Secure Architecture of the Mobile Healthcare Environment Using security protocols

문강남, 이정훈, 곽동엽, 토니 사하마, 김정태*
퀸즈랜드공과대학교, 목원대학교*

Secure Architecture of the Mobile Healthcare Environment using security protocols

KangNam Moon, JeongHoon Lee, DongYeup Kwock, Tony sahama, Jung-Tae Kim*
Queensland University of Technology, Mokwon University*

E-mail : moon@connect.qut.edu.au

ABSTRACT

Medical records must be well protected because they are needed to care for the health of patients. For that reason, user authentication and medical data encryption are essential for the security of both wired and wireless Healthcare Information Systems (HIS). The main focus of this paper is on the analysis of the numerous possible attacks and the countermeasures to overcome these attacks in Mobile Healthcare Environment (MHE) with an appropriate security protocols. To draw a conclusion, this will propose why a healthcare architecture should establish a multi-layered defense against the risks.

Key words
mobile healthcare, vulnerabilities, security protocols,

Ⅰ. Introduction

Since past few decades, medical organizations all over the world have employed or planned to have a Health Information System (HIS) based on a digital media, distributed storage systems and the Internet. Recently, E-mail access, high-pixel photography, bar code scanning and GPS functions can all reside within the mobile device which providing a progress to mobility of HIS. Needless to say, the use of a mobile agent device in the hospital environment offers an opportunity to deliver better services for patients and staffs. Also, healthcare experts increasingly require medical data delivered in real time to support their decision making process. Olla surveyed that “In the future Mobile Health (M-Health) applications will take advantage of technological advances such as nano-technology, device miniaturisations, device convergence, high-speed mobile networks, and advanced medical sensors.” in his article [1]. According to the U-healthcare R&D master plan of South Korea, sensor technologies play an important role in intelligent medical services using by wireless communications. For instance, sensor technologies used in acoustic instruments and ventricular-assist

devices are being developed to miniaturize and internalize body symptom instruments [2]. Recently, mobile devices like a smart phone assist the medical services with its portable, user-friendly and multi-functional features, but they cause privacy issues. To overcome these medical informatics' risks, wireless security mechanism of HIS should be designed as an indispensible component.

Ⅱ. Related Works

The success of mobile hospital network systems will eventually be determined by the secure information management. As U-health system comes closer to us, more security mechanism will be demanded. The Security Guidance report (2006) had been published by HIPAA in USA, which recommended two-factor authentications with a communications protocols [3]. The Department of Health and Human Services (HHS) in the United States has recently issued a temporary final rule regulating when and how patients must be notified if their healthcare information has been exposed in a security breach by hospitals, physician offices and other healthcare organizations. [4] With increasing concerns regarding the welfare and healthcare of the elders, efficient and secure system upgrades are regularly required. Even so, current healthcare services may have some limitation and issues which have to be resolved for the patient's safety and privacy. Lhotska indicated on his thesis (2008) that some well-known tools such as firewall, traffic analysis and honey-pots can be used for the protection of sensitive information from non-authorized attacks [5]. Whereas, many Australian hospitals have not realized benefits of ubiquitous healthcare system and have adhered to an office-based computing system through handwritten data. For the reason of that, this paper will discuss the successful case study of U-health system using mobile agent and suggest an enhanced security level for U-health services specifically in the aged care at home. Another one of main tasks is building a secure and efficient wireless data access architecture using optimal mechanisms and protocols as an improvement path to the U-health system.

Ⅲ. Possible vulnerability of Mobile Healthcare

With increasing number of mobile devices with 802.1x interfaces (as seen below), security of such mobile devices becomes a concern.

Table 1. Wireless Standards

	WLAN	Bluetooth	ZigBee
Standard	IEEE802.11b	IEEE802.15.1	IEEE802.15.4
Transfer Rate/Second	11-54Mbps	1-3Mbps	20-250Kbps
Range	Up to 150m	10-100m	10-75m
Device Scalability	Up to 1	Up to 7	over 65536

As a useful communications protocol, RFID tag provides secure delivery data in Wireless Local Area Network (WLAN). Recently, Bluetooth tag can be employed an identifying image and name on the mobile phone. Hence, users can find misplaced tagged items and preset specific times for the tag to go active. As a mesh networking proprietary standards, ZigBee also will provide lower cost of chips, lower power consumption of battery and higher scalability of node device over short distance in the wireless sensor network. IEEE 802.11 device transmissions are of low energy and short range, so the range of this attack is limited by the signal strength of the attacking device, which is typically low. Well shielded WLANs such as those for internal infrastructures should be relatively immune; however individual devices within range of the attacker may still be

affected. Public access points will remain particularly vulnerable [6].

