International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.59-66
http://dx.doi.org/10.14257/ijsia.2014.8.4.06

Attacks and Threats on the U-Healthcare Application with Mobile Agent

Jung Tae Kim

Mokwon University, Dept. of Electronic Engineering
Doanbuk-ro 88, Seo-gu, Daejeon, 302-729, Korea
jtkim3050@mokwon.ac.kr

Abstract

Wireless sensor network is widespread used in hospital environment with mobile device such as NFC, RFID tag and small sensor nodes. The use of a mobile agent in healthcare system under wireless network environment gives an opportunity to offer better services for patients and staffs such as doctors and nurses because of its mobility. But, optimized security protocols and schemes between sensor and patient device are essential for high performance and security problem in U-healthcare system. But a lot of threats, attacks and vulnerability are induced because of limited resources such as small memory and low computation capability in wireless sensor network. The characteristics of U-healthcare systems are analyzed to solve security issues in this paper.

Keywords: *Mobile agent, RFID, privacy and healthcare system, security issues*

1. Introduction

During last few years, many new technologies have been rapid developed in application of RFID (Radio frequency identification) system. The rapid development and changes of information technology give an effect on the healthcare system and life style in the future. As information technologies are developed rapidly in a variety of application. Especially, existing e-healthcare system has been realized in wired communication with specialized area such as database and network protocol in hospital environment. The rapid changes of modern technologies usually provide new requirement, request and give a new chance to generate new market and industry. Ubiquitous technologies based on mobile devices and sensor nodes can be applied and managed in healthcare information. Recently the trend of healthcare system has moved to U-healthcare system with wireless and mobility characteristics, many new technologies enable smart equipment and devices with low computing power to utilize wireless sensor nodes. These kinds of mechanism and devices can be fused with different compact devices module. Application of RFID enabled patient tracking within regional perspective of hospitals is major concerns because of its vulnerabilities and threats. But, it can be improved patient's safety and nursing efficiency and reduced manual handling error, monitor patient's medical information, and process efficiency. Therefore, it decrease healthcare expenses but it leads to security problem because of limited resources in smart device. This kind of fusion technology is called ubiquitous healthcare system, and it is highlighted technology that U-healthcare system makes many benefits and gives high quality of life. It also improves constraints and medical treatments by joining a living space and a medical treatment together [1]. Nevertheless the healthcare system is still faced with many difficulties in implementing RFID technologies due to security, privacy and cost matters. The major benefit of RFID technology includes the increasing patient's safety and saving more

ISSN: 1738-9976 IJSIA

lives with its mobility and usability. Wen Yao, et al, surveyed the use of RFID in healthcare system about benefits and barriers by analyzing distributed of literatures, benefits of RFID applications in healthcare and barriers to RFID adoption in healthcare system. RFID systems should be considered to resist all kinds of attacks and threats. Until now, many works have done on function about security matters how they can implement the standard cryptographic. But, a lot of security threats and violation attempts exist in RFID system which is unsolved yet. The application system is moving and converging on IoT (Internet of Things). Hailong Feng, *et al.,* surveyed a recent development about privacy and security of Internet of things [2]. In the future, RFID systems using cloud computing service as back-end database and computational capacity is strongly relevant when there are multiple facility providers who are connected to an executive company [3].

