International Journal of Bio-Science and Bio-Technology
Vol.6, No.3 (2014), pp.109-116
http://dx.doi.org/10.14257/ijbsbt.2014.6.3.13

Authentication Process between RFID tag and Mobile Agent Under 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 with embedded healthcare system have been widely studied. The representative vulnerabilities include eavesdropping, replay attacks, denial of service attacks, tracking, and traceability. Considering this RFID security issues, we analyzed the security threats and open problems related to these matters. In ubiquitous system with sensor node, we use small and limited resources and low memory. Then the application with these kinds of have lots of vulnerabilities and attacks such RFID protocol in healthcare system. Even though, concerns about the disclosure of personal medical privacy in e-healthcare system have already appeared. In this paper, we 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 breakthrough technologies for applying ubiquitous surroundings. The application system plays an important role for object identification such as ubiquitous infrastructure and wireless sensor networks. To integrate several heterogeneous open wireless networks into single networks domain, a lot of consideration and requirements should be taken into account to solve challenges, risks and threats 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 and ubiquitous application. There are a lot of diversities of the networks in open wireless network architecture. It is impossible to utilize only one security mechanism in open network topologies because wireless network is not sufficient to implement required security level with conventional security mechanism [1]. Especially, privacy is an important factor of pervasive and ubiquitous computing systems. With reference to previous approaches on developing privacy in sensitive and pervasive healthcare applications, many researchers made a framework to minimize the impact of privacy and security issues on such systems. Advanced technologies and existing medical technologies should be combined properly to meet requirements for service efficiency, accuracy and clinical significance. To design privacy sensitive ubiquitous systems, it is necessary to consider the properties of privacy, and how to solve ubiquitous computing impacts upon these properties. Information privacy is usually concerned with the confidentiality of PHI (Protected health information) such as EMR (Electronic medical records). Any vulnerability of security may cause a leakage of personal information. Therefore, security protocols should be prepared and considered prior to the implementation of u-healthcare system. Wireless sensor networks give many efficient advantages for ubiquitous health monitoring, improving

ISSN: 2233-7849 IJBSBT

users' well-being, making the healthcare system more efficient, and helping to quickly react on emergency situations. The strict security needs and requirements of ubiquitous medical applications is a big challenge. Also safety and privacy of patient data should be guaranteed from the sensor nodes to the back-end services, the system should be fulfilled latency needs, and lots of mobility devices. The owner of personal information will also suffer from hackers and malicious attackers. Their healthcare information has been exposed to a security breach by hospitals, physician offices and other healthcare organizations. Personal perceptions with health records on privacy and security are critical to maintain trusty information and reliabilities with their healthcare providers and their acceptance of electronic health records, whether or not they are for personal usage. 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 model of attacks in U-healthcare system. Section IV provides the security analyses in RFID application under U-healthcare system. Finally, section V made a conclusion.

2. Related Works

RFID system is widely used to identify objects and sensor module. But there are occurred to security problem and attacks, we analyzed the attacks and threats in RFID system. To illustrate example, we introduced a u-healthcare system based on wireless and wired system. The use of smart phone and sensor devices in hospital environment can give an opportunity to deliver better services for patients and staffs. Healthcare managers can operate daily's work easily using blended techniques such as wireless and sensor devices. These kinds of applications will grow to support medical service and M2M (Machine to machine) application. Finally a challenge in the near future will be developed and applied to a home healthcare service with mobility and integration applicable to u-healthcare system. Open issues cannot be solved with simple solution. Because we have to consider different security mechanism compared to conventional method. A lot of works have been done. Most of works focus on protocol matters between tag and network by using hash or encryption. But there are not mentioned of the privacy management mechanism. In order to ensure personal privacy protection service, a mechanism that encrypts and decrypts the outgoing data from tag and server has been proposed [2]. Simon Moncrieff proposed a framework for the design privacy preserving pervasive healthcare [3]. David Daglish analyzed a design and architectural issues of PHR systems, and focused on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable matters to consumers [4]. Kai wnag summarize some typical healthcare services, pervasive healthcare system can be provided, identified integration and security challenges regarding to pervasive healthcare systems. Specially, he proposed some solutions to these challenging problems [5]. Although pervasive healthcare system can be improved by the productivity of healthcare practitioners, they greatly can facilitate the delivery of a wider range of medical services, privacy and security needs in the most serious potential problems. Based on the unique characteristics among various wireless technologies, various cryptographic protocols are used to secure system against the attacks such as DOS (Denial of service), interception, manipulation, masquerading and repudiation. The MIS (Medical information system) is a typical collaborative computing application, staffs such as physicians, nurses, professors, researchers, health insurance personnel, share patient information and collaboratively conduct critical tasks through the networking system. Byunggil Lee proposed a customized policy based privacy management architecture for medical and healthcare application. The proposed mechanism is a useful solution for user centric privacy management in medical environment [6]. Remote health

