International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:10, 2007

Tag Broker Model for Protecting Privacy in RFID Environment

Sokjoon Lee, Howon Kim, and Kyoil Chung

***Abstract*—**RFID system, in which we give identification number to each item and detect it with radio frequency, supports more variable service than barcode system can do. For example, a refrigerator with RFID reader and internet connection will automatically notify expiration of food validity to us. But, in spite of its convenience, RFID system has some security threats, because anybody can get ID information of item easily. One of most critical threats is privacy invasion.

Existing privacy protection schemes or systems have been proposed, and these schemes or systems defend normal users from attempts that any attacker tries to get information using RFID tag value. But, these systems still have weakness that attacker can get information using analogous value instead of original tag value.

In this paper, we mention this type of attack more precisely and suggest 'Tag Broker Model', which can defend it. Tag broker in this model translates original tag value to random value, and user can only get random value. Attacker can not use analogous tag value, because he/she is not able to know original one from it.

***Keywords*—**Broker, EPC, Privacy, RFID.

I. Introduction

RFID system, in which we give identification number to each item and detect it with radio frequency, supports more variable service than barcode system can do. For example, some application services are possible in enterprise, such as WMS and ERP. Manufacturer and warehouse manager can easily find out the location, state and information of specific item, and deal with product orders or inventory. For customers, a refrigerator with RFID reader and internet connection will automatically notify expiration of food validity to them. In case of electronic products, they can access after-sale service information or online user manual.

But, in spite of its convenience, RFID system has some security threats, because anybody can easily get or counterfeit ID information of products. One of the most critical threats is privacy invasion [1, 2, 3]. Attacker with RFID reader can see RFID tag values of items that people carry in their body, wallet or bag. With simple operation, attacker can find out their privacy information, which can be sexual taste or richness.

So, to eliminate this undesirable side effect, RFID privacy protection problem is one of the most important issue. To solve this problem, Privacy policy management scheme or systems [4] have been suggested. These schemes or systems defend normal users from attempts to get information using RFID tag value. But, these methods still have weakness that attacker can get information using analogous value instead of original tag value.

In this paper, we mention this type of attack more precisely and suggest 'Tag Broker Model', which can defend it. Tag broker in this model transform original tag value to random tag value, and user can only get random tag value. Attacker can not use analogous tag value, because he/she is not able to know original one.

Section II gives background of RFID systems. Section III states brief description of privacy problems. In addition to background and privacy issues, 'Tag Broker Model' is introduced in Section IV. Finally, we conclude and discuss future works in Section V.

Manuscript received November 15, 2005.

Sokjoon Lee, Howon Kim, and Kyoil Chung are with the Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea (phone: 82-42-860-5455; fax: 82-42-860-5611; e-mail: {junny, khw, kyoil}@etri.re.kr).

II. Background

A. EPCGlobal

EPCglobal[5] is developing industry-driven standards for the Electronic Product Code (EPC) and its related specification to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks. The goal of EPCGlobal is to support visibility and efficiency throughout the supply chain, and to offer variable application service to companies and their partners.

EPCGlobal has five components, which are EPC code, ID systems, middleware, discovery service, information service. Fig. 1 shows its network architecture.

B. Mobile RFID Service

Mobile RFID Service means that RFID infrastructure is merged into mobile phones and networks, which spread abroad and are widely used, so as to create new RFID-related service. In the mobile RFID service, RFID tag value and its transformed URI are regarded as a kind of hypertext.

While fixed RFID readers are used in the existing RFID infrastructure, anyone can use RFID reader embedded in mobile phone in the mobile RFID service. For example, we can read the tag of exhibit in the exhibition hall, get its information using wireless internet, and then buy it from selling menu on mobile phone.

