Secure UHF/HF Dual-Band RFID : Strategic Framework Approaches and Application Solutions

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. In the mobile RFID (Radio-Frequency Identification) environment, scanning RFID tags which are personalized can bring some privacy infringement issues. In spite of the case that private information is not stored in those tags, one can identify entities, analyze their preferences, and track them by collecting data related with the tags and aggregating it. Especially, it might be more serious at the point of that data collection may be done not only by enterprises and government, but also by individuals. In this paper, we describe privacy infringements for the mobile RFID service environment. The proposed framework provides a means for securing the stability of mobile RFID services by suggesting personal policy based access control for personalized tags.

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

1 Introduction

RFID (Radio Frequency Identification) technology is currently widely used for supply chain management and inventory control. Furthermore, RFID is recognized as the vehicle to realize the ubiquitous environment. Though the Radio Frequency Identification (RFID) technology is being actively developed with a great deal of effort to generate a global market, it also is raising fears of its role as a 'Big Brother'. So, it is necessary to develop technologies for information and privacy protection as well as promotion of markets (e.g., technologies of tag, reader, middleware, etc.) The current excessive limitations to RFID tags and readers make it impossible to apply present codes and protocols. The technology for information and privacy protection should be developed in terms of general interconnection among elements and their characteristics of RFID to such technology that meets the RFID circumstances.

The typical architecture for RFID is composed of RFID tag, which is embedded or attached to an object, and the RFID reader and IS (Information Services) server. The RFID reader reads the code in the RFID tag and recognizes the meaning of the code via communicating with the IS server via proper communication network. This is the typical architecture defined by EPCglobal [1,2,3]. The RFID reader can be a type of stationary or mobile. If the RFID reader is mobile, then we can have more applications than the stationary RFID reader.

P. Jędrzejowicz et al.(Eds.): ICCCI 2011, Part I, LNCS 6922, pp. 488–496, 2011.

While common RFID technologies are used in B2B (Business to Business) models like supply channels, distribution, logistics management, mobile RFID technologies are used in the RFID reader attached to an individual owner's cellular phone through which the owner can collect and use information of objects by reading their RFID tags; in case of corporations, it has been applied mainly for B2C (Business to Customer) models for marketing. Though most current mobile RFID application services are used in fields like the search of movie posters and provision of information in galleries where less security is required, they will be expanded to and used more frequently in such fields as purchase, medical care, electrical drafts, and so on where security and privacy protection are indispensable. A method to solve the problem of the mobile RFID service has been studied by researchers [6,8,9,12].

In this paper, we explain UHF/HF RFID technology based on EPC and analyze threats of the mobile RFID service. We propose privacy protection service framework based on a user privacy policy. The proposed framework provides a means for securing the stability of mobile RFID services by suggesting personal privacy-policy based access control for personalized tags. This is new technology to mobile RFID and will provide a solution for protecting absolute confidentiality from basic tags to user's privacy.

2 Strategic Security Framework Architecture

This technology is aimed at RFID application services like authentication of tag, reader, and owner, privacy protection, and non-traceable payment system where stricter security is needed [6,11,12,14,15].

- Approach of Platform Level
  This technology for information portal service security in offering various mobile RFID applications consists of application portal gateway, information service server, terminal security application, payment server, and privacy protection server and provides a combined environment to build a mobile RFID security application service easily.
- Approach of Protocol Level
  It assists write and kill passwords provided by EPC (Electronic Product Code) Class1 Gen2 for mobile RFID tag/reader and uses a recording technology preventing tag tracking. Information technology solves security vulnerability in mobile RFID terminals that accept WIPI as middleware in the mobile RFID reader / application part and provides E2E (End-to-End) security solutions from the RFID reader to its applications through WIPI based mobile RFID terminal security / code treatment modules.
- Approach of Privacy Level
  This technology is intended to solve the infringement of privacy, or random acquisition of personal information by those with RFID readers from those with RFID attached objects in the mobile RFID circumstance except when taking place in companies or retail shops that try to collect personal information. The main assumptions are privacy in the mobile RFID circumstance when a person holds a tag attached object and both information on his/her personal identity (reference number, name, etc.) and the tag's information of the commodity are connected. Owners