M-019

Proxy-based privacy protection for RFID system

Toshiharu Sugiyama† Hiroaki Hagino† Kenichi Yamazaki†

1. Introduction

RFID (Radio Frequency IDentification) systems use radio-communications and are effective in realizing the ubiquitous computing environment. An RFID system enables a computer to automatically detect the objects around a person and to infer the environment around the person from the set of objects detected.

From the viewpoint of cost, it is said that an RFID tag should have only primary functions such as "store only own ID" and "always reply to request" [1]. However, such RFID tags open the user to severe privacy attacks. In fact, some associations insist that RFID systems will lead to the controlled society with no freedom [2]. The basic RFID tag cannot deny access from any RFID reader and always responds with its ID. This is the most significant factor degrading privacy. If a wallet carried by a user has a basic RFID tag, the location of the RFID tag indicates the location of the user. Any reader can detect the RFID tag, i.e. the location of the user, so if a malicious user collects RFID tag ID by placing some readers, he can easily track the user.

In the ubiquitous computing environment, the RFID reader will be also pervasive. Then, to protect the location of the RFID reader is also important. Without solving the problem of tracking the user's RFID reader, the privacy protection is insufficient.

The scheme proposed in this paper solves this problem as well as the related problem of tracking the user's RFID reader.

2. Privacy weakness of RFID systems

In the Auto-ID system [1] any basic tag can be read by any common reader because the tag has no authentication function. In [3, 4], it is said that there are two privacy threats.

a) User tracking

b) Information leak

Since the information leak can be solved by controlling access to the information databases, we focus on user tracking.

We consider the ubiquitous computing environment with a comprehensive RFID system. RFID tags are attached to all objects in the real world and each user has his/her own database server which holds profile information of his/her own objects. We believe that there are two kinds of RFID reader in the ubiquitous computing environment. One is set in public spaces and provides push type services to approved users. The other is mounted in portable terminals. A user carries one such portable terminal and is always able to own and public objects around him/her. Since each personal RFID reader has its own ID, to permit reader authentication, the reader's ID can be used to identify and track the user. That is, to fully solve the user tracking problem, we must prevent reader tracking as well as RFID tag tracking.

† Network Laboratories NTT DoCoMo Inc.

2.1 RFID tag tracking

In the Auto-ID system [1], since an RFID tag has a globally unique ID, a malicious user can detect when the user passes a certain point by setting a reader at that point.

To achieve RFID tag tracking, an attacker needs the following three pieces of information.

T-1. Victim's RFID tag ID or DB ID

T-2. Attacker's RFID reader ID

T-3. Association of physical information and IDs in RFID system (attacker's reader ⇔ location, user ⇔ RFID tag ID)

To prevent RFID tag tracking, user must prevent the attacker from collecting all three pieces of information. Since the RFID reader is placed by the attacker, it is difficult to conceal T-2 from the attacker. T-3 is also difficult to conceal because the attacker can easily get it from the real world. Therefore to avoid RFID tag tracking, we must conceal T-1 from the attacker.

Related works include the blocker tag [6], the Kill tag approach [1], the faraday cage approach [5], the active jamming approach [6] and the smart tag approach [3, 4]. Since the first three disable the tag's functionality, the smart tag approach is the most user-friendly. The smart tag approach uses variable IDs but it is not really practical since a malicious user can change IDs; tags have no authentication function and it is difficult to synchronize the information linking tags to the DB. Moreover, none of these approaches considers the need to shield the identity of the user's DB. Accordingly, this paper introduces a fully secure system based on encryption. This system enable RFID reader to correspond with RFID tag's DB with shielding the identity of the user's DB. DB logically distribution is possible in our proposal system. Then, the user can have own database without tracking by identity of DB.

2.2 RFID reader tracking

Since the RFID tag's ID and DB identity should be concealed, the RFID reader cannot judge whether the RFID tag and the DB can be trusted or not. If the RFID reader passes its own identifier to the DB, the RFID reader itself can be tracked.

RFID reader tracking requires the attacker to gather three items.

R-1. Victim's reader ID

R-2. Attacker's tag ID

R-3. Association between physical information and IDs in RFID system (attacker's tag ⇔ location, reader⇔ user)

Since the RFID tag is placed by the attacker, it is impossible to conceal R-2 and R-3. The key to preventing RFID reader tracking is to conceal R-1 from the attacker.

3. PPPR

We propose PPPR (Proxy-based privacy protection for RFID system) to prevent both RFID tag tracking and RFID reader tracking. PPPR has two main features.