monitoring has tremendous potential to improve quality of health care services in modern and ubiquitous medical environments. It helps to reduce the cost in modern healthcare by avoiding unnecessary hospital visits for frequent checkups. Debargh Acharya presented an overview of current security threats in pervasive healthcare applications and analyzed the outstanding issues and future challenges [7].

3. 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 depicted feasible threats by observing and manipulating communications between a server and tags. Replay attacks and interleaving attacks are examples of weak attacks. Strong attacks are threats by attackers in compromised a target tag part. An RFID tag's memory is vulnerable to compromise with conventional cryptographic mechanism. When the tags are attacked by side channel attacks, it can be serious security problem because the memory of a low cost tag is unlikely to be tamper-proof. The main reason is that tags have a limited resources and small memory to implement cryptographic functions. The current research fields of RFID systems are considerate with five functional elements, namely configuration, fault, performance, accounting and security management [8]. The representative security threats for RFID applications are tag cloning, privacy invasion, DoS (Denial of services), location-based attacks, and side channel analysis. To overcome the threats, we have to take into account following security properties such as mutual authentication between tag and reader/back-end server, forward security, secure key exchange and secure tag location. Particularly, for taking an example, we introduces u-hospital healthcare network environment. 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. Most of protocols between sensor node such as tag and mobile agents have fundamental flaws. The recent examples are shown in Table 1.

Table 1. Comparison of Security Analyzes for Different Protocols [9]

	LMAP	M2AP	EMAP	SASAI	JK	Enhanced-JK
Mutual Auth.	O	O	O	O	O	O
Eavesdropping	X	X	X	O	O	O
Reply attack	X	X	X	X	O	O
Spoofing	X	X	X	X	O	O
DOS	X	X	X	X	O	O
Position detection	X	X	X	X	^	O
Forward attack	X	X	X	X	^	O

O means satisfactory, X means partial satisfactory and ^ means unsatisfactory.

We described threats, attacks, vulnerable elements and security problem under u-healthcare system as shown in Table 2.

Table 2. Threats of RFID Applications in U-healthcare System [10]

Threats	Affected RFID component	Risk mitigation
Rogue reader	Tag, Air-interface, reader	Reader authentication
Eavesdropping	Tag, Air-interface	Encryption the data, shielding the tag or limit the tag-reader distance
Reply attack	Air-interface	Using short range tags, shielding the tag or implementing the distance bounding protocol
Replay attack	Tag, Air-interface	Encryption the data, shielding the tag or limit the tag-reader distance, tag authentication
Tag cloning	Tag, Air-interface	Tag authentication
Tracking object	Tag, Air-interface	Low range tags or shielding tags, authenticating the readers or disabling the tags
Blocking and jamming	Air-interface	Detect early and localize, take appropriate action
Physical tag damage	Tag	Use protective material

We described the u-healthcare service network architecture as shown in Figure 2. The system consists of wired devices and wireless devices which can be communicated with wireless channel such as WLAN, CDMA, Bluetooth and RF channel. The proposed scheme can be divided into three phases: registration, encryption, and decryption. The decryption phase is subdivided into two cases considering consent exceptions. The elements of attacks of each part of network are classified as shown in Figure 1 [11].

