Chapter 114
Analyses of Attacks on Embedded RFID Application Under U-Healthcare System

Jung Tae Kim

Abstract A variety of security and privacy threats to RFID authentication protocols have been widely studied, including eavesdropping, replay attacks, denial of service (DoS) attacks, tracking, and traceability. Considering this RFID security issues, we surveyed the security threats and open problems related to issues by means of information security and privacy. In this paper, we have analyzed and compared practical threat on U-healthcare system.

Keywords Attacks · Privacy · Tracking · Traceability · Denial of service

114.1 Introduction

Radio Frequency Identification (RFID) system is one of the promising technology that plays an important role for object identification as ubiquitous infrastructure and wireless sensor networks. RFID system can be applied to many applications in the field of access control, manufacturing automation, maintenance, supply chain management, parking garage management, automatic payment, tracking, and inventory control. In recent years, several RFID authentication protocols have been proposed to resolve the security and privacy issues in spite of limited resources. Despite the threats against user's privacy, a lot of problem related to the authenticity of an RFID tag due to its limited resources such as small capacity. One of them is tag spoofing it is a serious problem to RFID systems. For example, an attacker may try to copy this fixed serial number of an RFID tag attached to a product and place a fake tag with this serial number to an imitation of this product or to a cheaper product. As a result, it is vital for an RFID system to be able to

J. T. Kim (✉)
Deptartment of Electronic Engineering, Mokwon University, 800, Doan-dong, Seo-Ku, Daejeon 302-729, Korea
e-mail: jtkim3050@mokwon.ac.kr

H.-K. Jung et al. (eds.), *Future Information Communication Technology and Applications*, Lecture Notes in Electrical Engineering 235, DOI: 10.1007/978-94-007-6516-0_114,

authenticate a genuine RFID tag. These risks could be addressed if RFID tags were used that incorporate advanced cryptographic primitives and tamper-resistance packaging [1]. The remainder of this paper organized as follows. Section 114.1 is the introduction. Section 114.2 provides related works of application of RFID for fusion technologies. Section 114.3 presents the attacks analysis of protocol and discusses the various security and privacy issues including the associated attack. Section 114.4 provides the example of RFID application under U-healthcare system. Finally, Sect. 114.5 made a conclusion.

114.2 Related Works

RFID devices are expected to become the most densely interconnected network devices. Many researchers also tried to provide broader insights to the many prevailing issues and challenges in security system. We believed that that kind of matters are suitable topics for exploratory research. Future research efforts are particularly needed in many areas. Faouzi Kamoun described about RFID System management and state-of-the art and open research issues. Future research efforts are particularly needed in many areas, including (1) integration of RFID system management within the existing enterprise network management framework, (2) re-use of remote monitoring, distributed and collaborative network management concepts, (3) migration from RFID device management towards RFID services management, (4) adaptive self-reconfiguration and self-healing mechanisms of RFID readers, (5) real-time data analysis and visualization of RFID operations, (6) RFID policy-based management, (7) RFID asset management, (8) readers' behavior modeling and prediction, (9) efficient and lightweight cryptographic algorithms, (10) new security mechanisms, tailored to RFID applications and (11) unified and interoperable RFID reader management platforms [2]. Boyeon Song introduced server impersonation attacks, a practical security threat to RFID security protocols that has not previously been described. A server impersonation based de-synchronization attack is a feasible security threat because RFID tag memory is typically not tamper-resistant. In 2008, a scalable radio frequency identification (RFID) authentication protocol was proposed by Yanfei Liu to provide security and privacy for RFID tags [3]. This protocol only needs O (1) time complexity to find out the identifier of the RFID tag irrespective of the total number of the tags in the system. But the scheme is vulnerable to tracking attack, tag impersonation attack, and de-synchronization attack. Imran Erguler et al. compared the security of YL protocol that stated to have the required security properties for RFID communications. They reported that this protocol is vulnerable to a series of active attacks such as the tag tracking, tag impersonation, and de-synchronization attacks in their works [4].

114.3 Attack Models

There are a variety of vulnerable attacks in RFID system. Security threats to RFID protocols can be classified into weak and strong attacks. Weak attacks are threats feasible just by observing and manipulating communications between a server and tags. Replay attacks and interleaving attacks are examples of weak attacks. Strong attacks are threats possible for an attacker which has compromised a target tag. An RFID tag's memory is vulnerable to compromise by side channel attacks, because the memory of a low cost tag is unlikely to be tamper-proof. Hence, strong as well as weak attacks should be considered in RFID protocol design. Backward traceability, forward traceability, and server impersonation attacks, are all examples of strong attacks [3].

