Customized Healthcare Infrastructure Using Privacy Weight Level Based on Smart Device

Namje Park

Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju-do, 690-781, Korea
namjepark@jejunu.ac.kr

Abstract. Personalized radio-frequency identification (RFID) tags can be exploited to infringe on privacy even when not directly carrying private information, as the unique tag data can be read and aggregated to identify individuals, analyze their preferences, and track their location. This is a particularly serious problem because such data collection is not limited to large enterprise and government, but within reach of individuals. In this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID service. We propose a secure mobile RFID service framework leveraging mobile networking. Here we describe the proposed framework and show that it is secure against known attacks. The framework provides a means for safe use of mobile phone-based RFID services by providing security to personalized RFID tags.

Keywords: Mobile RFID, Privacy, Security, Hospital, Healthcare.

1 Introduction

The recent medical security guidelines and the development of information technology make hospitals reduce the expense in surrounding environment and it requires improving the quality of medical security of the hospital. That is, with the new guidelines and technology, hospital business escapes simple fee calculation and insurance claim center. Moreover, MIS (Medical Information System), PACS (Picture Archiving and Communications System) are also developing. Medical Information System is evolved toward integration of medical IT and situation si changing with increasing high speed in the ICT convergence. These changes and development of ubiquitous environment require fundamental change of medical information system. Mobile medical information system refers to construct wireless system of hospital which has constructed in existing environment. Through mobile RFID development in existing system, anyone can log on easily to Internet whenever and wherever.

RFID technology is widely used in supply chain management and inventory control, and is recognized as a strong potential vehicle for ubiquitous computing. However, continued development and global adoption has also raised fears of the potential for exploiting such tags for privacy infringement in 'Big Brother' type scenarios. We propose a secure framework for mobile-phone based RFID services

G. Lee, D. Howard, and D. Ślęzak (Eds.): ICHIT 2011, CCIS 206, pp. 467–474, 2011.

using personal privacy-policy-based access control for personalized ultra-high frequency (UHF) tags employing the Electronic Product Code (EPC). The framework, called mobile RPS, has dynamic capabilities that extend upon extent trust-building service mechanisms for RFID systems. This new technology aims to provide absolute confidentiality with only basic tags.

2 Security Framework Architecture

2.1 Privacy Protection Framework for Mobile RFID Services

The objective of personal privacy in mobile RFID services is to allow individuals to control their personal information related to RFID services. In other words, unauthorized distribution of personal information carried on the tag shall be prevented and a privacy protection mechanism shall be applied to the information collection process through the use of terminals. This paper aims to provide privacy protection services by adopting a privacy protection system (RPS) in the mobile RFID service network. Figure 1 shows the structure of mobile RFID service including RPS.

Privacy protection in mobile RFID services refers to technological measures against unauthorized access of personal information. Access to platform resources can be controlled based on each user's privacy protection level. Privacy protection in mobile RFID services is based on the following concepts.

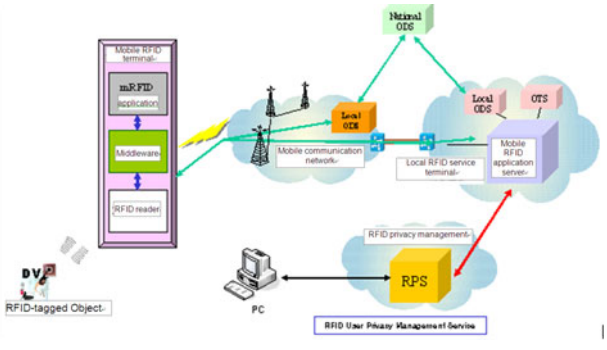

Fig. 1. Mobile RFID service

1) For privacy-secure mobile RFID services, the privacy protection system guarantees confidentiality and integrity of privacy information on the network and ensures authorization of entities.
2) Mobile RFID application and contents provides detailed access control mechanisms that can manage object information, log data, and personal information by user group.
3) Mobile RFID application and contents provision systems communicate with RPS systems through secure communication paths.

4) Mobile RFID application and contents provision systems provide auditing functions with stronger privacy based on the privacy protection policy that each individual user defined in the RPS system.
5) The Mobile RFID application and contents provision system manages personal privacy information based on the rules that individual users defined in the RPS system. The system operators are obliged to protect personal privacy information in earnest.
6) Mobile RFID application and contents provision systems have a mechanism to negotiate privacy policies with mobile RFID terminals to prevent them from gathering personal information.

2.2 Application and Contents Information Server of the Service Provider

The application and contents information server of the service provider provides an extended access control for greater stability. Depending on the tag owner's policy transmitted from RPS, the application and contents information server manages privacy contents, checks who is accessing information, and controls access based on the privacy protection level that shall be set by the object holder.

