Security Consideration for Implementation in Ubiquitous Healthcare System

김정태
목원대학교
유비쿼터스 환경하에서의 헬스케어 구현 시의 고려 사항
Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

Healthcare applications involve complex structures of interacting processes and professionals that need to exchange information to provide the care services. In this kind of systems many different professional competencies, ethical and sensibility requirements as well as legal frameworks coexist and because of that the information managed inside the system should not be freely accessed, on the contrary. it must be subject to very complex privacy restrictions. This is particularly critical in distributed systems, where additionally, security in remote transmissions must be ensured. In this paper, we address the fundamental security issues that must be considered in design of a distributed healthcare application.

Ⅰ. Introduction

The Business, Medical and Industrial communities have praised the benefits and progress created by state-of-the-art computer technology. However, these same communities have recognized the potential threats and malicious activities in cyberspace that can eliminate the advantages and reverse the progress. For these reasons, many steps have been taken by many stakeholders using this technology to reduce the level of assumed risk and create a computer environment with a high level of confidence. Security concern has also been focused upon the private patient information sharing among interconnected hospitals. Secure access of electronic healthcare records (EHR) which may be scattered across healthcare units has been considered in [1]. Electronic or mobile healthcare networks are established by connecting general practitioners, hospitals and national/private medical centers. This approach is an attractive solution for the already overstretched and under budgeted health sector since it reduces the current paper-based work, decreases waiting time, eliminates prior appointment requirements, enhances healthcare services with efficient, faster and more reliable methods, eliminates errors that can happen in the paper records and speeds up administrative procedures. However, in traditional healthcare systems, the stored health information in a healthcare center is usually accessible only to authorized healthcare personnel of that center [2]. For every healthcare center, there are separate systems to record patients' health information, and information flow between

systems is very limited. The use of mobile healthcare devices also allows the exploration of use within the promotion of healthy lifestyles, the prevention and treatment of major diseases, all within the setting of the home environment. Implementation of mobile healthcare devices requires the support of healthcare providers at a national level to ensure that a robust infrastructure is in place, allowing full interoperability to be supported. To support this activity, it may be prudent to study the implementation of mobile solutions in a range of other sectors.

II. System Security

EHR systems have two main security concerns: transmission and access. Transmission security refers to the healthcare delivery organization's ability to ensure that transmitted data is safe from potential security threats an route, and access security refers to the healthcare delivery organization's ability to ensure that system access is granted only to appropriate individuals.
Transmission security concerns typically arise during wireless network implementation. The Wired Equivalent Privacy (WEP) protocol was designed to provide the same level of privacy as a wired network, but due to security concerns over the WEP standard, experts continue to debate whether WEP alone is sufficient for HIPAA transmission security. Consequently, the healthcare delivery organization should use a combination of WEP and other security protocols for wireless networks. Authentication and privacy protection In order to avoid such potential security breaches, the existing HealthAgents architecture should tackle some generic security requirements as outlined below[2].
- Secure encrypted message passing among HealthAgents nodes.
- Local site authentication. Appropriate policy sets application wherever resources are required across centers without requiring extra identification.
- Global resource and service policy sets at the overall Health Agents level.
- Dynamic site addition to the Health Agents network and trust relationship management, straightforward new policy sets deployment and minimum intervene to the existing infrastructure.
- Individual policy sets for access authorisation at local sites which retain their independent control over resources reside in their own site and these policies should override the global policy sets wherever a conflict occurs.
- Transparent user interaction without requiring them to be aware of the security measures, their access privileges being dynamically managed and maintained. We can consider individual requirements, looking at a known solution and examining possible inconsistencies.
- Authentication
- Confidentiality
- Data integrity
- Non-repudiation
- Interoperability
- High-Availability(HA)

III. RISK ANALYSIS

healthcare environment is proposed as a Privacy and security threats in the electronic and mobile healthcare environments is essential. We should focus on the possible threats and solutions as follows.
- User anonymity
- Message privacy
- Message cofidentiality
- User authentication and authorization
- Replay attacks

In order to circumvent security threats, three fundamental security requirements, named confidentiality, integrity and

availability, have to be ad-dressed (Samarati and Vimercati 2001, Li et al. 2004):

- Confidentiality: Confidentiality is the assurance that sensitive information is not disclosed. For example, medical image transmission cannot be accessed by unauthorized parties.
- Integrity: Integrity prevents the unauthorized modification of information. For example, received images are not modified during transmission.
- Availability: Availability refers to the notion that information and services are not available for use when needed. For example, images are from correct sources to the claimed users.

Security regulations can mainly be distinguished by requirement standards and specifications on what to do and how to do it. In the regulations, the provisions regarding administrative, physical, technical, and communicative safeguarding are described from different viewpoints to guard integrity, cofidentiality, and availability of the health data [3].

Protecting the privacy and cofidentiality of medical records and patients' data is no longer a choice, but a necessity. In other words, without an elaborative key management scheme to integrate these mechanisms such as privacy and security regulations. The serious problems of complex operation and harmful impact will occur.

IV. Privacy preserving and security in distributed platform

A global privacy preserving and security solution has to start with a definition of a set of internal privacy and security rules, security guidelines. These rules specify how the sensitive data has to be treated, where it can appear. The rules must exactly define physical places of data in each of its life cycle. Then, we should pay attention to items below[4].

- Defense in Depth
- Privacy and Security Aspects
- Identification and authentication
- User profiling
- Secure Transmission of Data
- Private Data Protection

V. Conclusion

The health sensitive information is transmitted in the network. It is vital to protect patient's privacy against malicious activities. In the paper, we survey the fundamental security issues that must be considered in design of a distributed healthcare application.

References

[1] Stasia Kahn and Vikram Sheshadri, "Medical Record Privacy and Security in a Digital Environment", pp.46-52. IT Pro March/April 2008

[2] Dickson K.W. Chiu1, etcs, "Protecting the Exchange of Medical Images in Healthcare Process Integration with Web Services " Proceedings of the 40th Hawaii International Conference on System Sciences, pp.1-10. 2007

[3] Wei-Bin Lee and Chien-Ding Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations ", IEEE Transaction on Information Technology in Biomedicine, v. 12, n. 1, pp.34-41, January 2008

[4] Lenka Lhotska, etcs, "Security recommendations for implementation in distributed healthcare systems", pp.76-83, ICCST 2008