ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(25), DOI: 10.17485/ijst/2015/v8i25/85945, October 2015 ISSN (Online) : 0974-5645

Development of the Security Evaluation Methodology and Criteria for a Ubiquitous Healthcare System

Junghan Lee[1], Joon Tae Ahn[1], Myung Gon Kim[1], Su Jin Park[1], Gil Hong Park[1], Dong Min Kim[2]*

[1]Department of Biochemistry and Molecular Biology, College of Medicine, Korea University, Korea
[2]Department of Creative Arts Therapy, College of Medical Science, Jeonju University, Korea

Abstract

The present study aimed to develop a security evaluation methodology and criteria for a ubiquitous healthcare (u health) system. For this purpose, first, we classified the components of a u-health system. Second, security core technologies were selected that could be applied to a u-health system in three aspects, such as administrative safeguards dealing with the operator, policies, documents, systems, and user education, physical safeguards, dealing with control of entrance and exit, and screens or shared instruments, and technical safeguards, dealing with computer system-related technological elements. Then, each security core technology was assigned to each component of a u-health system, and the relative significance of each was determined. Finally, a methodology and criteria for the evaluation of security and privacy were developed. In conclusion, the outcome can be used for enhancing the security level in the design of a u-health system and setting authentication standards for authorization processes for security.

Keywords: Authentication Criteria, Personal Medical Information, Privacy, Security, Test Methodology, U-Health System

1. Introduction

The current reality in which the number of patients with chronic diseases, such as diabetes and hypertension, accounts for 20% of the entire domestic population, with resulting healthcare costs exceeding 7% of GDP, is expected to worsen with the advent of an ageing society[1,2,8-9]. Of the solutions to cope with this, u-health, an ICT-based healthcare service, may be regarded as the most promising alternative. In particular, u-health has rapidly secured its position, along with the prospect that cost saving is possible without impairing the quality of services related to patients with chronic diseases[3]. Additionally, u-health has come into the spotlight as a fresh opportunity to create a new convergence market by means of providing network-based medical and healthcare services.

However, u-health is raising growing concerns about privacy and security: personal medical information must be managed securely according to the three information security principles, confidentiality, integrity, and availability[4]. Otherwise, breaches of personal medical information are to be expected, which will compromise the prospects of the u-health industry, accompanied by even the possibility of health risks.

In this context, this study focused on devising an evaluation methodology and criteria for the security of personal medical information by virtue of deriving security requirements for each component of a u-health system, including hardware and software. The product is expected to be used for the enhancement of security levels in the design of u-health systems and setting authentication standards for authorization processes for security, contributing to the advancement of the u-health industry.

* Author for correspondence

2. Materials and Methods

2.1 Deriving Security Items for a U-Health System

The security elements, including administrative, physical, and technical safeguards proposed by existing international and domestic personal information security standards and guidelines[5-7], were arranged and reinterpreted in terms of privacy protection technology, health information security technology, and medical equipment safety assurance technology for u-health systems (Table 1), then selected according to the u-health system components (Table 2). In parallel, the security elements that need to be taken into account for u-health system were newly derived in consultation with security and u-health operation experts. Additionally, items required for the security evaluation of u-health systems were determined (Table 3).

Collecting and analyzing the information, we assigned security elements to each component of u-health

Table 1. Security elements proposed by existing international and domestic personal information security standards and guidelines

Classification	Elements	Definition
Privacy protection technology	User authentication technology	User authentication technology
	ID security technology	Pseudonymisation and anonymisation technology
	User identification technology	Code-based user identification technology
		RFID/IC card-based user identification technology
		PIN-based user identification technology
Health information security technology	Data security technology	Confidentiality assurance technology
		Integrity assurance technology
		Availability assurance technology
	Security infrastructure	PKI technology
		Directory service technology
	Accountability technology	Audit trail technology
		Log management technology
	Communication (messaging) security technology	VPN technology
		Intrusion detection and prevention technology
	ID management/access control technology	Privilege management technology
		ID/UHID management technology
		User authorization technology
		Access control technology
	Non-repudiation technology	Non-repudiation technology
	Security Management technology	Information security management system technology
		Technology for reserving/ registering/ hospitalization/discharge from hospital/transfer/amendments
	Security policy	Security policy
		Health management authentication
		Security training
	Safe backup/ storage/ archiving/ disposal technology	Safe backup/storage/archiving/disposal technology
Medical equipment safety assurance technology	Risk management technology	Risk management technology
	Emergency access technology	Emergency access technology
	Disassemble prevention technology	Disassemble prevention technology
	How to fix	Fixing method
	Equipment error check technology	Equipment abnormality check technology

systems and the operation of the system that is needed to secure the security level of each, and then developed the methodology and criteria to assess the adequacy of each security element. Finally, an overall evaluation procedure for the security level of u-health systems was devised.