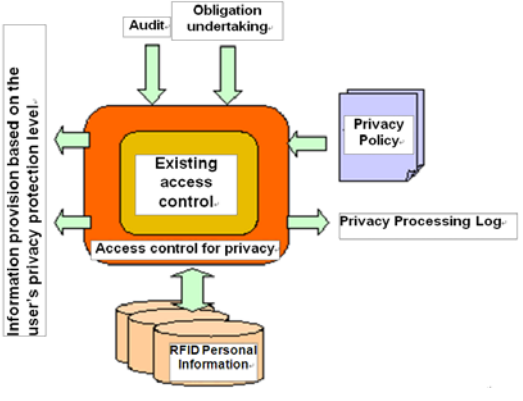

Fig. 2. Application and contents information system of service provider

2.3 Procedure for Secure Mobile RFID Services

There are three privacy protection scenarios for mobile RFD services.

2.3.1 Privacy Policy-Setting Stage

1) Subscribing to RPS and Setting the Privacy Policy

Figure 3 shows the procedure for subscribing to RPS. To use the privacy protection service, the user shall subscribe to RPS and define his/her privacy protection policy. In the same way, the service providers that intend to provide privacy-secured services shall also subscribe to RPS and comply with the default privacy policy of the corresponding service or the privacy protection policy set by the user.

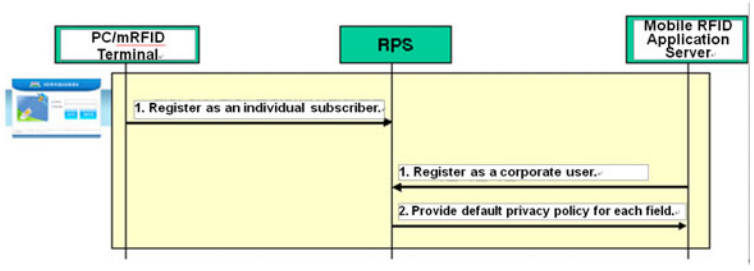

Fig. 3. Subscribing to privacy protection service in a mobile RFID environment

2) Personalization of Tag-attached Object (Privacy Information Combining Phase)
In Figure 4 above, the privacy policy is applied when the tag-attached object is personalized or when privacy information is combined. The following describes the procedure in more detail.

①The mobile RFID terminal reads the tag. Depending on the user's decision, the RFID terminal starts the application program to personalize the tag-attached object (such as purchase.)

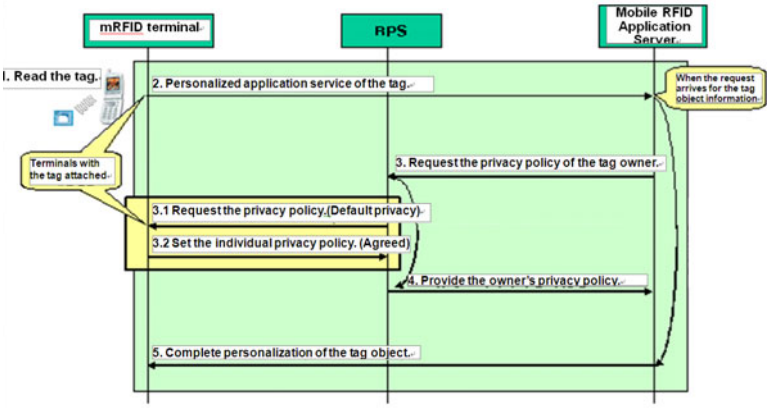

Fig. 4. Personalization of tag-attached object

②The RFID terminal finds the mobile RFID application server in the ODS server and sends the request. At this time, the mobile RFID application server receives information requests and checks whether there is any privacy policy for the owner's tag-attached objects.

③In case the application server does not have a privacy policy for the tag-attached object owner, the RFID terminal requests the policy from the RPS server. Then, RPS checks whether there is a privacy policy for the tag-attached object.

3) Provision of Privacy-protected Information

In the above procedure, privacy-protection information is provided in three ways as shown in Figure 5. The following describes the procedure.

①The mobile terminal reads the tag's information. At this time, the privacy policy stored in the tag is also sent to the mobile RFID terminal.

②The mobile RFID terminal is coupled with the user's terminal application service and finds the mobile RFID application server in the ODS server. At this time, the mobile RFID application server receives the request and checks whether it has the privacy policy of the tag-attached object owner.

③In case the mobile RFID application server does not have the privacy policy of the tag-attached object owner, the mobile RFID application server will request the RPS server to send the policy. Then, RPS checks whether it has the privacy policy of the tag-attached object owner.