According to the Apple's website, it has released an update to its iPhone operating system to protect against a vulnerability that could potentially allow criminals to hijack users' phones with malicious intent. As a good security practice, you should validate PGP keys you receive, and not trust keys that cannot be validated. [7] This Apple Product Security PGP key is also used to encrypt messages that users send to Apple via e-mail. Antivirus software also has significant flaws when used with mobile devices because it may act incorrectly on false positives. For instance, medical images like X-rays can be damaged because the virus scanner attempts to repair what it falsely identified. In mobile healthcare system, an appropriate configuration is critical for patient life and reliable treatment. In case mobile device has an error on its display, medical systems should be configured like "false open" leaving the system in working condition to provide persistent care service. Another serious attack can be developed on various types of SIM cards. In one class of attacks, known as partitioning attacks, timing and power consumption analysis could be used to recover key using as few as eight adaptively chosen plaintexts [8]. Consequently, a misplaced or lost mobile device could be cloned in a few seconds.

In addition, the interconnection of medical devices are more and more replacing stand-alone systems to improve medical process. However, mobile healthcare devices connected directly to the Internet have the greater risk. For example, internal and external forms of malicious code such as worms which can be propagated from one medical system to another.

Ⅳ. Security Protocols of Mobile Healthcare

From above discussion of mobile security drawbacks, this paper will show the following suggestions in order of importance:

1. Secure Socket Layer (SSL) acts at the socket layer which is between the application layer and transport layer. This is the relatively simple and well organised protocol, but public key operations are required.
2. IPSec resides at the network layer. Since IPSec is a component of the OS, changes to the OS are required in order to implement it. Both SSL and IPSec provide integrity of data and encryption of sessions.
3. KERBEROS is an authentication system that uses symmetric key cryptography. Whereas SSL and IPSec are designed for the Internet, Kerberos is designed for local area networks.
4. 3GPP was created by the 3rd Generation Partnership Project. It include mobility management, global roaming and utilisation of relevant Internet protocols.

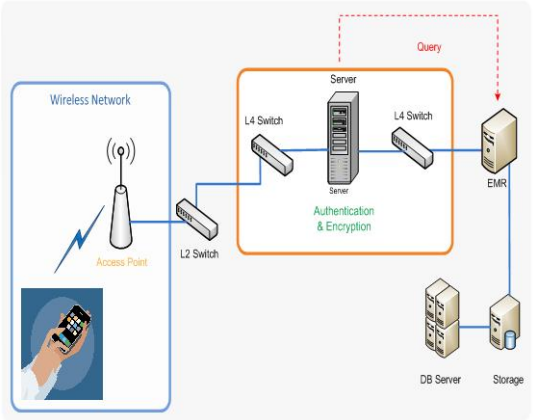

Figure 1. Diagram of Mobile Healthcare Environment

Encryption of WAP(Wireless Access Point) should be considered to prevent from revealing sensitive data. Periodic scanning of WAP is also required to discover unauthorised access. Keep these protocols in practices, selected security staff should be assigned the task of

suggestions as mentioned. These members should also maintain and verify updates on the operating systems from back-end to front-end.

Ⅴ. Conclusions and Future work

Security Awareness training is a primary defense measurement to cope with a social engineering. Good resistance education will help to prevent internal employees from being persuaded to offer critical information. Mobile healthcare systems must be also secure, effective and in compliance with government policies such as privacy regulations and system qualifications. This proposed work is a part of efforts aiming to allow all members involved to successfully consider security issues until the system under development satisfies all the security requirements. Therefore, future work includes the full integration of the suggested technique within the security oriented process. During the whole development of the mobile healthcare system, its application to more case studies in order to further assess its validity.

Acronym

HIS: Health Information System
MHE: Mobile Healthcare Environment
GPS: Global Positioning System
HIPAA: Health Insurance Portability and Accountability Act
RFID: Radio Frequency Identification
WLAN: Wireless Local Area Network
IEEE: Institute of Electrical and Electronics Engineers
PGP: Pretty Good Privacy
SIM: Subscriber Identity Module
SSL: Secure Socket Layer
IPSec: Internet Protocol Security
3GPP: Third Generation Partnership Project
WAP: Wireless Access Point

References

[1] Olla, P. (2007). Mobile health technology of the future: creation of an M-Health taxonomy based on proximity. International Journal of Healthcare Technology and Management (IJHTM)
[2] “U-healthcare R&D Master Plan Establishment” The Korea Ministry of Health and Welfare (2008)
[3] Healthcare Insurance Portability and Accountability Act (2006). Security Guidance
[4] Conn, J. (2009, AUG 20). HHS issues interim rule on patient privacy breaches. Retrieved SEP 25, 2009, from modernhealthcare.com: http://www.modernhealthcare.com/article/20090820/REG/308209956
[5] Lhotska, L., Aubrecht, P., Valls, A., and Gibert, K. (2008). Security Recommendations for Implementation in Distributed Healthcare Systems. IEEE, (pp. 76-83)
[6] AusCERT Advice (AA-2004.02) Denial of Service Vulnerability in IEEE 802.11 Wireless Devices, http://www.auscert.org.au/4091
[7] CVE-ID:2009-2204 Oct,1,2009 accessed to http://www.apple.com/support/security/pgp/
[8] J.R. Rao et al., Partitioning attacks: or how to rapidly clone some GSM cards (2002) IEEE Symposium on Security and Privacy, May 12-15, 2002