Security and Privacy on Authentication Protocol for Low-Cost RFID

Yong-Zhen Li[1], Young-Bok Cho[1], Nam-Kyoung Um[1], and Sang-Ho Lee[2,⋆]

[1] Department of Computer Science, Chungbuk National University, Cheongju, Chungbuk, Korea
{lyz2003,bogi0118,family}@chungbuk.ac.kr
[2] School of Electrical & Computer Engineering, Chungbuk National University, Cheongju, Chungbuk, Korea
shlee@chungbuk.ac.kr

Abstract. The Radio Frequency Identification (RFID) is an automatic identification system, relying on storing and remotely retrieving data about objects we want to manage using devices called RFID tag. Even though RFID system is widely used for industrial and individual applications, RFID tag has a serious privacy problem, i.e., traceability. To protect the users from tracing and also to support Low-cost RFID, we propose an authentication protocol which can be adopted for read-only RFID tag using XOR computation and Partial ID concept. The proposed protocol is secure against reply attacking, eavesdropping, and spoofing attacking so that avoiding the location privacy exposure.

1 Introduction

The Radio Frequency Identification (RFID) is an automatic identification system, relying on storing and remotely retrieving data about objects we want to manage using devices called RFID tag. A secure RFID system has to avoid eavesdropping, traffic analysis, spoofing and denial of service, as it has large read range and no line of sight requirement. There have been some approaches to the RFID security and privacy issues, including killing tags at the checkout, applying a read/write able memory, physical tag memory separation, hash encryption, random access hash, and hash chains [1].

The RFID technique, however, causes the serious privacy infringement, such as excessive information exposure and user's location information tracking, due to the wireless characteristics because it is easy to be recognizable without the physical contact between the reader and the tag while the tag information is sent[3,4]. These concerns become the setbacks to the embodiment of RFID, and the various privacy problems should be solved beforehand for the successful industrialization. Therefore, the research regarding the authentication protocol are now proceeding actively to protect the information stored in the tag and resolve the safety problems such as the location tracking of the tag [4].

⋆ Corresponding author.

Y. Wang, Y. Cheung, and H. Liu (Eds.): CIS 2006, LNAI 4456, pp. 788–794, 2007.

This paper is organized as follows. We describe RFID security and privacy problems in section 2. Then our approach is proposed in section 3. In this section, the assumption is stated. Under this assumption, the basic idea is presented and the working mechanism is detailed. We compare our scheme with other schemes about security and efficiency in Section 4. In the final section, we provide a summary of our work.

2 RFID Security and Privacy

2.1 Privacy

Privacy and cloning of tag must be solved for proliferation of RFID technology. Because everyone can query to a low-cost tag (which doesn't have an access control function, e.g., Class I tag) without recognition of the tag holder, privacy must be considered [1,5].

One of privacy problems is the information leakage on user's belongings. People don't want that their personal things are known to others. For example, exposure of expensive products can make a tag holder be a victim of a robber. A personal medicine known to another throws the user into confusion. Even though the information leakage problem is significant, it's easy to solve. It can be solved just by using the anonymous ID's that DB only can match with the real product codes [1,4].

Another problem about the user privacy is a user tracing problem. By tracing tag, adversary can chase and identify the user. If adversary installs a vast amount of R's at a wide area, each individual person's location privacy is violated by adversary. The user tracing problem is hard to solve, because we must update every response of tag in order to evade a pursuer while a legitimate user can identify tag without any inconvenience. Moreover, this job must be performed by tag with small computational power [5,12].

2.2 Authentication

For the security and privacy problems in RFID, we usually solve the mutual authentication between tag and reader by the approaches of random ID, hash or cryptography. In the following we will introduce several general RFID authentication protocols.

Hash Lock. The scheme [1] stores the hash of a random key K as the tag's meta-ID, i.e. meta-ID = h(K). When queried by a reader, the tag transmits its meta-ID. The database and the reader respond with K. The tag hashes the key and compares it to the stored meta-ID. Although this scheme offers good reliability at low cost, an adversary can easily track the tag via its meta-ID for its a certain value. Furthermore, since the key K is sent in the clear way, an adversary capturing the key can later spoof the tag to the reader.

Randomized Hash Lock. The scheme [1] is that each tag has its own ID and a random number generator to make its constant variable randomized. The tag

picks pseudo random number r uniformly and calculates c = hash(ID —— r) as the tag's unique identification for every session. The tag transmits its c and r to a back-end server by way of the reader. By the way of comparing c with the construction of r and all IDs that are stored in database of the server, the server authenticates itself by sending the unique identifier ID back to the tag.

Hash Chain. In [6], Okubo et al. proposed hash-chain based authentication protocol which protects users' location privacy and anonymity. They claim that their scheme provides strong forward security. However, hash-chain calculation must be burden on low-cost RFID tags and gives back-end servers heavy calculation loads.

