http://dx.doi.org/10.14400/JDPM.2013.11.11.747

U-Healcare 서비스를 위한 보안정책에 관한 연구

이근호
백석대학교 정보통신학부

A Study of Security Policy for U-Healthcare Service

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 IT기술과 의료정보기술을 융합한 U-Healthcare서비스의 연구가 활발히 진행되고 있다. 차세대 의료 서비스의 새로운 패러다임인 U-Healthcare 서비스는 많은 이용자에게 편의성을 보장하기 때문에 사회에서 그 중요성이 인식되고 있으며, 다양한 사업화 모델을 통한 상용화 시도가 이루어지고 있다. 다양한 U-Healthcare 서비스 시장이 안전하게 형성되기 위해서는 정부주도의 의료정보에 대한 체계화를 위한 표준과 의료법을 통한 다양한 사회 구조적 정책의 수립이 필요하다. 본 논문에서는 첫째, U-Healthcare 서비스와 정책가이드에 대한 연구를 살펴본다. 둘째, 안전한 U-Healthcare 서비스의 보안위협 요소를 분석한다. 분석된 보안 위협요소를 보안의 중요 3대 요소인 기밀성, 무결성, 가용성을 기준으로 분류하여 각 요소별 보안정책을 제안한다.

주제어 : 헬스케어, 보안, 위협요소, 보안정책, 인증

Abstract Researches on U-Healthcare service integrating medical information and IT technologies are actively conducted. U-Healthcare service is the next generation's medical paradigm that ensures conveniences to many users so that the society recognizes the importance and attempts for commercialization through various business model are performed. To form such U-Healthcare service market safely, various policies on the social structure should be established through the standard and the medical law to systemize of the medical information led by the governmen. Especially, the government's security policy to ensure the safety for the government leading visualization of U-Healthcare should be firmly established. Firstly, this paper presents U-healthcare Service and policy guideline. Secondly, it analyzes security threatening factors for the safe U-Healthcare service. By classifying the analyzed security threatening factors based on three major elements of the security, Confidentiality, Integrity and Availability of security policy for each element is proposed.

Key Words : Healthcare, Security, Threat, Policy, Authentication

1. Introduction

As IT's technological development based on the development of computer, information and communication being rapidly adapted in the medical area, various technological research are processed. One of the representative research areas would be U-healthcare service area. Various models are

Received 1 November 2013, Revised 20 November 2013
Accepted 20 November 2013
Corresponding Author: Keun-Ho Lee(Baekseok University)
Email: root1004@bu.ac.kr

ISSN: 1738-1916

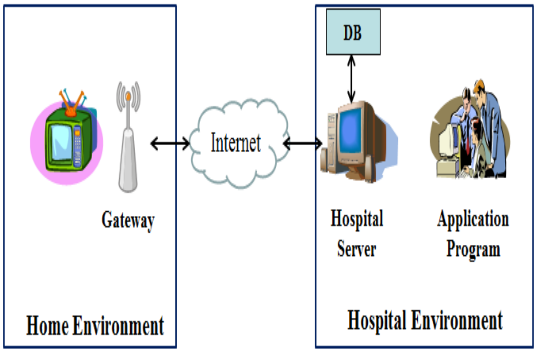
excavated on research developments and commercializations for the health care through remote diagnosis, medical information and treatment by easily using medical devices in anywhere. U-Healthcare is a new service satisfying the next generation's medical paradigm and many researches on the services are actively performed. Currently, medical services are performed in static forms with patients themselves visiting hospitals. Service in such formations has disadvantages of time waste for moving to hospitals, lack of efficient data transmission between hospitals and lack of realtime monitoring on urgent patients so than medical services in new formations are in demand [1].

U-Healthcare service is the service to break from the formation of existing medical service while improving the convenience of user and the efficient medicine. However, to achieve U-Healthcare service, various networks should be utilized so that the hacking threat are occurring. And since the human life is handled with IT technology so that the security technology stronger than any other services should be applied. The current U-Healthcare service is in the commercialization test phase and used by a small number of users are using by introducing real services. However, the international standard regarding the security of U-Healthcare is insufficient and the relevant domestic law is not legislated so that the social concerns are increasing.

In this study, U-healthcare system and the security threatening factors are reviewed and the security policy direction for solutions of the security threatening factors established based on characteristics classified with three elements of the security is, Confidentiality, Integrity and Availability is proposed.

