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.

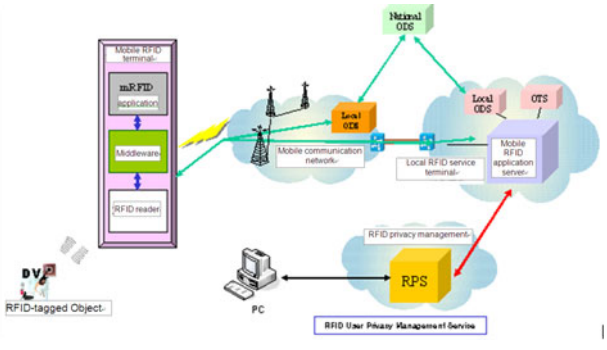

Fig. 1. Mobile RFID service

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.