1. PPPR uses a proxy-server to support DB logically distribution even though the RFID tag's ID is concealed.

2. PPPR uses a trusted DB's public key to encrypt the RFID reader's authentication information.

3.1 PPPR architecture

The architecture of PPPR is shown in Fig.1. Since the RFID tag responds by releasing a variable encrypted message, the RFID reader cannot get the RFID tag's identifier or DB identifier. To overcome this lack of information, PPPR uses a proxy-server named IDRS (ID Resolution Server). IDRS extracts the tag's ID and the corresponding DB ID from the RFID message; it then interacts with the DB on behalf of the RFID reader. Then, since the DB identifier is shielded by IDRS, the user can have own DB without tracking via DB ID

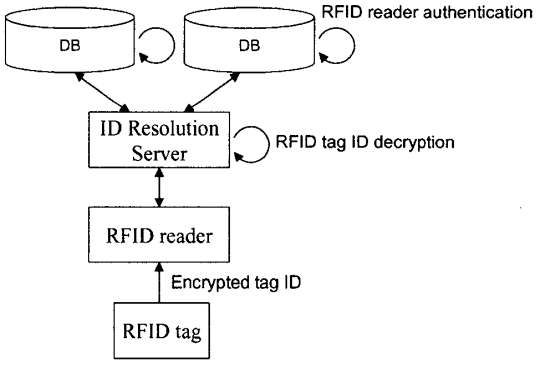

Fig.1 Architecture of PPPR

3.2 Message formats

The message formats shown in Fig. 2 are used. The tag message consists of RFID tag ID, tag DB ID, and a random text. The random text makes the message variable. The message is encrypted using the IDRS's public key.

The reader message consists of tag message, reader ID, password, and time stamp. The time stamp is effective for not only validating the date but also randomizing the message. The reader message is encrypted using the trusted DB's public key.

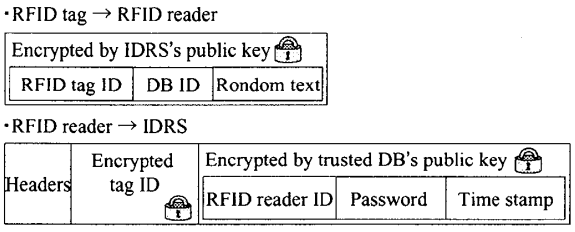

Fig.2 Message format

3.3 PPPR Procedure

The PPPR procedure is shown in Fig.3.

1. The RFID reader gets the RFID tag's message, which is encrypted by the IDRS's public key.
2. The RFID reader encrypts own authentication information using trusted DB's public key and transmits it to IDRS with the tag's message.
3. The IDRS decrypt tag's ID and identifies the DB that has RFID tag's information. The IDRS polls the tag's DB to acquire the tag's information.
4. The DB system authenticates the RFID reader.
5. The tag's DB transmits tag information to the IDRS and the IDRS forwards it to the RFID reader.

If reader authentication fails, the DB system releases only public information.

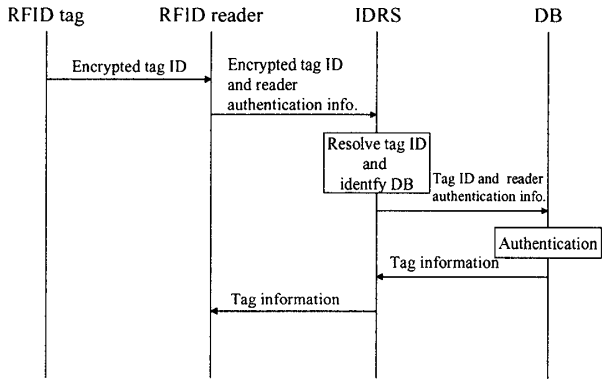

Fig.3 PPPR Procedure

3.4 PPPR impact

PPPR provides complete safety since it prevents the attacker from gathering the key data of T1 and R1. IDRS makes it impossible for the attacker to readily find the associations needed. Therefore, the user tracking problem is solved by PPPR.

4. Summary

In this paper, we described the user privacy problems raised by the use of RFID systems in the ubiquitous computing environment and proposed the countermeasure of PPPR. PPPR supports DB logically distribution and avoids user tracking via RFID tags or RFID readers.

References

[1] EPC Global, http://www.epcglobalinc.org/
[2] C.A.S.P.I.A.N, http://www.nocards.org/
[3] Shingo Kinoshita, Fumitaka Hoshino, Tomoyuki Komuko, Akiko Fujimura and Miyako Ohkubo, "Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection", NTT Information Sharing Platform Laboratories, Computer Security Symposium 2003.
[4] Miyako Ohkubo, Kourarou Suzukiy and Shingo Kinoshita, "Forward-secure RFID Privacy Protection for Low-cost RFID", NTT Information Sharing Platform Laboratories, Computer Security Symposium 2003.
[5] "インターネットの不思議，探検隊！", Jun Murai, TaroJiro co,.ltd, 2003 Sep.
[6] A. Juels, R. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In submission. 2003