안전한 모바일 RFID 서비스 네트워크를 위한 보안 통합 프레임워크의 설계 및 구현

박남제, 정교일*
한국전자통신연구원 정보보호연구본부
e-mail : {namjepark, kyoil}@etri.re.kr

Design and Implementation of Security Integration Framework for Secure Mobile RFID Service Network

Namje Park, Kyoil Chung*
Information Security Research Division
Electronics and Telecommunications Research Institute

Abstract

The mobile RFID (Radio Frequency Identification) is a new application to use mobile phone as RFID reader with a wireless technology and provides new valuable services to user by integrating RFID and ubiquitous sensor network infrastructure with mobile communication and wireless internet. However, there are an increasing number of concerns, and even some resistances, related to consumer tracking and profiling using RFID technology. Therefore, in this paper, we describe the security analysis and implementation leveraging globally networked mobile RFID services which complies with the Korea's mobile RFID forum standard.

I. Introduction

Currently, RFID technologies consider the environment in which RFID tags are mobile and RFID readers are stationary. However, in the future RFID technologies could consider an environment in which RFID tags are stationary and readers are mobile. RFID based on mobile telecommunications services could be the best example of this kind of usage. RFID-based mobile telecommunications services could be defined as services which provide information access through the telecommunication network by reading RFID tags on certain objects using an RFID reader in mobile terminals such as cell phones. RFID tags play an important role as a bridge between offline objects and online information.

A new security technology is required to provide a safe service among mobile RFID tags, terminals, and applications in order to minimize the threat of personal information infringements and leakage Therefore, in this paper, we present an analysis of security, and multilateral security approaches to promoting a globally mobile RFID service. This new technology to RFID will provide a solution that protects absolute confidentiality, from basic tags to the user's privacy information.

II. Secure Integration Framework

2.1 Proposed Architecture

The mobile RFID service structure provides its services by associating the mobile communication network and the RFID application service network based on the RFID tag. The areas to be considered with regard to security are essentially the RFID tag, reader terminal area, mobile communication network area, RFID application service network area, while other security issues such as confidentiality /

integrity / authentication / permission / non-repudiation shall be considered in each network area. Especially, as the mobile RFID service is the end-user service, the issue of privacy protection must inevitably become a serious issue to consider, and as contents accessibility increases due to the off-line hypertext property of RFID, the authentication for adult services is also highly likely to become another important issue for consideration.

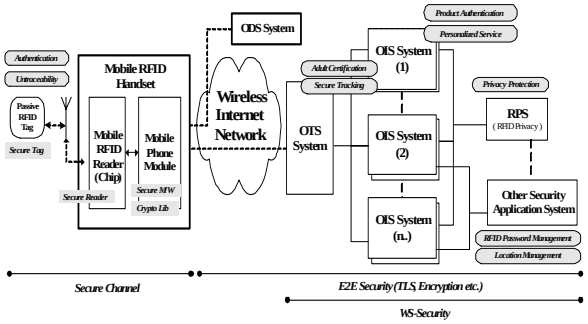

Figure 1. Conceptual Architecture for Secure Mobile RFID

2.2 Multilateral Approaches with Improved Security

For the provision of secure mobile RFID services, the author prepared the mobile RFID protection policy named MRF-Sec631 (Mobile RFID-Security 6.3.1.) and proposed the mobile RFID information protection service model. Specifically speaking, MRF-Sec631 means the development of 6 typical standard security functions out of mobile RFID terminal platforms, applies 3 main security service mechanisms on the basis of such development, and the execution of secure mobile RFID services through application portal services. The 6-standards security functions are mobile RFID data encryption API function, mobile RFID secure communication API function, mobile RFID password management API function, EPC C1G2 security command API function, adult certification API function, and privacy protection API function. The 3-security service mechanisms are authentication service mechanism, privacy protection service mechanism, and secure location tracking service mechanism. The 1-secure application service is secure mobile RFID application portal service.

Ⅲ. Implementation

The provision of secure mobile RFID services needs a combined security framework resolving many security issues like security among domains, personal privacy profile, authentication, end-to-end security, and track prevention. The following is the configuration of the service framework based on the MRF-Sec631 development. The main functions of the proposed mobile RFID information protection service model are the provision of WIPI based mobile security middleware, tag authentication, tag tracking prevention, reader authentication, message security, and protection of profile based privacy.

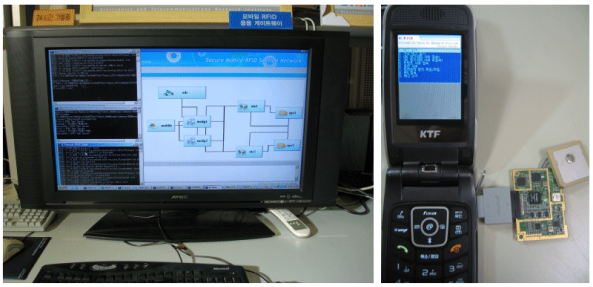

Figure 2. Conceptual Architecture for Secure Mobile RFID

Ⅳ. Conclusion

Technologies proposed in this paper, would contribute to the development of secure and reliable network RFID circumstances and the promotion of the mobile RFID market.

Acknowledgment

This work was supported by the IT R&D program of MKE/IITA [2005-S088-04, Development of Security Technology for Secure RFID/USN Service].

References

[1] Namje Park, Howon Kim, Kyoil Chung, and Sungwon Sohn, "Design of an Extended Architecture for Secure Low-Cost 900MHz UHF Mobile RFID Systems", IEEE Tenth International Symposium on Consumer Electronics 2006, Vol.1/No.1, pp. 666-671.

[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] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags", RFID Privacy Workshop, 2003