Privacy and Security Model for RFID Healthcare System in Wireless Sensor Network

김정태
목원대학교

무선센서네트워크 환경하에서 RFID 헬스 시스템을 위한 보안

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

The use of a mobile agent in hospital environment offers an opportunity to deliver better services for patients and staffs. Furthermore, medical errors will be reduced because M-health system helps to verify the medical process. Optimized security protocols and mechanisms are employed for the high performance and security. Finally, a challenge in the near future will be converge the integration of Ubiquitous Sensor Network (USN) with security protocols for applying the hospital environment. We proposed secure authentication and protocol with Mobile Agent for ubiquitous sensor network under healthcare system surroundings

Ⅰ. Introduction

As information technology is developed in recent year, many organizations such as government agencies, public institutions and corporations have used information system to improve efficiency of their work process. Recently, medical organizations all over the world have also employed or planned to use the information system based on network and database. Whereas, many hospitals have not realized with this kind of system and have adhered to working process based on offline work infrastructure. Typical paper-based systems, for example, waste resources such as man-powers and time, and many errors occure in medical records. E-health system such as EMR (Electronic Medical Record), PACS (Picture Archiving and Communication System), OCS (Order Communication System) and telemedicine provide effects like cost and time reduction, information assurance, real-time data access and customer-oriented services. In recent, the healthcare system based on information system has moved to ubiquitous healthcare system such as personal home networking healthcare in the digital consumer electronics, which system enables medical professionals to remotely make real-time monitoring, early diagnosis, and treatment for potential risky disease, and to provide the medical diagnosis and consulting results to the patient via wired/wireless communication channels[1,2,3].

II. Related Work

In the 21st century, population in the world has steadily been raised and the number of aged people also increased rapidly. Also health system is developed. Health system has been demanded to be changed to E-health system as interest in health is increased quickly. Accordingly, many developed nations such as United States and Europe make an effort and assign a lot of budget on u-health industry which is expected to get a rapid growth in the near future. U-health consists of various factors such as a medical E-commerce and remote medical service and is also introduced as national project which combine the existing health system with Information Technologies such as the Internet and mobile. This enables to provide health information, knowledge, services and products from anywhere and anytime. For this reason, many government also plans to develop the u-health system as a national project shown below.

- NSW government in Australia has announced that $100M u-health project will be launched to replace paper-based health records in 188 public hospitals.
- Smart use of data, information and communication is one of major part of a healthier future for all Australian, generated by National health and Hospital Reform Commission [4,5,6].

III. Proposed Security Mechanism

There are four different u-healthcare systems are introduced. Two of them, EMR and Schedule Manager, will be developed and implemented, and the others, RFID Technology and Remote Diagnosis, will be researched and documented.

- Electronic Medical Record (EMR) System
- Schedule Management Application
- RFID Technology
- Remote Diagnosis (U-Healthcare system)

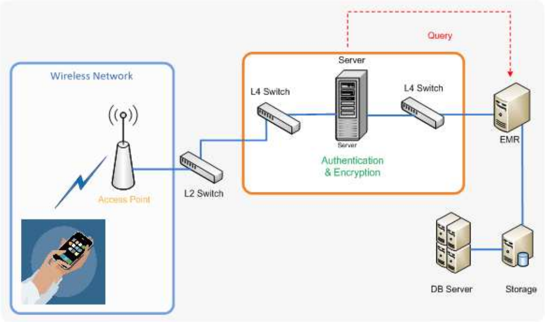

Fig 1. Virtual Hospital Network Topology

IV. Security Components

As shown in Figure 2, mainly security components are divided into two groups such as administrative and technical security. As a process of administrative security, security policy will be firstly generated to control all of security aspects. It should be in the center of security components to make a balance between various security technologies. All of security aspects can work properly together as security policy is well prepared. Security policies are usually documented and provide a high-level description of the various controls which the organization will use to protect data.

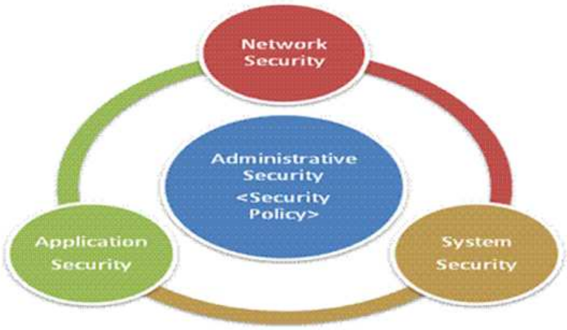

Fig 2. Virtual Hospital Network Design Draft Version

Written security policy documents are also a formal declaration of management's intent to protect data, and are required for compliance with various security regulations. It contains the statement for how an organization intends to protect information.

Elements of security policies are briefly described below and it will be extended as the work is progressed further.

- Title: Brief description of the document
- Number: Unique identifier for the policy document
- Publish Date: Date the policy has been officially approved
- Scope: Security assets that this policy applies to
- Policy Text: Written policies
- Sanctions: Information on violations of the written policy

Example of security technologies are briefly described below and it will be extended as the project is progressed further.

- DMZ (Demilitarized Zone) is prepared to control data traffic between internal and external access.
- Firewall is responsible for preventing intrusion onto the private network from outside and installed in the traditional single DMZ, this will aid the protection of the internal network.
- Access control is also implemented to classify user's authorization. VLAN will be employed to deploy the access control.
- Secure ID and tokens are also used to protect data transaction against attacks.

V. Conclusion

Medical contexts are especially interesting because of the legal constraints related to privacy preserving and security. In this paper, we have presented a design framework for implementing privacy measures in ubiquitous computing environments, and demonstrated its application to pervasive healthcare. Given the sensitivity of healthcare environments, and the associated data, addressing privacy issues will play a large part in the adoption of pervasive healthcare applications.

References

[1] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of selected areas in communications, V.24, N.2, pp.381-394, February, 2006

[2] H.Y. Chien. "SASI: A New Ultra-weight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing., vol.4, n.4, pp.337-340, Oct. 2007

[3] M. Feldhofer, etcs, "Strong authentication for RFID systems using the AES algorithm," Cryptographic hardware and embedded systems", CHES 2004, v.31, n.56, pp.357-370, 2004

[4] Azzedine Boukerche, et al, "A Secure Mobile Health System Using Trust-Based Multicast Scheme", IEEE J. On selected areas in communications, v.27, n.4, may 2009, pp.387-399.

[5] J.H.Kim and Sahama, T. "A Study on the Encryption Model for Numerical Data,", International Journal of KIMICS , vol.7, pp.31-34. 2009.

[6] Shinyoung Lim, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring", 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp.327-332, 2010.

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:2011-0026950)