Thomas Schaberreiter et al. described an enumeration of RFID related threats. They classified three breach information related attack issues in a RFID system including breach confidentiality, breach integrity and breach availability. To illustrate attach model, they proposed attack tree for the threat of compromising data through the RF-link and listing of threats against availability [2]. Classification of RFID attacks model in Fig. 114.1 (Table 114.1).

RFID systems are vulnerable to a broad range of malicious attacks ranging from passive eavesdropping to active interference. RFID tags may focus on a considerable security and privacy risk to organizations and individuals using them [5]. Even when the content of the tags is protected, individuals may be tracked through predictable tag responses. Even though many cryptographic primitives based on software mechanism can be used to remove these vulnerabilities, they cannot be applied to a RFID system due to the prohibitive cost of including protection for

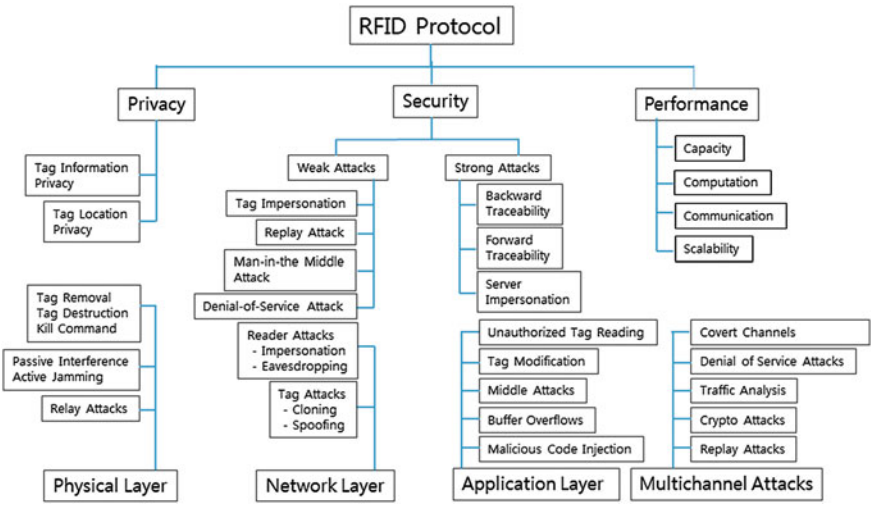

Fig. 114.1 Classification of RFID attacks model

Table 114.1 Benefits, barriers and attacks of RFID applications in U-healthcare system [7]

Increased safety or reduced medical errors	Interference	Denial of service
Real-time data access	Ineffectiveness	Physical attack
Time saving	Standardization	Tag cloning attack
Cost saving	Cost	Replay attacks, spoofing attack
Improved medical process	Privacy and legal issues	Side channel attack
Other benefits: improve resource utilization	Other barriers: lack of organizational support, security	Tag tracking

each and every RFID tag. Today's technology cannot meet technology because of fabrication of semiconductor could not support high density process. To analyze the performance and security analysis of RFID protocol, we can estimate the following elements [6].

A. Performance analysis

- Computational cost
- Storage requirement
- Communication cost

B. Security analysis

- Data confidentiality
- Tag anonymity
- Mutual authentication and data integrity
- Relay attacks
- Forward security

Imran Erguler et al. described possible attacks to RFID system in their paper. To understand protocols previously published, they referred a classification of RFID attacks and presented a comprehensive analysis of possible security threats and privacy risks in RFID system [4].

- Tag impersonation attack: In this type of attacks, an adversary attempts to impersonate a legal tag to spoof an authorized reader. Thus, the adversary convinces the reader to believe that the fake tags are legitimate.
- Tag tracking attack
- Denial of service attacks
- Replay attack
- Eavesdropping

114.4 Example of U-Healthcare System

The main objective of U-healthcare system with embedded RFID system is to design an e-health system with wireless communication in order to provide customers with convenient and comfortable service. To improve efficiency of tasks for staffs in a hospital, wireless network will be employed so that it could allow mobile and wireless services. The consideration of realizing U-healthcare system, we take into accounts as follows.