2. U-Healthcare Service Structure and Guidelines

The remote medical service is the core of U-Healthcare service having high possibility of the most fatal outcome caused by security threats.



[Fig. 1] architecture of remote medical service

To form a remote medical service, technologies in a combination form as shown in Fig.1 is used [2]. In the process forming the process, the physical information acquired through sensors the patient has is delivered to U-Healthcare service provider connected through various wired or wireless networks. The medical doctor makes a diagnose on the patient using the information acquired after processed by U-Healthcare service provider. And the diagnoses information is delivered to the display device owned by the patient through wired and wireless network and the service is completed.

The Queensland Health Centre for Healthcare Improvement and the Patient Safety and Quality Improvement Service released the Guide to Informed Decision-making in Healthcare. The new policy and guide reflect a more contemporary, patient-centred approach than the previous 2002 policy Informed Consent for Invasive Procedures and supports the rights of patients and their substitute decision-makers to receive information about their healthcare, make informed decisions and have their decisions respected. Although a principle of the policy is to share responsibility for informed decision-making across all health practitioners, both inside and outside Queensland

Health, it is likely to impact most heavily on nurses and midwives as the largest occupational group[12]

3. U-Healthcare Security Threat

Based on CIA(Confidentiality, Integrity, Availability), the most representative standards to classify various threats on information protection, the description is made in the aspect of U-Healthcare service and check on what situation may be occurred specifically.

3.1 Confidentiality Threat

The security threat on confidentiality is the threat to open the sensitive physical information handled by U-Healthcare service to third parties through tapping attacks in send and receive sections of data. The physical information is one of the most sensitive information that may cause serious privacy invasions. Specifically, the threat may cause insurance problems and social isolations by opening the status of specific disease[3].

3.2 Integrity Threat

In U-Healthcare, the integrity threat is on the attack tempering physical information in various saving spaces and/or transmission sections. If tempering is occurred on physical information before processing, either abnormal services or diagnostic information may be delivered to users. More specifically, with a tempering attack on a user's health information, the doctor's wrong diagnosis is induced and through the wrong diagnosis, health deterioration or threat of life may occur.

3.3 Availability Threat

In U-Healthcare, the availability threat is the attack stoping devices or service servers so that the threat should be considered as the most important in any situation for being the factor directly connected to the life. Especially, in case of the heart disease patient, if the availability is fallen in an emergency situation, saving the patient life becomes impossible. If the availability of a device actually implanted in body controlling with electrical signals, the serious outcome stoping the heart may occur.

4. Security Policy Direction

The direction of market service is determined based on the government's security policy on U-Healthcare. Theretofore, the direction should be carefully considered to implement the safe society.

<Table 1> U-healthcare Service security policy

Elements	Proposal Contents
Confidentiality	Mandatory Encryption for the Data Transmission Section Mandatory Encryption for the Data Storage Area Mandatory Encryption the Standard Protocol Design
Integrity	Mandatory Authentication Application on Transmitted Data Mandatory Authentication Application on User Integrity Detection Solution Recommendation with Medical Approach
Availability	Anti-DDoS Application Recommendation Mandatory Mirror Installation on Dangerous Devices Mandatory Rapid Response to 0-day

If only the commercialization and the efficiency of the service are pursued and the service is developed without order, additional solution development costs and manpower will be required as the existing internet network and countlessly many initial victims will be produced. To avoide the occurrence of such negative result, the security policy directions on threats classified through the three elements of security as shown in Table is proposed.

4.1 Confidentiality Protection Policy

To ensure the confidentiality of U-Healthcare service, the encryption in various data transmission sections should be mandatory to lead safe market formation. Also, in the domestic market, the domestic encryption technology should be used to reinforce the competitiveness of the domestic encryption. Also, for the length of key, to prevent the minimization only for the service performance, various situations should be counted and the security should be reinforced ti the maximum by setting the adequate level with the performance. THe encryption for DB is essentially required. The physical information should be saved and managed in the DB according to the service characteristic. Since threats exist for the DB to be open to hackers via SQL injection attacks, the DB encryption solution to defend such threats should be applied. In case of using physical characteristic as the encryption key or authentication measure, special process is required. In the situation using the collected data without a special process, if the key is tapped, the hacker will have the master key for the forever use. Such situation will produce a unreversible result and no user can use the service before changing the whole method.