2. Related Works

As an initial model of U-health system, m-health system is designed as an enhancement of e-health system supported by wireless EMR (Electronic Medical Record) access. The rapid developments in technology and semiconductor process made their cost to reduce sharply and new technologies to emerge. As a result of reduced cost of RFID, hardware became cheaper with more storage capacity and enhanced processing power. It gives a standard algorithm to be implemented in real world. These developments made it possible for the technology to be more adopted among different industries [4]. Although RFID can provide trustworthy benefits in the healthcare industry, it is not widely used due to the lack of security on the RFID tags and limited space for data storage. To solve this kind of concerns, Li-Shiang Tsay, *et al.,* proposed an integrated framework to build a RFID card system by embedding smart tags in insurance cards, medical charts, and medical bracelets to store medical information. Their scheme gives and simplifies the maintenance and transfer of patient data in a secure, feasible and cost effective way [5]. Figure 1 depicts a concept of the network topology for the U-health system. It represents a brief network topology for a virtual hospital. This kind of network can be modified and extended based on the requirement of the security issues and protocol requirements. To overcome the additional vulnerabilities, wireless security architecture should be designed with essential requirement for wireless access. Especially, patient's privacy concerns are very important in HIS (Hospital information system) environment. The information should be secured safely, either when transmitted or stored in databases. At the end of network topology, mobile device and wireless access point are utilized to implement a visual interaction between the end device and the database servers through network and air medium. It is essential for an enterprise information system to obtain real-time data from the distributed and dynamic manufacturing environment for decision making. Wireless sensor network and radio frequency identification systems provide excellent infrastructure for data acquisition, distribution, and processing. Li Wnag, *et al.,* proposed that some key challenges related to the integration of WSN and RFID technology are presented. Five layer system architectures have been proposed to achieve synergistic performance. For the integration of WSN and RFID, one of the critical issues is the low efficiency of communication due to redundant data as redundant data increases energy consumption and causes time delay. They addressed improved data cleaning algorithm with simulation results [6]. Haluk Demikan, *et al.,* proposed a smart healthcare systems framework. He focused on a smart healthcare systems framework for conceptualizing data-driven and mobile and cloud enabled smart healthcare systems. With the adoption of smart healthcare system, healthcare organizations can provide cost-effective quality healthcare services with less IT set-up costs and reduced risk [7]. Hyeong-Chan Lee proposed improved limitations of exiting RFID authentication protocols and achieved the same security level and performance

that can be obtained through active tags. The proposed protocol meets various security requirements such as tag protection, location and traffic tracking prevention with lightweight protocol and the desired level of performance [8]. Heung-Kuk Jo, *et al.*, have been experimented the transmission of tag's ID over wireless and TCP/IP communication. By using this scheme, RFID systems can be simply installed and made long distance monitoring [9]. As advanced technologies of computer and networking technology are converging different devices, pervasive computing is regarded as key technology to assist real time medical and healthcare information service with deploying different kinds of sensor, communication with wireless sensor networks, interpreting sensor data and developing large number of medical and healthcare service. Bing Wang, *et al.*, evaluated RFID and Wi-Fi technologies for RTLS (Real time location system) applications in healthcare organization. They also give retrieval guideline for the RTLS selection and demonstrated with RFID and Wi-Fi technologies [10]. In recent years, hospitals are introduced by wireless communication systems. However, not many hospitals are aware of the security issues because their working process is mainly focused on emergency than security. This may result in a security problem such as information leakage. Therefore, we reviewed a suitable wireless security mechanism for the hospital. The characteristics of the hospital organization should be analyzed before selecting the wireless mechanism. To overcome the additional vulnerabilities and security problem, wireless security architecture should be designed with essential requirement for wireless EMR access. Especially patient' privacy and security issues should be considered more important in hospital information system environment.

