot know the actual serial number from the tag's response.

- ***Tracking*** : Even if an attacker can eavesdrop all communications of the reader and the tag, he cannot find the relationship from different responses.

- ***User's privacy*** : It is impossible that the reader can obtain the information on user's privacy such as credit information and purchase patterns without user's recognition.

4. The Proposed RFID System

4.1 Settings

- ***Database(DBi)*** : *DBi* is storing authentication value used for identification of tags. And it performs an authentication of tags through comparison between received information from the reader and own stored information. Fig. 2 is presented the information stored in each *DB*.

- ***Reader(R)*** : *R* transmits a RF signal to tags and sends the information received from tags to back-end database. It is not necessary of additional memory.

- ***Tag(T)*** : *T* in the proposed system stores serial number *SN*, hash function *g()*, *h()* and random number generator. *T* generates different responses for every session using random number.

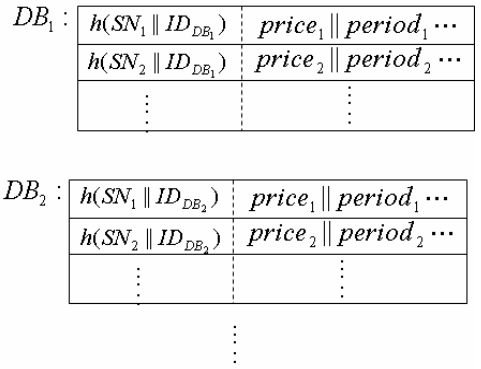

Fig. 2 : Stored information in DB_i

4.2 The identification process in the proposed system

The identification operation of the proposed RFID system between R_1 and T_1 is as follow(see Figure 3).

(1) R_1 sends a query containing connected DB's identification information to T_1.

$$R_1 \rightarrow T_1 : \text{query} = \{\text{query} \| ID_{DB1}\}$$

(2) T_1 generates a response and sends (response || r_1) to R_1.

$$T_1 \rightarrow R_1 : \text{response} = g (h (SN_1 \| ID_{DB1}) \| r_1)$$

(3) R_1 sends the received information (response || r_1) from T_1 to DB_1.

$$R_1 \rightarrow DB_1 : g (h (SN_1 \| ID_{DB1}) \| r_1) \| r_1$$

(4) DB_1 checks follow equation for all stored h(SN_i || ID_{DB1}) and finds a identical value.

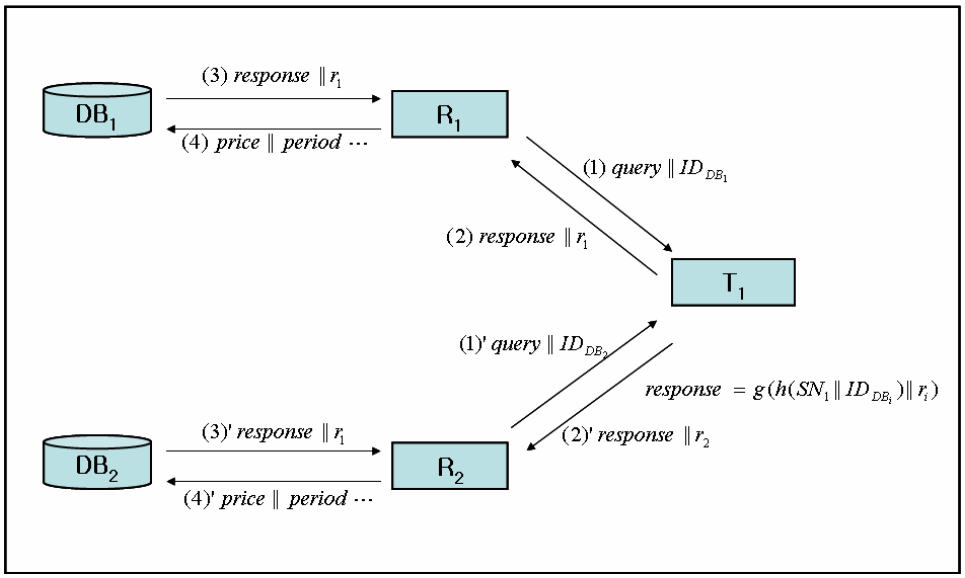

Fig. 3. The proposed RFID system

response ?= g (stored h (SN_i || ID_{DBi}) || received r_1)

(5) If DB_1 finds an identical value in (4), authenticates the T_1 and sends the related information to R_1.

