A Design of Privacy Conscious RFID System Using Customizing Privacy Policy Based Access Control

Byungil Lee and Howon Kim

Electronics and Telecommunications Research Institute, Korea,
161 Gajeong-dong, Yuseong-gu, Daejeon, Korea
{bglee, khw}@etri.re.kr
<http://www.etri.re.kr>

Abstract. Recently, research related to RFID technology has progressed vigorously for the ubiquitous world. However, the privacy violation on tags embedded in products has become a major stumbling block. This paper suggests a new architecture for a user-friendly and secure RFID service, which uses customizing privacy policy based access control for collection or gathering of tagged information in an RFID information system. Proposals on feasible security mechanisms for low cost RFID systems and analyses of these mechanisms from both security and privacy points of view are also presented. The proposed architecture of an RFID privacy enhancing middleware system can expand the multi-domain level for various user services. Consequently, the proposed scheme effectively protects against abuse of tag related personal information using a consumer-configured privacy policy.

1 Introduction

Recently, low-cost radio frequency identification (RFID) has attracted growing interest from both industry and academic institutes. The RFID industry is very active, with numerous companies developing RFID tags of varying capabilities. With the growing importance of RFID for the ubiquitous infrastructure, numerous works on RFID technology including development of related applications have been conducted in a variety of fields. RFID can be potentially utilized in a broad range of everyday applications because of its capacity to readily relay information. Using RFID, the information of tagged products is given from an information server that utilizes data identified by a RF reader via the emission of an RF signal. While people often think of RFID tags as simply an updated replacement of the familiar bar code, they differ in several important ways, including usage of memory, identity individual items, writing of new data, interfacing with sensors, and digital data source. In order to adapt limited computing resource, such as RFID to secure sensor networks, new security approaches to cope with new threats have also been studied[1].

The areas where RFID technology can be applied are diverse, from inventory management and supply chain management to environmental surveillance and detection of intrusion in security systems. Using these kinds of management systems, an innovative business process can be constructed and various convenient services can be realized[2]. However, unless these systems are properly designed and constructed,

they can cause massive collateral damage to consumer privacy and company security. A store's inventory labeled with unprotected tags may be monitored by unauthorized readers on behalf of competitors. In addition, personalized tags would radiate identifying personal information to any tag reader anywhere, thus making their every movement traceable. Despite RFID's many advantages, there are many problems in deploying RFID technology extensively. The privacy violation of people carrying tag embedded items is one of the most serious problems in terms of expanding services utilizing this technology[3]. Consequently, in the present work, we address the privacy violation in the RFID system and investigate previously proposed algorithms for privacy issues.

With regard to the previously mentioned security threat to a store's inventory several approaches to RFID security have been reported, including killing tags at the checkout, applying a rewritable memory, physical tag memory separation, hash encryption, random access hash, and hash chains[3-8]. These approaches are introduced in detail in the next section.

Based on the pervasive deployment of RFID tags, we propose a novel privacy-aware RFID architecture followed by a hierarchical privacy policy for customizing privacy preference in real-time.

The remainder of this paper is organized as follows. Section 2 gives a brief description of privacy problems and previously proposed algorithms for privacy protection. Section 3 delineates a model of privacy protection and a technical working mechanism using a hierarchical and customizing privacy policy. Finally, conclusions and a discussion of potential areas for future research are presented in Section 4.

2 Privacy on RFID and Analysis of RFID Security

2.1 Security and Privacy for RFID Service

Many companies and organizations, including EPC Global Network, have developed RFID systems and international standardization is ongoing. The architecture of an RFID system is shown in figure 1.

Fig. 1. RFID System Architecture

In this model, the user holding the RFID reader requests information from the tag attached to the product and the reader transmits this information to the back-end information server via middle-ware. The information server subsequently returns the product information to the reader and displays it to user. The service model, as shown in Figure 1, is comprised of a RFID Tag, a reader, middleware, and an information server.

In view of information protection, a serious problem for the RFID service is a threat to privacy. Here, the privacy issue involves the risk of exposing information stored in a tag and the leakage of information including personal data related to the carrier of the tagged products. Privacy protection in a RFID system can be considered from two points of view. One is privacy protection between the tag and the reader in this regard, ID encryption, prevention of location tracking, and countermeasures against tag forgeries are utilized. The other is the exposure of information stored in the information server along with tagged items. First, we consider the exposure of information between the tag and reader, and then discuss the proposed privacy mechanism.

2.2 Previous Works on Smart Tag Based Security of RFID for Secure Communication

The previously proposed algorithms for the protection of traceability are Hash-Lock, Randomized Hash Lock, Re-encryption and Hash-Chain[3-9].