Re-encryption. The method uses public key cryptosystem[9]. Tag data is re-encrypted when a user requires using the data transferred from an external unit. As public key encryption needs high computation cost, a tag cannot process for itself. Thus, this job is generally processed by a reader. Each tag data is randomly shown until next session, the attacker eaves dropping the tag data cannot trace the tag for long-term period. However, this method has difficulty to frequently refresh each tag's data since the encrypted ID stored on tag is constant so that user location privacy is compromised. This job is processed by users (or tag bearers) and is considered impractical.

Low-Cost Authentication. In [10, 11], a security model is proposed that introduces a challenge-response mechanism which uses no cryptographic primitives (other than simple XORs). One of the key ideas in this work is the application of pseudonyms to help enforce privacy in RFID tags. Each time the tag is queried, it releases the next pseudonym from its list. In principle, then, only a valid verifier can tell when two different names belong to the same tag. Of course, an adversary could query a tag multiple times to harvest all names so as to defeat the scheme. So, the approach described involves some special enhancements to help prevent this attack. First, tags release their names only at a certain prescribed rate. Second, pseudonyms can be refreshed by authorized readers. Although this scheme does not require the tags to perform any cryptographic functions (it uses only XOR operations), the protocol involves four messages and requires updating the keys and pads with new secrets.

3 Proposed Authentication Protocol

3.1 The Initialization Stage

At first, make every tag each own secret information, SID (secure ID), and store the corresponding information to the database; Secondly, install in the reader the random number generator which can generate pseudo random numbers; Finally, establish the random length of the PID used for a mutual authentication of the next reader and tag; We find that the length of n1 and n2 has the $2L \geq n1 + n2 \geq L/2$property.

3.2 The Detail of Proposed Protocol

The proposed protocol comprises of 4 steps as shown in the figure 1.

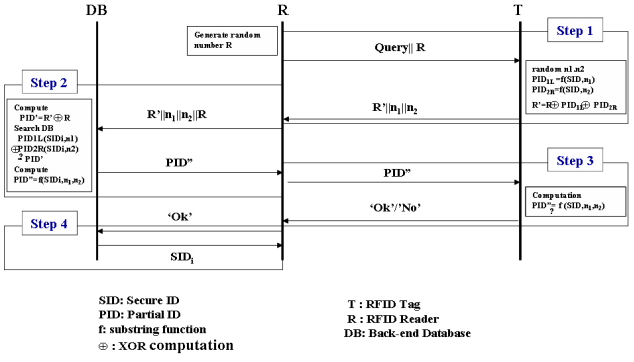

Fig. 1. Proposed protocol

Step 1 : Generating PID

- The readers generate the random number and send them to the tag along with the inquiry information.
- In its own SID, the tag selects 2 PIDs, and each length of PIDs is determined randomly. PID_{1L} is selected from the start location of SID, and PID_{2R} is from the end. Then calculate R by XORing PID_{1L}, PID_{2R} and R received from the reader.
- The tag sends to the reader the calculated R and two parameters n_1,n_2, which respectively mark the length of PID_{1L}, and PID_{2R}.

Step 2 : Searching SID and Tag Authentication

- The reader sends to the database the random number R generated above and R received from the tag and n1, n2.
- The database calculates the tags PID, by XORing R and R received from the reader; And by using the calculated PID, the database searches for the every tags SID making this PID exactly equal to the value XORing PID_{1L} (selecting the part from the start location of SIDi to the location of n1) and PID_{2R}(selecting the part from the location of n2 to the end location of SIDi) and collects the value of PID, which is selected from the location of n1 to the location of n2 in the searched SIDs; acknowledges the tag as a disguised one, if there is no SID filling the requirements of the PID as a result of search.
- Sends to the reader the collected PID values;

Step 3 : Reader Authentication

- The reader sends the collected PID values to the tag;
- The tag judges if the value of selected in SID from the location of n_1 to the location of n_2 is identical to the PID values received from the database; acknowledges the reader disguised if they are not identical;

– The tag sends to the reader the PID Ok, if it finds PID identical to the value of selected in SID from the location of n_1 to the location of n_2. Otherwise, it sends to the reader the no find information;

Step 4 : Return Result

– The reader sends to the database the information received from the tag, if it is Ok. And it terminates the protocol if it received the No find information;
– The database provides the collected SID information for the reader.

4 Analysis

4.1 Security Analysis

Safety Against Location Privacy. The user's privacy mainly means the leakage of location information or tag information of the tag's owner. The messages sent and received between the tag and the reader is transmitted as different messages each time during all the authentication procedures. It is impossible to track the tag's location through the previous unchanged messages, because different messages are exchanged each time due to the sending of the randomly selected PID. However, the tag's location can be estimated even though different messages are sent each time, in case the tag's SID is known. The tag tracking for a special purpose (legal investigation) becomes possible through the administrator's authorization;

Safety Against Spoofing Attack. In most cases, the symmetry key cipher technique is used to guarantee the secrecy of sent messages. However, is costs too much to use such cipher techniques because the storing space and computation capability of RFID tag is limited. In the proposed protocol, the secrecy of the messages sent and received during the authentication procedure is guaranteed, by concealing and sending the sent message (PID) through the bit computation with random numbers. That is, the PID of the sent tag can be calculated, only if the random number and its own PID information is known. It is safe against the message eavesdropping attack, because it is impossible to calculate the tag's overall SID even though the PID is exposed.