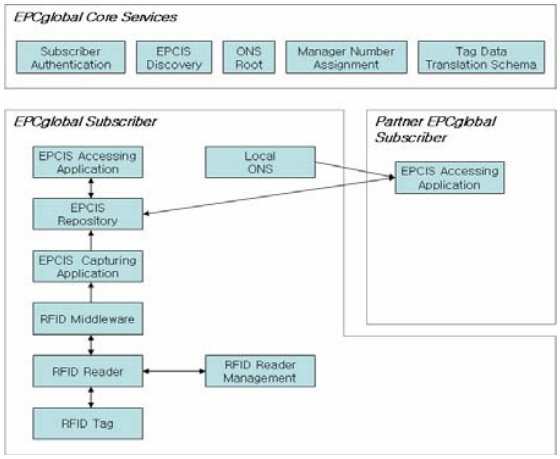

Fig. 1 EPCGlobal Network Architecture

Moreover, in conjunction with SCM, it is possible to provide more variable service. With mobile phone with RFID reader, we can search for electronic product records (production date, factory information, price and so on), purchase electronic device, and access after-sale service information or online user manual if necessary.

But, because of its mobility and portability, security threats become more severe problems in this service. Attacker can access tag value of someone's possessions at anytime and anywhere.

Fig. 2 shows mobile RFID service architecture including privacy policy management system, which is introduced in the next part C.

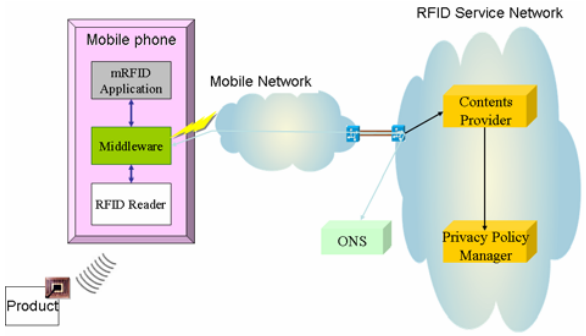

Fig. 2 Mobile RFID Service Architecture

C. Privacy (Policy) Management System

Therefore, if there is privacy policy management system in mobile RFID service, we can solve some privacy problems. The system collaborates with contents provider or EPCIS. If a customer purchases some products, the sale event will be notified to privacy manager. When any attacker near the customer probes RFID tags, detects the tags of his/her own products and wants to find out products information using contents provider, the systems will give signals to contents provider that the products is not owned by the attacker.

Thus, this system blocks off attackers or user that try to get the privacy information of other people with its policy.

III. Privacy Threats in RFID Service

It is explained in Section I, how the situation that any user can easily access RFID tags is privacy invasion. Generally the problem would not arise only if product information and records are to be accessed by the owner of it.

To give solutions, first choice is that RFID tag gives its ID value to authenticated reader. But this choice will not be good because of tag and reader production expenses. Second choice is the use of 'kill' or 'lock' command. This method is no better than first one, because the 'kill' or 'lock' password is too short generally and it is very simple to crack it. So, we need privacy management system, described in Section II. The system blocks off any attempt to get the privacy information of other people.

However, there is still remained privacy threat. Most RFID code systems (tag encoding scheme) such as EPC-TDS[6], ISO15963[7], etc, don't have randomness. For example, EPC GID-96 is composed of several fields – header, company number, object classifier, and serial number. Using this aspect, an attacker comes to know item information corresponding tag value without much effort.

Also, he/she can try to access contents server with the analogical value which is equal to original tag in all fields but not in serial number. If the item with modified value is not sold, contents provider will return the information of item for selling purpose. Thus, attacker can know privacy data such as the price of item, its brand, etc. This problem results from the absence of randomness in RFID code system.

To solve this, we propose 'Tag Broker Model'. Tag broker translate tag pseudonym from original tag value in production step, and retranslate it when user requests. The same type of items will have entirely different tag value.

IV. Our Solution – Tag Broker Model

As mentioned in Section III, there are still some privacy threats using analogical tag value, even if privacy policy management of item information with specific tag value is possible. So, we introduce 'Tag Broker Model' for protecting this type of threat in this section.

