
Security Issues, Challenges and Techniques for U-Healthcare System

양지수, 김한규, 김승민, 김정태
목원대학교

유비쿼터스 환경하에서의 헬스케어 시스템에서의 보안 문제, 해결책 및 기법

Ji-su Yang, Han Kyu Kim, Sung Min Kim, Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless network in open wireless network and the unique security mechanism used in each one of these networks. In the paper we analysed some elements to guarantee security and privacy preserving in distributed IT applications which provide some kind of support to complex medical domains.

I. Introduction

There is much work on how to apply information and communication technologies to healthcare services, especially with regard to wireless networks and pervasive devices combined to provide more applications in electronic medical care. Thus, wireless and mobile communications lead to the emergence of a new type of advanced service for healthcare, making mobile healthcare systems more realistic and feasible in terms of providing expert-based medical care [1]. Sensor network technology promises a vast increase in automatic position data collection capabilities through efficient deployment of tiny sensing devices. Recent advances in information technology (IT) have introduced new systems that can support healthcare delivery, patient support, and education. This in turn enables a redesign of health

care processes that are supported through the integration of electronic communication and healthcare records.

II. Related Work

Privacy preserving and data security is a complex field, which deals with many different problems and provides different solutions, as privacy and security can be threatened in many ways. Solutions usually lead to obstructions in normal use. Security and privacy issues are raised automatically when the data is created, transferred, stored and processed in information systems. Especially, data transfers for the medical and healthcare purposes should be secure, safe and reliable. Previous work on monitoring human body signals guides us the place where we should put security and privacy features. With the advance of computer and networking technology convergence

trends, pervasive computing is regarded as key technology to assist real time medical and healthcare information service with the help of deploying different kinds of sensors, communicating with wireless sensor networks, interpreting sensor data and developing large number of medical and healthcare service rule sets cooperated with medical professionals [2].

III. Security requirements

Traditional security approaches to protect information systems have focused on preventing attacks from being successful by hardening the system to be protected with various mechanisms. While security approaches may protect one layer of a networked system, they often introduce vulnerabilities to other layers. We present reusable security requirement and use them as examples of reusable security requirements that can be extracted from legislation[3].

- Identification and authentication requirements
- Authorization requirements
- Integrity requirements
- Privacy requirements
- Security Auditing Requirements
- Survivability requirements
- Non-repudiation requirements

The attacks on healthcare system are as follows.

- Denial of service attack
- Physical attack
- Tag clonig attacks
- Impersonation attack
- Replay attack
- Tag tracking

IV. Security threats in pervasive healthcare application

We survey a non-exhaustive list of privacy and security issues that concern patients and will serve as requirements/

objectives in future e-healthcare system design. We also discuss the suitable cryptographic techniques for solving these issues.

- Privacy and Access control
- Authentication and Confidentiality and integrity
- Secure data storage

V. Conclusion

In this paper, we analysed detailed discussions on the privacy and security issues in e-healthcare systems and corresponding viable solutions. A simple yet flexible and scalable framework of a scalable wireless biosensor system tuned for real-time remote monitoring as a case study of security threats assessment should be considered.

References

- [1] Azzedine Boukerche, and Yonglin Ren, "A Secure Mobile Healthcare System using Trust-Based Multicast Scheme", IEEE J. of Selected Areas in Communications, V.27., N.4, May 2009, pp.387-399.
- [2] 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
- [3] Jostein Jensen, etal, "Reusable Security Requirements for Healthcare Applications", 2009 International Conference on Availability, Reliability and Security, pp. 380-385.

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: 2012-0007896)