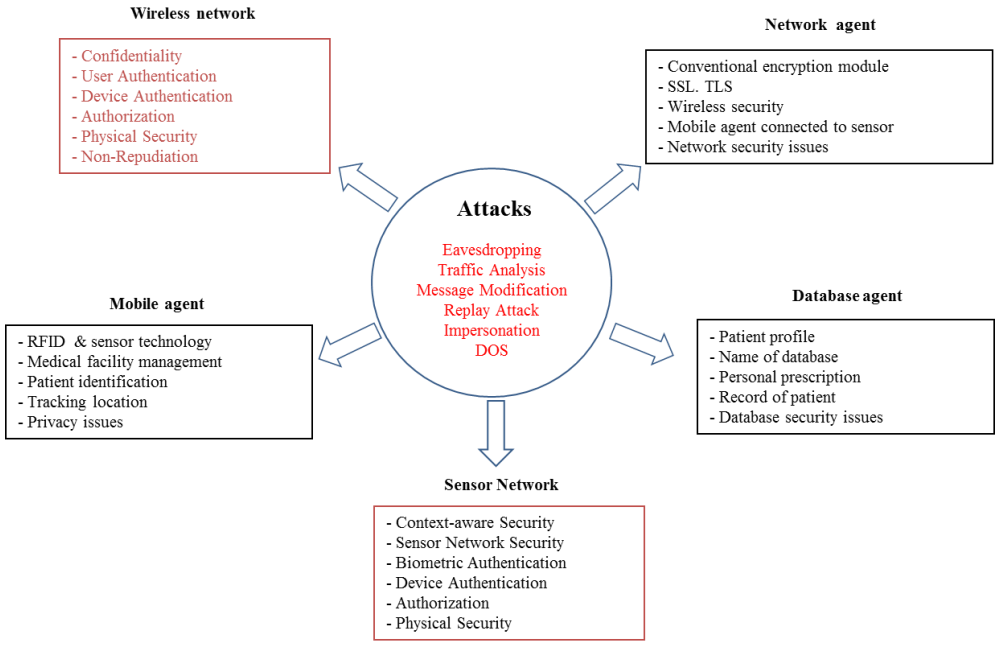

Figure 1. Model of Attacks of RFID System under U-healthcare System

The authentication between tag and database are as follows. We have to consider the attack issues in each protocol level as shown in Figure 1[12].