Safety Against Reply Attack. There are two kinds of attack; resend attacks disguised as a reader and as a tag. In case of disguising as a reader, the attacker eavesdrops on the message sent from the reader to the tag and resends it. In the proposed protocol, the resend attack is prevented by establishing the pseudo random number R, n1 and n2.

Through the above security analysis, we can know that the authentication protocol proposed in this paper solve the secure problems of spoofing attack, reply attack and user location tracking.

4.2 Efficiency

In the RFID system, power consumption, processing time, memory space and gate number work as main variables. Therefore, it is very important to decrease the above 4 elements in embodying the RFID system of low cost. Comparing the hash and cryptography approaches, which both cost 20,000 30,000 gate numbers, the Juels and Eunyoung approaches only cost 500 5000 gate numbers. So we need only compare our scheme with the more efficient methods. The table 1 shows a result of comparing and analyzing the Juels[10] and Eun-young[11] techniques and proposed protocol.

	Juels[10]	*Eunyoung*[6,9]	Our Scheme
Memory	k*L	2L	1L
Computation	4k (XOR)	8(XOR)+4(+)	4(XOR)
Write Op	k*L	L	Unused

k: number of secure key(4 or 5); + : module addition;
L: Length of SID

As shown in the table 1, the proposed protocol makes the tag's computation quantity evidently decrease in comparison with the Juels and Eun-Young techniques [10,11]. Also our protocol decreases memory requirement to half (from 2L to L) of the Eun-Young arithmetic, and the chief bit computation decreases to 1/3 (8(XOR)+4(+)4(XOR)). Furthermore, the write operation is not needed in tags during the authentication procedure. Besides, in the RFID system, it is not realistic to reserve the additional space for writing computation and storage. And while the information protection of RFID system using the tag only for reading is previous possible through the physical approach, it is so through the software method in the proposed protocol, which is an evidence of superiority over the previous techniques.

5 Conclusions

Previous RFID techniques cause serious privacy infringements such as excessive information exposure and user's location information tracking due to the wireless characteristics and the limitation of RFID systems. Especially the information security problem of read-only tag has been solved by physical method. This paper proposes the mutual authentication protocol of low cost using the simple XOR computation and PID concept, which is applicable to the fields of logistics activity, medicine transfer management with the read-only tag. Furthermore proposed authentication protocol decreases memory requirement to half of the Eun-Young arithmetic, and the chief bit computation is decreased to 1/3. Furthermore, the write operation is not needed in tags during the authentication procedure. Therefore the proposed protocol supports major desirable security features of RFID systems such as implicit mutual authentication, traffic encryption and privacy protection.

References

1. Weis, S.A., Sarma, S., Rivest, R., Engels, D.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)
2. Juels, A., Pappu, R.: Squealing Euros: Privacy protection in RFID-enabled banknotes. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 103–121. Springer, Heidelberg (2003)
3. Molnar, D., Soppera, A., Wagner, D.: A scalable delegatable pseudonym protocol enabling ownership transfer of RFID tags. In: Preneel, B., Tavares, S. (eds.) Selected Areas in Cryptography-SAC 2005. LNCS, Springer, Heidelberg (2005)
4. Henrici, D., Muller, P.: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshop, PERCOMW '04, pp. 149–153. IEEE Computer Society Press, Los Alamitos (2004)
5. UHF wireless tag, Auto-ID Center, http://www.autoidcenter.org/research/mit-autoid-tr007.pdf
6. Ohkubo, M., Suzuki, K., Kinoshita, S.: A Cryptographic Approach to 'Privacy-Friendly' tag, RFID Privacy Workshop (November 2003)
7. Yoshida, J.: RFID Backlash Prompts 'Kill' Feature, EETimes, (April 28 2003)
8. Juels, A., Rivest, R.L., Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103–111 (2003)
9. Golle, P., Jakobsson, M., Juels, A., Syverson, P.: Universal re-encryption for mixnets. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 163–178. Springer, Heidelberg (2004)
10. Juels, A.: Minimalist cryptography for low-cost RFID tags. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 149–164. Springer, Heidelberg (2005)
11. Choi, E.Y., Lee, S.M., Lee, D.H.: Efficient RFID Authentication protocol for Ubiquitous Computing Environment. In: Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., Yang, L.T. (eds.) International Workshop on Security in Ubiquitous Computing Systems - secubiq 2005. LNCS, vol. 3823, pp. 945–954. Springer, Heidelberg (2005)
12. Avoine, G.: Radio frequency identification: adversary model and attacks on existing protocols, Technical Report LASEC-REPORT-2005-001, EPFL, Lausanne, Switzerland (September 2005)