4.2 Integrity Protection Policy

Integrity protection policy is protected by the user authentication, the device authentication and the service providing server authentication. U-Healthcare service performed remotely transmits data through various networks so that the system may be weak against Man in the middle attack. To detect such attack, message digest should be implemented in every sections. Also, in case using Something you have element to authenticate a user, it should be used in a unconditional security not opening to any third party. Also, although a maliciously changed result due to damaged integrity appears as a normal process, the user shouldn't accept the malicious diagnosis by performing filtering in the application through a medical approach.

4.3 Availability Protection Policy

To assure the availability of U-Healthcare service, the application of security solution against various availability threatening attacks should be mandatory. In case of DoS attack, complicated problems may occur in all IT infra so that the application of Anti-DDoS using the unique pattern of each service should be recommended. Also, in the server security, as mirrors are be installed to respond to the availability destruction, the mirror installation should be mandatory in U-Healthcare for critically dangerous devices threatening the life. At last, since there are possible attacks on the availability through weak points acquired through reversing in applications connected to devices or servers so that the application of anti-reversing is required and the management should be performed legally to complement as soon as possible in case of finding a weak point.

4. Conclusion

In this study, the security threats that may occur in U-Healthcare are classified based on the three elements of security, Confidentiality, Integrity and Availability and reviewed and the policy directions for the treats are proposed. U-Healthcare service is a rapidly emerging service currently and will become a popular service that can be easily approached in daily life in soon future. Therefore, to prevent various threats on security in advance, confirmed policy managements are required. The proposed directions are desired to contribute to the establishment of safe society by being reflected in the policy for U-Healthcare market that will be vitalized in the future.

REFERENCES

[1] Dong-Gu Kim, In-Kook Song, "Necessity and

Development plan of the U-Healthcare Service ", Korean Society for Internet Information, Vol.10, No.3, pp.9-17, 2009.

[2] ChungGeon Song, Keun-Ho Lee, "Threat to Security of Remote-Controlling Medical Care Service and Countermeasure Under U-Healthcare Environment", 2nd ICCT, pp.319-321, 2013.

[3] DongHoo Shin, Byoung-Jin Han, HwanJin Lee, Hyun-Chul Jung, "Analysis of Security Threat in u-Healthcare Service", Korea Computer Congress 2010, Vol.37, No.1, pp.52-55, 2010.

[4] R. Mark, M. Mateo, M. Angelo, G. Salvo and J. Lee, "Balanced clustering using mobile agents for the ubiquitous healthcare systems", Convergence and Hybrid Information Technology, ICCIT'08, Vol.2 , pp.686-691, 2008.

[5] Cho, D.W., Kim, B. H., "The Implementation of u-Health Home Services Environment", Korea Information Processing Society, Korea Information Processing Society Review, Vol.15, pp.62-70, 2008.

[6] Seong-Hoon Lee, Dong-Woo Lee, "A Study on Review and Consideration of Medical Industry Convergence Based on U-healthcare", The Journal of Digital Policy & Management, Vol.11, No.6, pp.193-197, 2013.

[7] Jeong Yoon-Su, Lee Sang-Ho, "u-Healthcare Service Authentication Protocol based on RFID Technology, The Journal of Digital Policy & Management, Vol.10, No.2, pp.153-159, 2012.

[8] Jeong Yoon-Su, "Design of Patient Authentication Model in u-healthcare Environment using Coalition ID", The Journal of Digital Policy & Management, Vol.11, No.3, pp.305-310, 2013.

[9] Jaebum Son, Soonseok Kim, Gilhong Park, Jihun Cha, Kijung Park, "Security Requirements for the Medical Information Used by U-Healthcare Medical Equipment", International Journal of Security& Its Applications; Vol. 7 Issue 1, pp.169-180, 2013.

[10] Jung, Eun-Young, Kim, Jong-Hun, Chung, Kyung-Yong, Park, Dong, "Home Health Gateway Based Healthcare Services Through U-Health Platform", Wireless Personal Communications, Vol. 73, Issue 2, pp.207-218, 2013.

[11] Yong Sik, Jung, "Implementation Plan of Integrated Medical Information System for Ubiquitous Healthcare Service", Journal of the KOrea Society Industrial Information Systems, Vol. 15, No.2, pp.115-126, 2010.

[12] Queensland Nurse, "Informed decision-making in healthcare -NEW POLICY AND GUIDELINES", 2012.

이 근 호 (Lee, Keun Ho)

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
- 관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
- E-Mail : root1004@bu.ac.kr