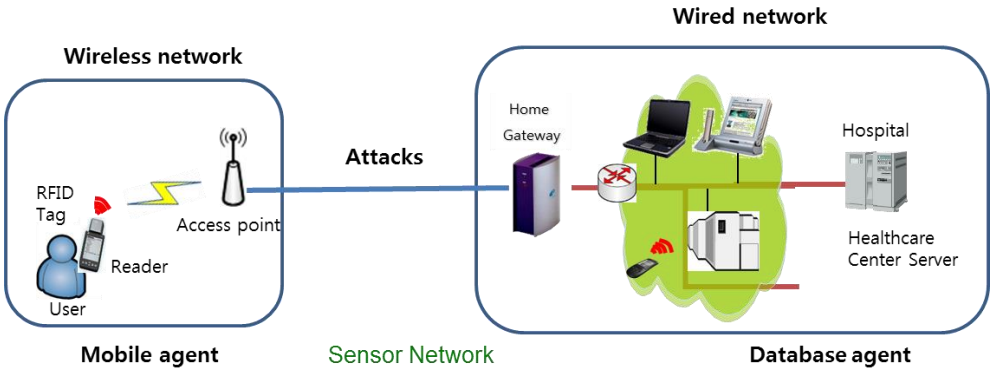

Figure 1. Model of Ubiquitous Healthcare System

3. Attacks and Threats of RFID Protocol

This section introduces a concept of security layer for RFID system. Figure 2 depicts security problem in each layer. The architecture is divided into four layers: user layer, network layer, application layer and database layer. Each layer contains several elements to support their function. To realize U-healthcare system, we should take into consideration components such as confidentiality by authentication and encryption, data privacy, confidentiality, and availability by authorization, encrypted database and backup of database. The measures can be categorized into four security layers [11]: Authentication based on network, authentication based on application, database protection and user's privacy. Wie Tounsi, *et al.*, analyzed security solutions to protect the communication of the wireless components of a healthcare system and outlined some important aspects that must be guaranteed given the existence of low-cost and resource constrained RFID components. To evaluate key exchange protocols for resource-constrained devices, we should consider the

following evaluation criteria such as computation costs and communication costs [12]. To protect users from tracing attack, Kavitha S. M, *et al.*, proposed a hardware implementation of RFID with secure mutual authentication protocol [13].

