Advanced Science and Technology Letters
Vol.40 (Healthcare and Nursing 2013), pp.101-104
http://dx.doi.org/10.14257/astl.2013.40.24

Requirement of Authentication between RFID tag and Agent for Applying U-healthcare System

Jung Tae Kim

Dept. Of Electronic Engineering, Mokwon University,
800, Doan-dong, Seo-Ku, Daejeon, 302-729, Korea
jtkim3050@mokwon.ac.kr

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 ubiquitous sensor node, it is possible to collect the data from end node and track patient's location without awareness. Even though, concerns about the invasion of personal medical privacy have already appeared in e-health care system and medical industry rules. In this paper, we have analyzed and compared practical threat on U-healthcare system.

Keywords: Attacks, Privacy, Tracking, Security, RFID Protocol.

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. To integrate several open wireless networks into single networks, a lot of consideration should be taken into account to solve challenges for supporting for mobility management, quality of service provision and security interoperability. An integrated security mechanism is one of the key challenges in open wireless network architecture. There are a lot of diversities of the networks in open wireless network architecture. The unique security mechanism used in each of the networks is impossible to utilize secure network because wireless network security is not sufficient to implement required security level. We analyzed attacks on embedded RFID application under U-healthcare system. Integration of RFID system management within the existing enterprise network management framework can be used for re-use of remote monitoring, distributed and collaborative network management concepts. There are many applications to employ RFID utilization. The usages are to migrate from RFID device management towards RFID services management. It can be adaptive self-reconfiguration and self-healing mechanisms of

ISSN: 2287-1233 ASTL

RFID readers. The major application are classified such as real-time data analysis and visualization of RFID operations, RFID policy-based management, RFID asset management, readers' behavior modeling and prediction, efficient and lightweight cryptographic algorithms, new security mechanisms, tailored to RFID applications, and unified and interoperable RFID reader management platforms. Until now, RFID system is widely used to identify objects, sensor module. But many security problems are reported and not solved until now. 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 with embedded RFID system will be widely extended to support medical service and sensor node in wireless networks [1, 2]. The remainder of this paper organized as follows. Section I is the introduction. Section II provides related works of application of RFID for fusion technologies. Section III presents the attacks analysis of protocol and discusses the various security and privacy issues including the associated attack. Section IV provides the attacks model in RFID application under U-healthcare system. Finally, section V gave a conclusion.

2 Model of Attacks in U-healthcare System

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. The current research fields of RFID systems are considerable under five functional elements, namely configuration, fault, performance, accounting and security management [3]. We have to take into consideration privacy, security and performance. To illustrate attach model, they proposed attack tree for the threat of compromising data through the RF-link and listing of threats against availability and risk assessment [4]. When discussing information security of an RFID application, this generalized threat model can be taken as a starting point to build attack trees for each threat relating to this application.

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 protocol separates the authority of hospital doctor, nurse, pharmacy to access to patient's information by level of access authority of hospital which is registered to management server and makes the hospital do the minimum task. We introduced the u-healthcare service network architecture. Particularly we consider u-hospital healthcare network environment in here. The u-hospital network allows the medical steps to use mobile medical devices, to measure and record medical data users, and to get information related to their patient or treatment from HIS. Wei-Bin Lee proposed a cryptographic key management scheme. The proposed process is to facilitate interoperations of multiple cryptographic mechanisms in order to comply with the HIPAA (Health Insurance Portability and Accountability Act) privacy/security regulations. The proposed scheme can be divided into three phases: registration, encryption, and decryption. The decryption phase is subdivided into two cases because of the consent exceptions [4-7].

We described attack model, vulnerable element and security problem under U-healthcare system in figure 1.