- Examination of key factors around wireless technology related to medical environment
- Development of Network design (Cost effective and high performance)
- Development of end user application (Interaction between mobile phone and DB system)
- Secondly, this kind of system will identify security vulnerabilities and threats which could occur during the implementation of e-health system. Security solutions and counter plans will be suggested to mitigate all of risks defined through this project
- Establishment of security policy
- Analysis of various security technologies applied to hospital
- Implementation of security features in the network
- Implementation of security features in the application

Finally, the applications in this system will provide efficient, accurate and real-time health care services. The application development process will follow the developer's project plan. Main features of the applications are described below.

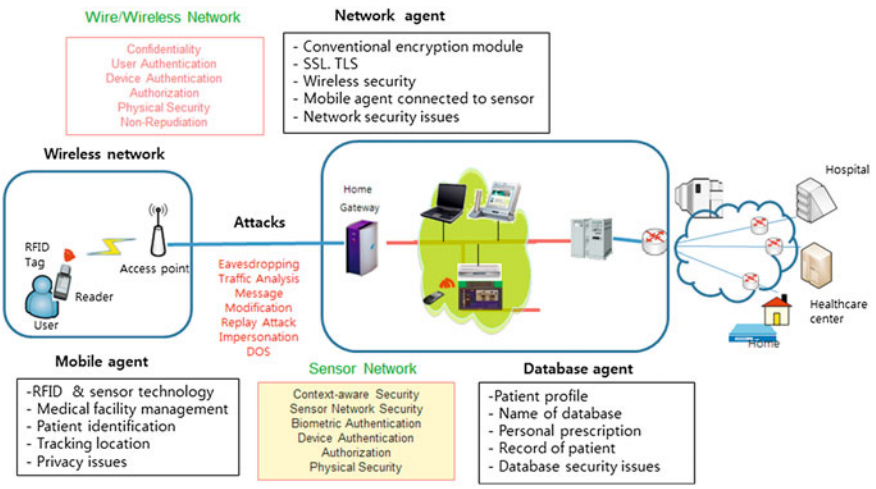

Fig. 114.2 Model of attacks of RFID system under U-healthcare system

- Offer friendly graphic user-interface
- Simple and optimized development process
- Easy maintenance oriented implementation for code recyclability
- Compatibility with database system and end-user device

We described attack model, vulnerable element and security problem under U-healthcare system in Fig. 114.2.

114.5 Conclusion Remarks

RFID system is widely used to identify objects, sensor module. But there are occurred to security problem. We analyzed the attacks and threats in RFID system. To illustrate example, we gave a U-healthcare system. The use of smart phone and sensor devices in the hospital environment can give an opportunity to deliver better services for patients and staffs. Healthcare managers can manage daily's work with easy using blended techniques such as wireless and sensor devices. Applications will continue to grow to support medical service. Finally a challenge in the near future will be development a home healthcare mobile service and integration with hospital service. Open issues are not solved with simple solution. We will try to find out new mechanism to merge several skills.

Acknowledgments This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2012-0007896).

References

1. Poulopoulos G, Markantonakis K, Mayes K (2009) A secure and efficient mutual authentication protocol for low-cost RFID systems. In: 2009 international conference on availability, reliability and security, pp 706–711
2. Schaberreiter T et al (2008) An enumeration of RFID related threats. In: The second international conference on mobile ubiquitous computing, systems, services and technologies, pp 381–389
3. Song B (2009) Server impersonation attacks on RFID protocols. In: The second international conference on mobile ubiquitous computing, systems, services and technologies, pp 50–55
4. Erguler I, Anarim E (2011) Practical attacks and improvements to an efficient radio frequency identification authentication protocol. In: Concurrency and computation: practice and experience, pp 1838–1849
5. Park YJ et al (2012) On the accuracy of RFID tag estimation functions. J Inf Commun Converg Eng 10(1):33–39
6. Eslam Gamal A, Eman S, Mohamed H (2010) Lightweight mutual authentication protocol for low cost RFID tags. Int J Netw Secur Appl 2(2):27–37
7. Hsu C, Levermore DM, Carothers C, Babin G (2007) Enterprise collaboration: on-demand information exchange using enterprise databases, wireless sensor networks, and RFID Systems. IEEE Trans Syst Man Cybern Part A Syst Hum 37(4):519–532