A. Tag Broker

Tag broker make contract with product manufacturer to create tag pseudonym. Product manufacturer manages original tag value and its related contents provider. Tag broker does not need to maintain all tag pseudonyms, while it has tag translation rule. The rule will be explained in part B. Fig. 3 shows tag broker model, merged in mobile RFID service architecture.

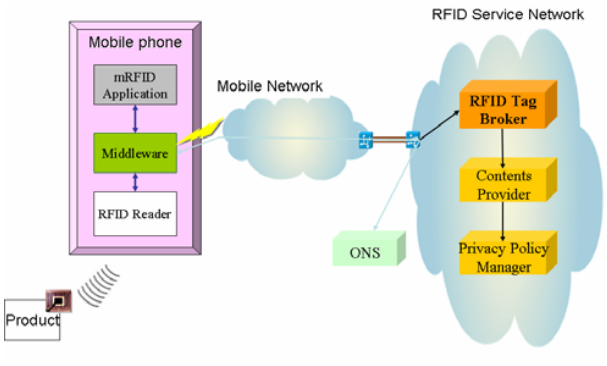

Fig. 3 Mobile RFID Service Architecture

The scenario within tag broker model is as follows:

1) Manufacturer, which made contract with tag broker, obtains tag pseudonyms when it attaches RFID tag to its products.
2) User with RFID reader detects tag pseudonym from any item, and then tries to get internet address of the item information from ONS server.
3) ONS server returns the address of tag broker.
4) RFID reader transmits tag pseudonym and user profile to tag broker.
5) After tag broker receives tag pseudonym from RFID reader, translate it to original tag value. Tag broker request the item information to contents provider or EPCIS with original tag and user profile.
6) Contents provider or EPCIS responses the information which is permitted to the user.
7) Tag broker returns the response.

Of course, user cannot find out original tag value from tag pseudonym in this scenario.

B. Tag Pseudonym

Tag Pseudonym must have randomness such that attacker cannot use analogical tag value improperly. Anyone without tag broker cannot find out original tag value from pseudonym. The formation of tag pseudonym compatible with EPC is as shown below:

Tag Pseudonym (160bits) = Header (8 bits) +
Tag Broker Number (12 bits) +
Tag Broker Key Id (12 bits) +
Modification of Original Tag Value (128 bits)

- **Header**: identical with EPC code header. We can use one of reserved value for future use.
- **Tag Broker Number**: for identifying Tag Broker Company. Maximum 4096 Tag Broker Companies are possible.
- **Tag Broker Key Id**: used for identifying Tag Broker Key. Tag Broker uses Tag Broker Key for transformation of 'Original Tag Value' into 'Tag Pseudonym', which would be secure encryption key, such as an AES key.
- **Modification of Original Tag Value**: encrypted value of Original Tag Value using Tag Broker Key. Tag Broker must be able to find out Original Tag Value using this value and Tag Broker Key, inversely. We can use AES encryption scheme as transformation method.

This model has weakness that it is impossible to use tag pseudonym if RFID tag memory size is smaller than 160 bits. In another example of EPC Class 1 Gen 2 specification [8], if EPC memory size is smaller than 160bits, it is possible to save some part on USER memory area.

C. Example of EPC GID-96 Tag Translation using AES

When tag broker translate tag pseudonym from EPC GID-96 typed value, the broker takes the procedure in Fig. 4.

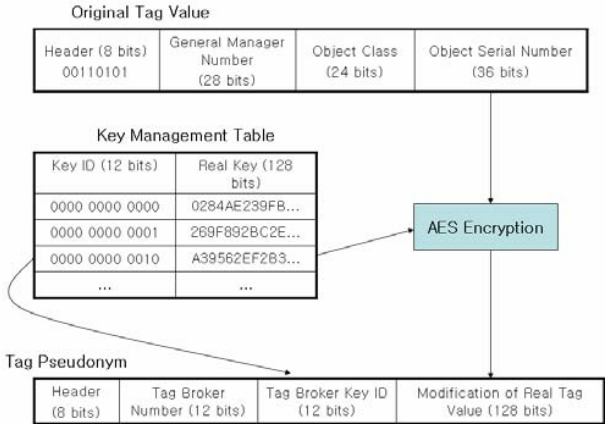

Fig. 4 Translation Tag Pseudonym from EPC GID-96 Tag

Inversely, when tag broker retranslate original EPC GID-96 tag value from tag pseudonym, the broker takes the procedure in Fig. 5.