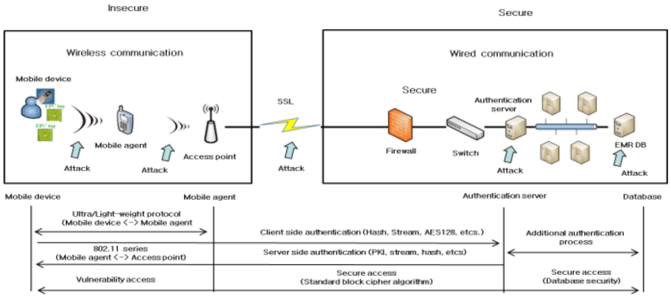
Insecure
Secure
Wireless communication
Mobile device
EPC tag
EPC tag
Mobile agent
Access point
Attack
Attack
SSL
Attack
Wired communication
Secure
Firewall
Switch
Authentication server
Attack
EMR DB
Attack
Mobile device
Mobile agent
Authentication server
Database
Ultra/Light-weight protocol (Mobile device <-> Mobile agent
Client side authentication (Hash, Stream, AES128, etcs.)
Additional authentication process
802.11 series (Mobile agent <-> Access point)
Server side authentication (PKI, stream, hash, etcs)
Vulnerability access
Secure access (Standard block cipher algorithm)
Secure access (Database security)

Fig. 1. Model of Attacks of RFID System under U-healthcare System

The authentication between and tag are as follows. We have to consider the attack issues in each protocol level.

A. Registration Phase

After reading the “Notice of Privacy Practices,” each patient has to register at SG. The patient signs and dates the permitting consent to verify acceptance of the PHI access rules, and further sends the signed consent with his/her fundamental data to SG. When receiving the request, SG first checks the validity of the received consent and then creates contract. The contract consists of the signed consent, the data received from the patient, and a summary of the duties of SG as well as its fundamental data, such as identification or name of the organization.

B. Encryption Phase

For simplicity, assume that M is the PHI (Protected Health Information) part of the health information and R represents the remaining parts. To ensure confidentiality and privacy, M must be encrypted. To encrypt PHI, the patient must enable the health data card by entering his/her PIN or verifying the biometric information. The enabled card will do the following to encrypt M.

C. Decryption Phase

The purpose of the decryption phase is to reveal the encrypted PHI. Without a legal authorization, disclosure of PHI would damage a patient’s privacy, and is, therefore, forbidden. Hence, construction of the appropriate operations in the decryption phase is a means to protect privacy and rights of a patient. Due to the consideration of whether the patient is directly involved, two cases have to be discussed in this phase.

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.

3 Conclusion Remarks

RFID system is widely used to identify objects, sensor module. But there are occurred many security problem. We analyzed the attacks and threats in RFID system, especially. Also, we have surveyed security, and user's privacy in RFID protocol. Many schemes are published to secure against replay attacks, tracking attacks, tag spoofing, denial of service attacks, attacks against users' privacy so far. But there are many open issues in RFID system.

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: 2013-052980)

References

1. George Poulopoulos, Konstantinos Markantonakis and Keith Mayes.: A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems. In: 2009 International Conference on Availability, Reliability and Security, pp.706-711 (2009)
2. Boyeon Song.: Server Impersonation Attacks on RFID Protocols. In: The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp.50-55. (2009)
3. Imran Erguler and Emin Anarim.: Practical attacks and improvements to an efficient radio frequency identification authentication protocol. In: Concurrency and Computation: Practice and Experience, pp.1838-1849, (2011)
4. Thomas Schaberreiter, et al.: An Enumeration of RFID Related Threats. In: The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp.381-389. (2008)
5. Cheng Hsu, David M. Levermore, Christopher Carothers, and Gilbert Babin, Enterprise collaboration.: On-demand information exchange using enterprise databases, wireless sensor networks, and RFID Systems. In: IEEE Transaction on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol.37, no.4, pp.519-532 (2007)
6. Young-Jae Park, et al.: On the accuracy of RFID tag estimation functions. In: Journal of Information and Communication Convergence Engineering (JICCE), vol.10, no.1, pp.33-39 (2012)
7. Eslam Gamal Ahmed, Eman Shaaban and Mohamed Hashem.: Lightweight Mutual Authentication Protocol for Low Cost RFID Tags. In: International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010, pp.27-37. (2010)