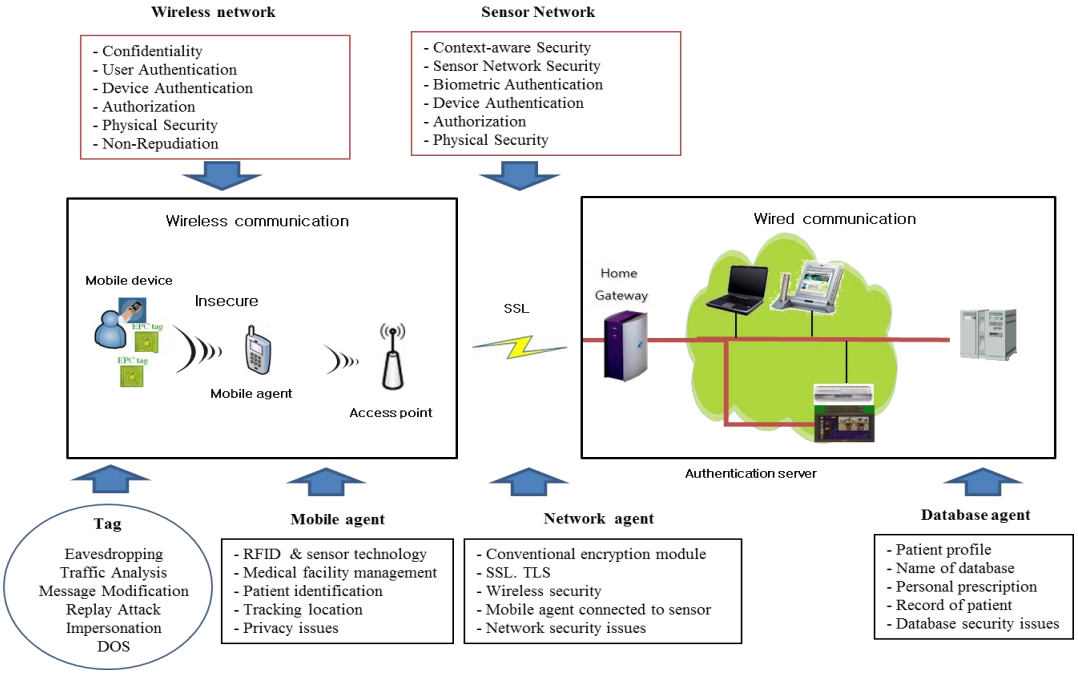

Figure 2. Example of Attacks Model of Ubiquitous Healthcare System

To exchange secret information over Internet, it is necessary to secure the channel in advance. The security may be applied into the different layers of the TCP/IP model. One of the most common technologies used to ensure secure communication in the Internet is IPsec (Internet Protocol Security) protocol. IPsec is an end-to-end security scheme operating in the IP stack, enabling both authentication and confidentiality. Although IPsec ensures, this security service to any protocol in the upper layers. At the transport layer, the SSL (Secure Socket Layer) protocol is standard model which is used all over the Internet. SSL protocol replaces the TCP/IP sockets with SSL sockets and simplifies the implementation of a secure end-to-end secure channel. Although SSL provides a very good solution and simple technique, it authenticates only the devices in both ends, TLS (Transport Layer Security) is developed and utilized these days. Until now, no normalized and standard protocol has been yet released.

These evaluation criteria are used to guide us to decide on the capacity of some selected protocols to evaluate the limited costs incurred by the set of nodes.

To solve security problems such as disclosure of private information, malicious tracking, impersonation behaviors, protocol of RFID should be required to meet following characteristics.

▪ Confidentiality: Transmitted information should be protected, and sensitive information should not be disclosed, such as healthcare card, condition and personnel records.

▪ Falsification: Attackers could not disguise as tags or readers for cheating

▪ Location privacy: Location privacy of a user should be protected. Attackers could not judge the past location with tag; in other word, attackers could not judge the tracking object from the information of a tag.

▪ Scalability: The communications between tags and servers should be rapid and efficient to be applied.

Even though many works have been done for many security threats with RFID technology, but many issues are still unsolved and some others need to be investigated. These issues can be solved following scheme [14].

▪ Functional lightweight cryptographic primitives:
▪ Possibility of certain cryptographic tasks:
▪ Security model for new techniques: multiple tags scanning:
▪ Effective methods against location-based attacks:
▪ Protection against side channel analysis:

The design of an efficient and secure protocol for RFID systems with simple cryptographic techniques is an important issue. Although many authentication protocols have recently been developed for RFID, they either cannot protect the location privacy of tags nor have high overhead on identifying tags for the back-end server. None of them provide satisfactory solutions for both problems at the same time. Zen-Yu Wu, *et al.*, proposed and compared an efficiently mutual authentication scheme for RFID that not only verifies the location privacy of tags, but also efficiently identifies tags for the back-end server [15].

We should consider the following measures for security protocol.

A. Secrecy/Authentication

The cryptographic methods used and reasonably guarantee the secrecy of the message. Thus, we assure the recipient that the messages originate from valid sources.

B. Indistinguishableness/Tracking/Passive Replay

Using a freshly generated random nonce with every message in the protocol, it is impossible to track the tag. Of course, with multiple tags in an area, tracking a specific tag without keys is extremely difficult if not impossible.

C. Forward Security

This means that the current key of a tag has been found, and can be used to extract previous messages. The tag always communicates using a hash function. The adversary cannot use the key to decode any of the tag's messages because the one-way hash function is considered computationally un-invertible. There are a number of solutions proposed so far to solve the security problems and threats associated with the use of RFID systems [16]. Comparison of benefits, barriers and attacks of RFID applications in healthcare system is shown in Table 1.

Table 1. Benefits, Barriers and Attacks of RFID Applications in Healthcare System

Benefits	Barriers	Attacks
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

Nowadays, RFID application can be applied in many fields for a variety of applications. Although having a great productivity benefits, RFID systems may cause new security and privacy threats to individuals or organizations. Therefore, it is important to protect the security of RFID systems and the privacy of RFID tag owners. Unfortunately, none of the existing solutions provide the contents of tags. Kazuya Sakai, *et al*., proposed two RFID backward channel protection protocols, namely dynamic bit encoding and optimized dynamic bit encoding and analytical models to estimate simulation results [17].

4. Conclusion

The health information system based on the wireless network infrastructure is generally adapted nowadays. As a part of the wireless network, a mobile device and agent has been employed in hospitals environmental. Especially, RFID system is widely used to identify objects, sensor module and IoT (Internet on Things) services. But there are occurred a variety of security problem. We surveyed U-healthcare system with small devices such as RFID and NFC. A challenge in the near future will be developed a home healthcare mobile service and integration with hospital service. Until now, open issues are not solved with simple solution with conventional techniques because of wireless characteristics. We will apply new schemes to merge several skills to solve open security issues.

