무선 센서 네트워크에서의 유비쿼터스 헬스케어 시스템을 위한 보안 구조

신윤구, 김한규, 김수진, 김정태
목원대학교

Security Architecture for U-Healthcare Application in Wireless Sensor Network

Yoon-gu Shin, Hankyu Kim, Sujin Kim, Jung Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

ABSTRACT

The use of Radio Frequency Identification technology (RFID) in medical context enables not only drug identification, but also a rapid and precise identification of patients, physicians, nurses or any other health care related staffs. The combination of RFID tag identification with structured and secured Internet of Things (IoT) solutions enables ubiquitous and easy access to medical related records, while providing control and security to all interactions. This paper surveyed a basic security architecture, easily deployable on mobile platforms, which would allow to establish and manage a medication prescription service in mobility context making use of electronic personal health records.

Keyword
RFID, IoT, Security issues, Wireless sensor network

Ⅰ. Introduction

A wireless sensor network (WSN) is an ad hoc wireless network composed of a large number of small sensor nodes collecting environmental data. Emerging as a new technology, WSNs have a wide range of potential applications, especially in the realtime monitoring scenarios, such as battlefield surveillance, wildlife tracking, healthcare monitoring, and emergency response. Security in WSNs can be categorized into two broad classes: content security, and context security. Content security relates to the protection of data traversing the sensor network such as data secrecy, integrity, and key exchange. Context security is thus concerned with protecting such contextual information associated with data collection and transmission. User query privacy, source location privacy and temporal privacy are typical contextual security issues [1]. Security and privacy concerns associated with the widespread adoption of RFID systems in healthcare environments have been a major deterrent for the penetration of this technology in key application areas. In the last five years, many works have worked some of these issues by proposing different schemes that facilitate a secure execution of certain healthcare functions. We provide example cases in the health care domain where such scenarios are observed and present brief security analyses of the developed protocols.

Ⅱ. Related Works

RFID is an emerging technology that is rapidly becoming the standard for hospitals to

track inventory, identify patients, and manage personnel. RFID systems are seen as valuable because of their ability to collect data in real-time. We assess the security of our scheme by following the basic goals of confidentiality, authenticity, and privacy protection. With respect to confidentiality, we are concerned with concealing the contents of the data from an attacker. This process involves encryption and possibly randomization to help prevent multiple encryptions of the same plain-text from looking similar, i.e., semantic security. Integrity is concerned with being able to detect if a message has been tampered with while authenticity translates into making sure that the message was indeed sent by its intended sender [2, 3].

The followings are summary of recent research trends [4].

Information technologies, such as RFID-based systems, are being routinely integrated into hospital infrastructure in order to increase the efficiency and effectiveness of health care delivery.

- RFID systems can be used in hospitals to locate equipment, verify the identity of patients during medical procedures, and collect data on staff workflow to find inefficiencies in current hospital operations, but little empirical evidence exists on how to implement the systems effectively.
- RFID systems do not adapt easily to hospital settings because the infrastructure of hospitals, in terms of space, equipment, personnel, and patients, is much more complicated than factory or warehouse settings.
- Most of the literature focuses on the technical efficacy of RFID systems, not the social and organizational effects of such systems.

We briefly consider a few security violations that can arise in the protocol.

- Denial of Service (DoS)/desynchronization attack: Denial of Service (DoS) attacks can arise due to several reasons including desynchronization between tag and reader and can lead to disconnect between tag and reader.
- Forward Security: Forward security is necessary to maintain the integrity of the system and is especially critical in systems where messages are exchanged over the air.
- Replay attack: Replay attack occurs when an adversary passively observes communication among entities and copies those messages for later use.
- Impersonation attack: Impersonation attack occurs when an adversary is able to completely impersonate an entity to all other entities that participate in the protocol.

III. Conclusion

Many researcher and scientist try to work to implement low cost security and privacy protocol to increase the applicability. A Lot of lightweight solutions have been proposed for RFID, but they are still expensive and vulnerable to the security and do not fully resolve the security issues.

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] Yanjiang Yang, Jianying Zhou, Robert H. Deng and Feng Bao, "Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks," Security and Communication Networks, 2011, N.4, pp.11 – 22.

[2] Alina Olteanu, Yang Xiao, Fei Hu, Bo Sun and Hongmei Deng, "A lightweight block cipher based on a multiple recursive generator for wireless sensor networks and RFID," Wireless Communications and Mobile Computing, 2011, N. 11, pp.254 – 266

[3] Cannire, C., Dunkelman, O., and Kneevi, M., Katan and Ktantan, "A family of small and efficient hardware-oriented block ciphers. In: Cryptographic Hardware and Embedded Systems," CHES 2009. Lecture Notes in Computer Science, Vol. 5747, pp. 272 – 288. Berlin: Springer, 2009.

[4] Jill A. Fisher and Torin Monahan, "Tracking the social dimensions of RFID systems in hospitals," International Journal of Medical Infiormatics, V.77, 2008, pp.176-183.

[5] Wei Zhou, Eun Jung Yoon and Selwyn Piramuthu, "Simultaneous multi-level RFID tag ownership & transfer in health care environments," Decision Support Systems N.54, 2012, pp.98 – 108