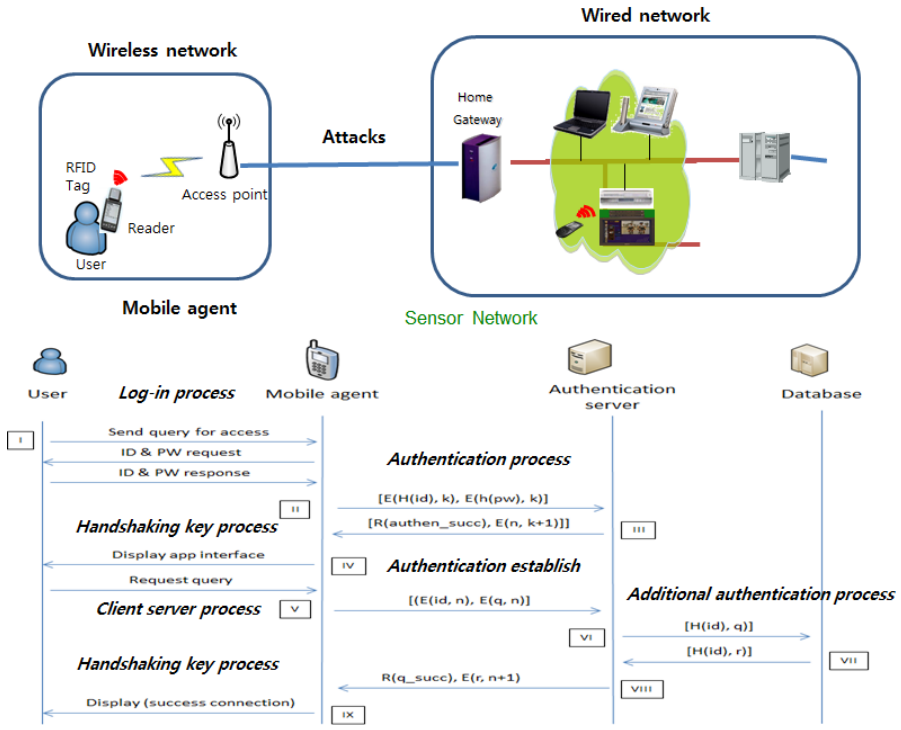

Figure 2. Model of Attacks of RFID System under U-healthcare System

As a first step of security, well-organized authentication processes based on network should be prepared against various threats especially for wireless networks. To connect database to conform user's identification, we consider three phase.

A. Registration Process

To confirm user's authentication, user send query to mobile agent, mobile agent request tag's ID to identify tag's ID, after user's tag is justified, the mobile agent request authentication process with hash function to authentication serve. For example, each patient' information has to register at server. 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 data to server. When receiving the request, server first checks the validity of the received consent and then creates authentication process. The server consists of the confirmed user's tag information and the data received from the patient such as identification or name of the organization.

B. Authentication Process

The mobile agent sends user's tag information with hashed data to authentication server. The server compares the user's tag information with data stored in server. If there is exactly equal the tag's information, the server can authenticate the tag. To ensure confidentiality and privacy, tag's information must be encrypted. To encrypt PHI, the patient must enable the health data card by entering his/her PIN or verifying the biometric information.

C. Additional Authentication Process

Mobile agent received server's confirmation and sends the result of authentication information. At this time, the process can be operated handshaking key process. Each tag has capability for generating random number. Even if the attacker gets the information in the tag, it cannot be able to find any relation between the current output and past output. Thus, it cannot trace the information back through history events related to the tag. It can protect from eavesdroppers because it provides un-traceability and forward security.

4. Security Analyses

This mechanism provides not only reader to tag authentication but also tag to reader authentication which is used to prevent an unauthorized user from accessing the tag or updating its data to the tag. After additional authentication process, multi-level security mechanism is recommended by hashed based cryptographic primitive compared to security mechanism which can often be used in real industries. The information can be categorized as below. In terms of mutual security, the use of ID and password for access to EMR database can be vulnerable. While, authentication using the digital certificate will prevent illegal access even if hackers obtain the user's ID and password. Through connection between the database and the reader, information is transmitted in plaintext. Since the protocol only authenticates the tag and database which leaves the reader alone, a spoofed reader can access to the information for the tag. Also, each individual or group will be assigned different authorization for access to database based on their role. To disclose information, hackers or unauthorized person need to know all different encryption methods and their keys. In many practical applications, the transmitted information could be eavesdropped more easily because the connection between the database and mobile agent is via wireless networks. The latest wireless devices may be required because some of old devices cannot support WPA2 (Wi-Fi Protected Access2), but it could be worth to invest in new devices because it may provide mutual security to the wireless hospital system in the future [13]. Jelena Misi proposed healthcare wireless sensor networks implemented using 802.15.4 beacon enabled technology, in which security processors are implemented with low power microcontrollers. In this setting, we propose to use elliptic curve cryptography for key distribution, in order to decrease energy consumption compared to the better known RSA algorithm [14].