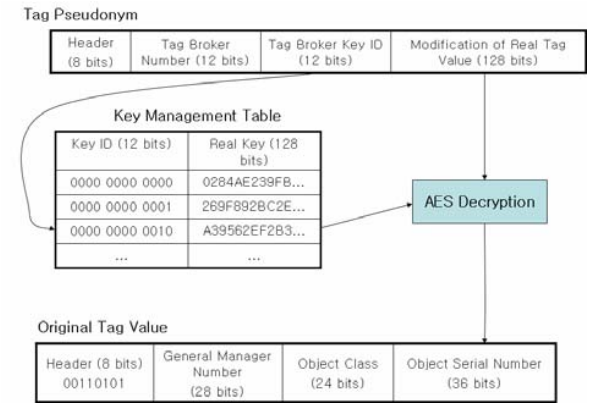

Fig. 5 Retranslation EPC GID-96 Tag from Tag Pseudonym

V. Conclusion

Currently, RFID services are applied to the restrictive area such as SCM and WMS. But its ability of auto-detecting using radio frequency makes application service increased. However, though its convenience, there is still remained some problems, which come to be setbacks to RFID service deployment. Especially privacy threat is one of the most critical issues.

In this paper, we discussed the privacy issue and suggested 'Tag Broker Model', which has the capability of blocking any privacy related attack. As our model uses 'Tag Pseudonym' concept, anybody without manufacturer and tag broker cannot get original tag value. If attacker cannot see the original value, he/she cannot also guess analogical one at all, therefore he/she is not able to find out any product information.

The translation method of this paper is to give cryptographic relationship between original tag and tag pseudonym. With this method, if tag broker maintains key management table indexed by key ID, the broker can translate/retranslate any value. But variety of this translation method is also possible. For instance, the broker can make table to maintain original tag value-tag pseudonym pairs. Here we don't need to have cryptographic relationship between them. If the broker uses this method, the "Modification of Original Tag Value" in part B, section IV, can be smaller than 128 bits such as 64 bits. Then the whole size of tag pseudonym can be 96 bits, and this is equal to currently distributed tag size. The proper translation method would be selected and applied, according to RFID tag memory size, RFID tag encoding scheme, interface between tag and reader, etc.

As RFID chip price is decreased and computing power is increased gradually, cryptographic operation such as encryption, hash and authentication will be possible on the RFID tag. Many researchers try to work out privacy issues using tag ability. We are interested in this field for the future works. We are also concerned in RFID intrusion detection method in the infra-network.

References

[1] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags", RFID Privacy Work-shop, 2003.
[2] Ari Juels, Ronald L Rivest, and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", 10th ACM Conference on Computer and Communications Security, 2003.
[3] Stephen A. et al., Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Security in Pervasive Computing 2003, LNCS 2802, 2004, pp. 201–212.
[4] Byungil Lee and Howon Kim, "Enhanced Security and Privacy Mechanism of RFID Service for Pervasive Mobile Device", CIS(Computational Intelligence and Security) 2005, LNAI 3802, Dec. 2005.
[5] EPCglobal, http://www.epcglobalinc.org/
[6] EPC Tag Data Standards Version 1.1 Rev.1.24, Apr. 2004.
[7] Information technology – Radio frequency identification for item management – Unique identification for RF tags, ISO/IEC 15963, Sep. 2004.
[8] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.7,Sep. 2004.