④RPS stores personal privacy policy when the object is personalized and sends the privacy policy to the application server. In case RPS does not have a policy, the owner will send the privacy information request in a short text message and will inform who is requesting the privacy information. To avoid delays, the default privacy protection policy determined based on the privacy impact assessment result is sent to the application server.

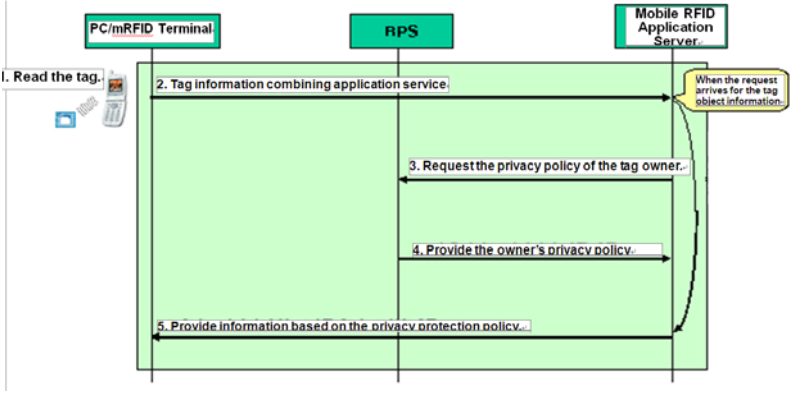

Fig. 5. Mobile RFID privacy protection scenario

⑤The mobile RFID application server sends information of which privacy protection level is lower than the one defined by the user. In other words, only privacy-protected information is sent to the one who is requesting the information. Appendix 1 shows an example.

2.4 Classification of Privacy Levels

The following table is an example of how the privacy levels are classified and how each level is applied. The privacy level is from 0 to 10. In Level 0, virtually no privacy protection is provided, and in Level 10, tags are killed or the levels are not in use.

As shown in Table 1, levels actually used for privacy protection are from 1 to 9. These levels are again classified into Low Level (1 ~ 3), Medium level (4 ~ 6), and High Level (7 ~9.) Each level is for the privacy protection in each application service. However, it is recommended that the privacy protection system should support the following levels to ensure compatibility with the RPS system. In other words, privacy platforms have three groups of privacy protection levels that are from 1 to 10. Three groups of privacy protection levels include Low Level (where most information is disclosed), Medium Level (where object information and history are disclosed) and High Level (where only part of the object information and object category are disclosed.) The default privacy level is applied to the tag and the RPS system.

1) Low Level (Open)
Low levels refer to levels where privacy is least protected among all privacy protection levels. When the privacy level is a low level, most mobile RFID terminals can access the system and related information including parts of personal information. Low levels are allowed only for those who are reliable.

2) Medium Level (Object Information and History)
When mobile RFID accessing individuals are reliable or information carried on the tag does not infringe on a users' privacy, Medium levels are applied. In Medium levels, parts of information are not protected because some security keys are disclosed and disclosed information does not affect security.

3) High Level (Part of Object Information and Object Category)
Access to High-level information is not reliable, and all access is controlled. Only limited parts of information such as object names or object categories are allowed in High levels. For example, in a High level, mobile RFID service is sensitive to privacy and the object owner allows the least information to be exposed to third parties.

Table 1. Default privacy protection level

Privacy Level / Object Information	Low Level (1~3)			Medium Level (4~6)			High Level (7~9)		
	1	2	3	4	5	6	7	8	9
Object Category	O	O	O	O	O	O	O	O	X
Object Name	O	O	O	O	O	O	O	O	X
Object Code	O	O	O	O	O	O	O	X	X
Object History	O	O	O	O	O	O	X	X	X
Price	O	O	O	O	O	X	X	X	X
Distribution Information	O	O	O	O	X	X	X	X	X
Object Description	O	O	O	X	X	X	X	X	X
Owner ID	O	O	X	X	X	X	X	X	X
Owner Account	O	X	X	X	X	X	X	X	X
Owner Personal	O	X	X	X	X	X	X	X	X

X: Not to be disclosed/ O: To be disclosed.

3 Implementation of Application Solutions

3.1 Implementation of Customized Healthcare Service

In the proposed hospital data management system, RFID-tagged medical card are given to patients on registration. Patients with sensitive conditions, for example, heart disease or cerebral hemorrhage, can use the medical card to rapidly provide medical history that can used for fast application of first aid. Further, biosensors can be incorporated to provide real-time data to the doctor for each specific patient. The RFID patient tags also can be used to verify patient identity to ensure the correct treatment is administered. Thus, the system allows chartless service.