5. Conclusion

The usage of a mobile device or agent in hospital environment offers an opportunity to deliver better services for patients and staffs. Furthermore, to reduce medical errors and to use friendly u-healthcare system based on mobile or sensor node is useful for medical process. Optimized security protocols and mechanisms are employed for the high performance and security. We analyzed security issues to estimate performance, threats and performance of security related to issues by means of information security and privacy. The security functions to be adopted in a system, strongly depend on the application. In future work, we have to develop a ultra-lightweight cryptographic primitive, this can be realized by means of semiconductor process in the future.

Acknowledgement

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] Y.-J. Park and Y. B. Kim, "Accelerating RFID Tag Identification Process with Frame Size Constraint Relaxation", Journal of Information and Communication Convergence Engineering, vol.10, no.3, **(2012)**, pp. 242-247.
[2] J. Jensen, I. A. Tondel, M. G. Jaatun, P. H. Meland and H. Andresen, "Reusable Security Requirements for Healthcare Applications", Proceedings of 2009 International Conference on Availability, Reliability and Security, **(2009)**, pp.380-385,
[3] S. Moncrieff, S. Venkatesh and G. West, "A Framework for the Design Privacy Preserving Pervasive Healthcare", Proceedings of 2009 IEEE International Conference on Multimedia and Expo (ICME2009), **(2009)**, pp.1696-1699.
[4] D. Daglish and N. Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", Proceedings of 2009 World Congress on Privacy, Security and Trust and the Management of e-Business, **(2009)**, pp.110-120.
[5] K. Wang, Y. Sui, X. Zou, A. Durresi and S. Fang, "Pervasive and Trustworthy Healthcare", Proceedings of 22nd International Conference on Advanced Information Networking and Applications, **(2008)**, pp. 750-755.
[6] B. Lee and H. Kim, "Privacy Management for Medical Service Application using Mobile Phone collaborated with RFID Reader", Proceedings of Third International IEEE Conference on Signal-Image technologies and Internet-Based System, **(2008)**, pp.1053-1057.
[7] D. Acharya, "Security in Pervasive Health Care Networks: Current R&D and Future Challenges", Proceedings of Eleventh International Conference on Mobile Data Management, **(2010)**, pp.305-306.
[8] I. Erguler and E. Anarim, "Practical attacks and improvements to an efficient radio frequency identification authentication protocol", International journal of Concurrency and Computation: Practice and Experience, **(2011)**, pp.1838-1849.
[9] D. Jeon, S. Choi and S. Kim, "An Enhanced Forward Security on JK-RFID Authentication Protocol", Journal of the Korea Institute of Information Security and Cryptology, vol.21, no.5, **(2011)**, pp.161-168.
[10] H.-Y. Chien,"Varying Pseudonyms-Based RFID Authentication Protocols with DOS Attacks Resistance", Proceeding of In 2008 IEEE Asia-Pacific Services Computing Conference, **(2008)**, pp.507-615.
[11] W. Yao, C.-H. Chu and Z. Li, "The use of RFID in healthcare: Benefits and barriers", Proceedings of IEEE International Conference on RFID Technology and Applications, **(2010)**, pp.128-1342.
[12] Jung Tae Kim, "Requirement of Authentication between RFID tag and Agent for Applying U-healthcare System", Proceedings of International workshop on Healthcare and nursing, **(2013)**, pp.101-104.
[13] Jung Tae Kim, "Enhanced secure authentication for mobile RFID healthcare system in wireless sensor networks", Proceeding of Future Generation Information Technology Conference, **(2012)**, pp.190-197.
[14] Jelena Misi, "Enforcing Patient Privacy in Healthcare WSNs Using ECC Implemented on 802.15.4 Beacon Enabled Clusters", Proceedings of Sixth Annual IEEE International Conference on Pervasive Computing and Communications, **(2008)**, pp.686-691.

Author

Jung Tae Kim, he received his Ph.D. degrees in Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI, where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information security technology that includes network security system design, RFID&USN and wireless security protocol.