2.2.1 Randomized Hash Lock

Randomized Hash Lock algorithm improved the problem of traceability that the Hash-Lock algorithm has because of the unchanged meta-ID. Tag has two different hash functions and RNG (acronym for random number generator). The algorithm is following.

- 1) Tag generates a random number R using RNG.
- 2) Tag computes the Hash function $H(x)$ using the result of concatenation($\parallel$) of tag ID and R as input and gets hash value V, $V = H(ID \parallel R)$
- 3) Tag sends V and R to Reader and reader sends them to the database server storing tag ID. The server calculate the hash function using the result from concatenating the received R and tag ID stored in database and compares the calculated result with the received V from reader. If the server finds the same value with V, server returns tag ID back to reader.

This algorithm can solve the privacy violation by generating a different random number every challenge. However, there is a problem that the database server has to traverse sequentially all records to find a matched tag ID.

2.2.2 Re-encryption

A re-encryption algorithm can avoid traceability since it periodically updates and encrypts the stored data on a tag's memory space. However, due to the restricted resources of a passive tag, the data on the tag cannot be updated by the tag itself. Therefore, the data is encrypted by another party outside of the tag. Even though traceabil-

ity can be prevented by changing the data on the tag memory, additional equipment should be made available.

2.2.3 Hash-Chain

In this algorithm, tag embeds the two different hash functions $G(x)$ and $H(x)$ and stores the initial state information $S1$. As the response to the reader, tag sends $a1$ which is the result of calculating the hash function $G(S1)$, $a1 = G(S1)$

The tag's secret information S_i is altered into the value acquired as the result of the computing $H(S_{i-1})$, $S1 = H(S_{i-1})$

The Back-End database server stores the pair of tag ID and $S1$. The reader sends a_i received from the tag to the database server. The server finds the tag ID which results the identical value with a_i by computing hash function using S as input.

$$S1 = G(H(S1))$$

By these two different hash functions, there are benefits that the privacy of the owner can be protected and the tag can work with low power. However if the tag information is exposed, there are a few problems such as traceability and the forgery of the tag.

2.3 Privacy Protection for Personalized RFID Tag

Passive RFID systems, as opposed to smart active tags, are the most promising approach to provide low-cost ubiquitous tagging capability with adequate performance for most supply chain management applications. However, due to limitations in resources and computing capability in a low-cost RFID tag, a smart security mechanism is not applicable[10]. As highly coupled limited resource problem of a low-cost passive RFID tag, security and privacy technologies (reader, middleware and server side) can be added or enhanced to overcome the security weaknesses in an RFID system.

As tags are more widely utilized, the amount of information around us will increase dramatically, thus posing a critical privacy problem[10]. Privacy can be defined as the right that personal information be protected from exposure to others. From this point of view, we define requirements of privacy protection in an RFID system.

- Avoid collecting unnecessary private information in the RFID system
- Employ a controllable access control mechanism to the collected data in the RFID system
- Avoid collecting unnecessary private tracing in the RFID system
- Secure communication should be established for all communication links with the RFID system

Using the code acquired from the tag, the accessing application can access information about the tagged product by querying the server. In order to ensure privacy in this process, a mechanism that encrypts and decrypts the outgoing data from tag and server has been proposed. However, this creates limitations in the applicability of the RFID service. In addition, if decryption of the tag data is successful, all information can be exposed. For this reason, we propose a method that protects privacy in the RFID system using a personal privacy policy in order to administer information more flexibly and securely as well as mitigate the aforementioned problems.

3 Proposed Privacy Conscious RFID System

The way which protects privacy through implementing Privacy Preference is described like the following: the technology that provides pre-defined information in the level tag owner has selected and set according to his (or her) preference.

3.1 The Architecture for Personal Privacy Policy

Our proposed architecture is uniquely identified by the attachment of an RFID tag. Figure 2 shows the fundamental architecture for the privacy conscious RFID system proposed in this paper. The components of this architecture, as depicted in Figure 2, are (i) Tag and RFID Readers, (ii) Middleware, (iii) Information Servers, (iv) a Privacy Manager, and (v) a Privacy Policy Manager.

The tag owner set up his (or her) privacy policy for the tag and configures the authority of access and the related privacy level for sharing of information through a terminal in the Privacy Manager. The tag sends the pre-established privacy value when the reader requests it and the reader sends it back to the back-end information server. The server analyzes the data received from the reader and provides information in accordance with the privacy level set previously.

Fig. 2. Architecture of Privacy Protection with a RFID system

In this paper, we discuss an information system that allows access of information at the right place and time with low communication cost through a user privacy profile. The proposed system employs the following procedures:

- 1) Introduction of an information management table based on the user configured privacy and access policy
- 2) Provision of privacy controlled tag related information if a user requests information inform a personalized tag.