$DB_1 \rightarrow R_1$: {price || valid period || … }

(6) R_1 authenticates a T_1 as valid tag and performs accounting using received information.

5. Security analysis

(1) ***Eavesdropping*** : In the proposed system, tag's response for the reader's query is hash value. So, if secure one-way hash function such as SHA-1 and MD5 is used, it is infeasible that an attacker computes serial number SN_i even if he can eavesdrop all.

(2) ***Replay attack*** : Replay attacks are divided two cases. One is that an attacker wants to impersonate the legal T_1 to R_1 with eavesdropping of previous communication. The other is that an attacker wants to impersonate the legal tag to R_2 with eavesdropping of communication of T_1 and R_1. If secure hash function is used and actual serial number is not compromised, two replay attacks are impossible.

(3) ***Impersonation attack*** : The reader does not have a computational ability or memory, and only has a limited ability of simply transmitting and receiving information in the proposed system. That is, even if an attacker can impersonate the legal reader, he cannot discover the useful information because the reader doesn't participate in storing and generation of information

(4) ***Tracking*** : In case the reader attempts tracking by collecting information transmitted from the tag, tracking by the reader is impossible since information transmitted from the same tag changes for every session.

(5) ***User's privacy*** : Reader only know that the tag is a valid or not since the actual serial number is not transmitted. Therefore, it can protect discovering of information related a user's privacy such as purchase pattern using actual serial numbers of keeping items.

6. Conclusion

In this paper, we proposed the RFID system provides protecting the user's privacy more securely compared with the existing method. The proposed system is secure

against eavesdropping, replay attack, impersonation as the reader and tracking since transmitted information is change for every session. Furthermore, it can protect discovering of information related a user's privacy because actual serial number is not.

References

[1] D. L. Brock. The electronic product code (EPC): A naming scheme for objects. Technical Report MIT-AUTOID-WH-002, MIT Auto ID Center, 2001.

[.2] D. L. Brock. EPC Tag Data Specification. Technical Report MIT-AUTOID-WH- 025, MIT Auto ID Center, 2003. Available from http://www.autoidcenter.org.

[3] D. Engels. The Reader Collision Problem. Technical Report. MIT-AUTOID-WH-007, MIT Auto ID Center, 2001.

[4] D. M. Ewatt and M. Hayes. Gillette razors get new edge: RFID tags. Information Week, 13 January 2003.

[5] K. Finkenzeller. RFID Handbook, John Wiley and Sons. 1999.

[6] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled ban- knotes. Financial Cryptography03, LNCS 2742, pp. 103-121, Springer-Verlag, 2003.

[7] A. Juels, R. L. Rivest and M. Szydlo. The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy. In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.

[8] MIT Auto-ID Center, http://www.autoidcenter.org.

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita. A Cryptographic Approach to "Privacy- Friendly" tag. RFID Privacy Workshop, Nov 2003.

[10] S. E. Sarma. Towards the ¯ve-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001.

[11] S. E. Sarma, S. A.Weis, and D. W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[12] S. E. Sarma, S. A. Weis, and D. W. Engels. Radio-frequency identi¯cation systems. Workshop on Cryptographic Hardware and Embedded Systems, CHES02, LNCS 2523, pp. 454-469, Springer-Verlag, 2002.

[13] S. E. Sarma, S. A. Weis, and D. W. Engels. Radio-frequency-identification security risks and challenges. CryptoBytes, 6(1), 2003.

[14] T. Scharfeld. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Indentification System Design. MS Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, 2001.

[15] S. A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T. May 2003.

[16] S. A.Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In First Internation al Conference on Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212

Soohyun Oh is a full-time instructor in the Department of Information Security, Hoseo University in Korea. She received the B.S. and M.S. degree in the Department of Information Engineering from SungKyunKwan University at Korea, in 1998 and 2000, respectively. She obtained the Ph.D degree in school of Information and Communication at Korea, in 2003.

Jin Kwak received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 2000, 2003, and 2006 respectively. He is currently a visiting scholar of Faculty of Computer Science and Communication Engineering of Kyushu University in Japan. Also he is currently special researcher of Kyushu Institute of System and Information Technologies in Japan. His main research areas are cryptography and ubiquitous computing security, particularly regarding the design of secure RFID system in ubiquitous network.