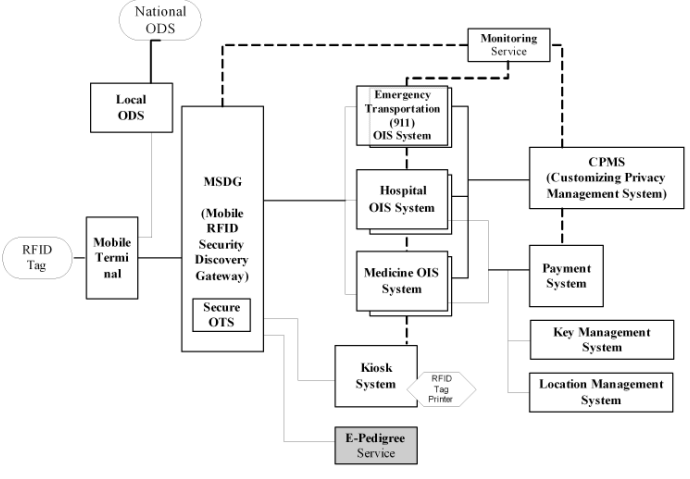

Fig. 6. Proposed customized ubiquitous hospital model

3.2 Implementation

The hospital generated an initial set of control data, which included the patient code, medical ID, and related information. The default privacy level was used and the patient was not allowed to control security policy. In order to provide authentication and privacy interface to patient as a agent in medical discovery gateway and hospital's information server system. Essentially, each bit of sensitive data was initially classified by the default privacy weight, which was then modified by the end user's detailed policy. The user-controllable privacy policy in this system evaluation is considered a basic part of RFID privacy management. The compatibility and scalability may be limited, which will hamper system migration, but the mechanism is suitable for policy based privacy control. The proposed privacy management mechanism was implemented in an actual medical emergency room, including a networked medical information RFID kiosk, RFID networked emergency rescue system, and medical examination service. There is some approach applying the RFID to medicine and hospital. From above, proposed privacy scheme has advantages in custom centric approach aspect for constructing a privacy aware ubiquitous medical system.

4 Conclusion

RFID technology will evolve to become ubiquitous, allowing automatic detection and delivery of information on the surrounding environment, and interconnecting them through the network. This will require RFID implementation of security measures as the technology is vulnerable to privacy infringement via counterfeiting, falsification, camouflage, tapping, and tracking. Therefore, it is necessary to enact laws and regulations that meet the expectations of consumer protection organizations that are sensitive to individual privacy, and develop and apply secure technologies that can follow such laws and regulations.

Mobile RFID readers are being actively researched and developed throughout the world, and more efforts are underway for the development of related service technologies. Though legal and institutional systems endeavor to protect privacy and encourage data protection, the science and engineering world must also provide suitable technologies. Seemingly, there are and will be no perfect security/privacy protection methods. The technologies proposed in this paper, however, would contribute to the development of secure and reliable RFID systems.

Acknowledgments. This paper is extended from a conference paper presented at The 3rd International Conference on Computational Collective Intelligence. The author is deeply grateful to the anonymous reviewers for their valuable suggestions and comments on the first version of this paper.

References

1. Mobile RFID Forum of Korea: Mobile RFID Privacy Protection Framework (Framework for Privacy Protection of Mobile RFID Services). MRFS-4-08. Standard Paper (2006)
2. Park, N., Song, Y., Won, D., Kim, H.: Multilateral Approaches to the Mobile RFID Security Problem Using Web Service. In: Zhang, Y., Yu, G., Hwang, J., Xu, G. (eds.) APWeb 2008. LNCS, vol. 4976, pp. 331–341. Springer, Heidelberg (2008)
3. Park, W., Lee, B.: Proposal for participating in the Correspondence Group on RFID in ITU-T. Information Paper. ASTAP Forum (2004)
4. Park, N., Kwak, J., Kim, S., Won, D., Kim, H.: WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. In: Shen, H.T., Li, J., Li, M., Ni, J., Wang, W. (eds.) APWeb Workshops 2006. LNCS, vol. 3842, pp. 741–748. Springer, Heidelberg (2006)
5. Park, N., Kim, H.W., Kim, S., Won, D.H.: Open Location-Based Service Using Secure Middleware Infrastructure in Web Services. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 1146–1155. Springer, Heidelberg (2005)
6. Park, N.: Security scheme for managing a large quantity of individual information in RFID environment. CCIS, vol. 106, pp. 72–79. Springer, Heidelberg (2010)
7. Park, N.: Secure UHF/HF Dual-band RFID: Strategic Framework Approaches and Application Solutions. In: ICCCI 2011. LNCS, Springer, Heidelberg (2011)