3.2 Privacy Level of RFID by Product

In order to gain maximum privacy protection for a personalized tag, the high level of privacy policy databases must be kept in the tag memory and information server. The privacy preference level refers to a grade of information the owner of the tagged item can open to the public. Table 1 shows 4 different privacy levels for example. Because of the difference of sensitivity to privacy according to different users, these levels were selected by tag attached product-owner in this paper. For example, if level of privacy set as level 4, only information about product class can be provided. If owner select level 3, product name, company of production, price etc can be served. If the privacy level of tag is set to 1, all information related to this tag can be presented. When a tag is read by a user, the tag sends the privacy level to the reader. Using the data sent by the tag, the reader can obtain the location of the server and request information customized to the privacy level obtained from the tag.

Table 1. Privacy Level in Tag attached Product

Privacy Level	1	2	3	4
Product Class	O	O	O	O
Product Info.	O	O	O	X
History Info.	O	O	X	X
Owner Info.	O	X	X	X

O : permit
X : not permit

Diagram description: A 5x5 grid with columns 1-4 and rows Product Class, Product Info., History Info., Owner Info. A diagonal line from (1,1) to (4,4) separates the grid. The area above the line (top-left) is green and contains 'O'. The area below the line (bottom-right) is blue and contains 'X'. A pink arrow on the right points down, labeled 'Increase of Information Security'. A pink arrow at the bottom points right, labeled 'Increase of Privacy Level'.

Table 2 shows an example of the access control policy in a tagged and personalized product by purchase.

Access control policy of the information of the tag attached product can describe the description document of the product. In the figure, if the owner selects privacy

Table 2. Access Control Policy in Tag attached Product

Privacy Level Access Policy	Product Class	Product Info.	History Info.	Owner Info.
Third party(others) : $A_G(1)$	O	X	X	X
Transportation Company : $A_G(2)$	O	X	X	X
Object Production Company : $A_G(3)$	O	O	X	X
Merchandise : $A_G(4)$	O	O	O	X
Service Company (after sale) : $A_G(5)$	O	O	O	O

O : permit X : not permit

Diagram description: A 5x5 grid with columns Product Class, Product Info., History Info., Owner Info. and rows for different access policies. A dashed line separates the first column from the others. The area to the right of the line is pink and contains 'X'. The area to the left of the line is white and contains 'O'. A pink arrow at the bottom points right, labeled 'Increase of Access Security'.

level 3 for an access group third party(others), the information of product class(such as health, food, cloth etc) can only provide to others. The associated table access policy with privacy level is needed for the following purpose in the policy database of the privacy manager. When the third party queries the information of tag, the owner wants to know who contact the database to obtain the tag related information. And owner wants to make the decision whether provide or not the information of the tagged product. For example in table 2, access group 3 mapped to the privacy level 3 and access group 4 mapped to the privacy 2. Owner of product can select privacy level for access group.

3.3 Privacy and Access Policy of RFID by Product

The user memory bank of RFID tag can store the encrypted data of privacy policy owner configured, as shown in Figure 3. For example in Table 2, access control policy is 4,4,3,2,1 and the data is stored in tag. When anyone read the tag, encrypted the policy data must be transport to server securely and the information of tag can be provided by the access policy.

The tag memory is insecure and susceptible to physical attacks. This includes a myriad of attacks such as shaped charges, laser etching, ion-probes, tempest attacks, clock glitching, and many others[10]. Fortunately, these attacks require physical tag access and are not easily carried out in public or on a wide scale without detection[10-13].

Fig. 3. Data Structure of Tag for Privacy and Security

The security level is a key factor to ensure the privacy policy and related data along with the tag, reader, middleware, and server. Furthermore, it can be an alternative to solve a request for information by maliciously changing the privacy level. Table 3 represents the additionally required phases according to the request. A variety of access control methods can be added as the importance of the information increases. The enforcement of the access control should be proportionally complicated and stronger according to the security level.

Table 3. Security Level for Secure Communication in RFID system

Security Level	1	2	3	4
No Security	o	x	x	x
Symmetric key based Security(password based lock/unlock)	x	o	x	x
Symmetric based Security(encryption of Tag code), Protection of Location based Traceability	x	x	o	x
Public Key based Encryption, Protection of Location based Traceability	x	x	x	o

3.4 Privacy Protection Mechanism for Consumer Privacy

The information about a product can transfer as a XML format with security(WS Security) and also can be subject to access controlled by a standard technology such as XACML.