Acknowledgements

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. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung and J. H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks", IEEE Journal on Selected Areas in Communications, vol. 27, no. 4,**(2009),** pp. 400-408.
[2] H. Feng and W. Fu, "Study of Recent Development about Privacy and Security of the Internets of Things", 2010 International Conference on Web Information Systems and Mining, **(2010),** pp. 91-95.
[3] J. T. Kim, "Analyses of Attacks and Vulnerability on the U-healthcare System", 2014 International Conference on Green and Human Information Technology, **(2014),** pp. 309-312.
[4] J. A. Rrub, J. Al-Jabi and K. El-Khatib, "Security Model for Real Time Tracking System in the Healthcare Sector", The 2nd Internal Conference on Communications and Information Technology: Wireless Communication and Signal Processing, **(2012),** pp. 360-373.
[5] L.-S. Tsay, "Avery Williamson and Seunghyun Im, Framework to Build and Intelligent RFID System for Use in the Healthcare Industry", Conference on Technologies and Applications of Artificial Intelligence, **(2012),** pp. 109-112.
[6] L. Wang, L. D. Xu, Z. Bi and Y. Xu, "Data Cleaning for RFID and WSN Integration", IEEE Tran. On Industrial Informatics, vol. 10, no. 1, **(2014)** February, pp. 408-418.
[7] H. Demirkan, "A Smart Healthcare Systems Framework, Software Engineering", IT Pro, **(2013)** September, pp. 38-45.
[8] H.-C. Lee and J. H. Yi, "Development of Privacy-Preserving RFID Authentication System Using Mobile Devices", ICTC2011, **(2011),** pp. 760-765.
[9] H.-K. Jo and H.-J. Lee, "A Relay Transmission of the RFID tag ID over the Wireless and TCP/IP with a Security Agent", Springer-Verlag, LNAI4496, **(2007),** pp. 918-927.
[10] B. Wang, M. Toobaei, R. Danskin, T. Ngarmnil, L. Pham and H. Pham, "Evaluation of RFID and Wi-Fi Technologies for RTLS Application in Healthcare Centers", 2013 Proceedings of PICMET'13: Technology Management for Emerging Technologies, **(2013),** pp. 2690-2703.
[11] W. Yao, C.-H. Chu and Z. Li, "The Use of RFID in Healthcare: Benefits and Barriers", IEEE International Conference on RFID Technology and Applications, **(2010),** pp. 128-1342.

[12] W. Tounsi, "Securing the Communications of Home Health Care Systems based on RFID Sensor Networks", 8th Annual Communication Networks and Services Research Conference, **(2010),** pp. 284-291.
[13] S. M. Kavitha, T. Suresh and J. M. Rani, "MRFID Implementation with Secure Mutual Authentication Protocol", International Conference on Computing, Electronics and Electrical Technologies, **(2012),** pp. 746-751.
[14] P. Olla, "Mobile Health Technology of the Future: Creation of an M-Health Taxonomy based on Proximity", International Journal of Healthcare Technology and Management, **(2007),** pp. 370-387.
[15] Z.-Y. Wu, T.-L. Chen, S.-C. Lin and C. Wang, "A Secure RFID Authentication Scheme for Medicine Application", 2013 Seventh International Conference on Innovative and Internet Services in Ubiquitous Computing, **(2013),** pp. 175-181.
[16] D.-H. Jeon, S.-U. 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.
[17] K. Sakai, W.-S. Ku, R. Zimmermann and M.-T. Sun, "Dynamic Bit Encoding for Privacy Protection against Correlation Attacks in RFID Backward Channel", IEEE Transaction on Computers, vol. 62, no. 1, **(2013)** January, pp. 112-123.

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 (Electronic Telecommunication Research Institute), 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 optical security technology that includes network security system design, RFID&USN and wireless security protocol.