The procedures to set the policy for the disclosure of the product information and processing by the information server are shown in Figure 4.

Fig. 4. RFID Privacy Protection Mechanism in Information Server

- 1) The company's privacy manager receives the privacy rule and policy from owner. They are the information defined in the tag and server with the owner's privacy, security and access policy.
- 2) The accessing application requests tag attached product information with the tag code and the security and privacy policy data to the information server.
- 3) The information server parses the user request.
- 4) The privacy manager make decision the final privacy level using the privacy and security level in the tag's user memory, the user's previous policy stored in the

server, and the information(who, what propose etc) of accessing user and company's privacy rule.

$$\begin{array}{l} P_{\text{server}} : \text{Policy defined in Policy Server} \\ P_{\text{tag}} : \text{Customized Policy in Tag} \\ [P_{\text{tag}} \oplus P_{\text{server}} \oplus P_{\text{company}}] \text{ with access policy} \rightarrow P_{\text{out}} \rightarrow \text{Server Decision} \end{array}$$

- 5) If the server needs to notify to the owner by notify policy to make decision access policy, the server notifies and polls via a mobile SMS message.
- 6) If the user replies with a positive response and the response is authenticated, the server provides the information according to the authority previously configured by the tag owner.

The Information server stores the event logs and notifies them to the owner. Through monitoring the notified logs, the owner can re-configure the privacy preference and the access control for optimized privacy protection.

3.5 Hierarchal Structure of Privacy Domain for RFID Privacy

In this section we discuss the structure for the RFID privacy domain, which provides a personal policy based global combination of the RFID network.

First, our privacy domain architecture is hierarchical in nature, organized as a balanced tree topology, as shown in Figure 5.

Fig. 5. Hierarchal Structure of RFID Privacy Domain for User's Privacy Protection

The root server of the privacy policy sets up the personal preference policy according to service category. The low positioned local privacy manager inherits the root's policy and adapts the policy to its own products. The local manager is audited by the root manager in terms of whether the inherited policy is properly adapted and whether the user's policy as been maintained properly. In hierarchal structure, PPP (Privacy Policy Protocol) is used between the root privacy manager and the local privacy manager for exchange of policy. The root privacy manager establishes a permitted limit, which is also used for application to the local domain policy.

The messages of PPP consist of Query Message, Reply Message, Privacy Policy Message, Ack Message, Transfer Message, and Keep Alive Message.

In the hierarchal structure, the user can configure a customizing policy to root the privacy manager. Then, the policy is applied to the local privacy manager for local domain RFID privacy using PPP.

4 Conclusion

In this paper, we considered privacy protection for the owner of a tagged product in terms of two aspects: privacy between the tag and reader and exposure of the product information. The proposed algorithms were presented in terms of privacy policy whereas we introduced a privacy protection scheme using owner configured privacy preference policy. In the proposed mechanism, the owner of the tagged product sets the privacy level and security level on tag data fields and configures the level of the information that will be accessible to the public and the access control. By doing so, customized privacy protection can be realized. In this regard, the suggested mechanism is an effective solution for privacy protection in an RFID system.

References

1. Seunghun Jin, et al.: Cluster-based Trust Evaluation Scheme in Ad Hoc Network. *ETRI Journal*, Vol.27, No.4 (2005)
2. 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)
3. Weis, S. et al. "Security and Privacy Aspects of Low-Cost Radio Frequency identification Systems", First Intern. Conference on Security in Pervasive Computing (SPC) (2003)
4. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets (2002)
5. M. Ohkubo, K. Suzuki and S. Kinoshita, Cryptographic Approach to "Privacy-Friendly Tags, RFID Privacy Workshop2003 (2003)
6. Jan E. Hennig, Peter B. Ladkin, Bern sieker, Privacy Enhancing Technology Concepts for RFID Technology Scrutinised, RVS-RR-04-02, 28 October (2004)
7. Ari Juels, Ronald L Rivest, Michael Szydlo "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" 10th ACM Conference on Computer and Communications Security (2003)
8. Ari Juels, Ravikanth Pappu, Squealing RFID-Enabled Banknotes In R. Wright, ed., *Financial Cryptography* (2003)
9. Simson Garfinkel, Beth Rosenberg, *RFID Applications, Security, and Privacy*, Addison-Wesley (2005)
10. 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
11. Sanjay E. Sarma, et al., RFID Systems and Security and Privacy Implications, *CHES 2002*, LNCS 2523, pp. 454–469, (2003).
12. Dirk Henrici and Paul Müller, Tackling Security and Privacy Issues in Radio Frequency Identification Devices, *Pervasive 2004*, LNCS 3001 (2004) pp. 219–224