Table 2. Components of a u-health system

Field	Category	Group
Component (C)	Medical Device	U-health medical device
	Server Hardware	Safeguard of U-health server hardware
	Server Software	No support function of web-based service
		Support function of web-based service
	Client Software	No support function of web-based service
		Support function of web-based service
	Document	Documents for basic guideline such as compatibility and security maintenance
Operation (O)	Operation of administrative and physical safeguard in ISMS(Information Security Management System)	

3. Results

3.1 Medical Device

- Only u-health medical devices that passed the security evaluation by an authoritative agency should be used in the u-health system.

3.2 U-Health Server Hardware

- The reliability of the server hardware (Technical safeguard)

Evaluation method: Verifying that the server hardware is specifically developed for the server. [Proof document]

3.3 U-Health Server Software

- Duplication of the user ID (Technical safeguard).

Evaluation method: Make sure that the user ID can be specified without duplication [Technical document].

- Password creation rules (Technical safeguard)

Evaluation method: Checking the password creation rules comply with the Korea Communications Commission Notice No.2009-21. [Technical document] [Test]

- Encrypted password (Technical safeguard)

Evaluation method: Checking whether the password is kept in a hash value. [Technical document]

- Exposure of the password (Technical safeguard)

Evaluation method: Password should be displayed in *** form on the screen. [Test]

- Duplicated login prohibition (Technical safeguard).

Evaluation method: Verify whether the login is duplicated when connecting with same ID from two different clients. [Test]

- Access allowed only to authorized clients (Technical safeguard)

Evaluation method: Checking that only authorized client access to the server. [Technical document]

- Encrypted transmission (Technical safeguard)

Evaluation method: Ensure that the data transmission to the u-health server goes through an encryption process. [Technical document]

Web-Enabled Server Software

- Web log-on SSL support (Technical safeguard)

Evaluation method: Make sure that https is created in the address bar when you login. [Test]

3.4 U-Health Client Software

- Session time-out (Technical safeguard)

Table 3. Items required for the security evaluation of a u-health system

U-health system	Evaluation list		Evaluation method
	1	Design document	To check the applicability of the technology required.
	2	Evidential document	Example) To submit the software "license" such as anti-malware and intrusion detection software
	3	User manual	Checking that the encryption, security requirements are adequately described.
	4	Evaluation	Exterior security evaluation: It is tested the security of medical devices by appearance form and simple tools and does not require expertise in security related technique.
			Security performance evaluation: It is an item evaluated with driving the medical devices and required expertise in security related technique.
	5	Actual inspection	Remote inspection: It is performed a security evaluation with connection from the client to the server remotely.
			Site inspection: It is evaluated the security items to be provided by server on-site

Evaluation method: Verify the session time-out within 5 min after login. [Test]

- Encrypted data (Technical safeguard).

Evaluation method: Make sure that the contents cannot be read by a text or binary editor through checking the data file. [Technical document] [Test]

- Self-integrity check function (Technical safeguard)

Evaluation method: A function to verify the integrity of files and data should be provided. [Technical document]

- Keyboard capture prevention technology (Technical safeguard)

Evaluation method: Verify that the keyboard capture prevention technology is applied. [Technical document] [Test]

- Recommendation to prohibit the storage of personal health information into a client (Technical safeguard).

Evaluation method: Make sure that it includes a function for the recommendation to prohibit the storage of personal health information into the client hardware. [Test]

- Web-enabled client software

- Web log-on SSL application (Technical safeguard)

Evaluation method: Make sure that https is created in the address bar when you login. [Test]

- Avoid using ActiveX (Technical safeguard)

Evaluation method: Verify that it is driven by ActiveX after client installation. [Technical document] [Test]

3.5 U-Health System Document

- System building manual (Administrative safeguard)

Evaluation method: A configuration and elements should be described in the user manual, and (1) hardware requirements, (2) software requirement, and (3) a security notice building of each element should be described. [User manual]

- System operation manual (Administrative safeguard).

Evaluation method: A configuration and elements should be described in the user manual, and operational security notice of each element also should be described. [User manual]

3.6 U-Health System Operation

3.6.1 Administrative Security Elements

- Securing a security officer and appointment

Evaluation method: Security officer should be appointed and his/her responsibilities/authorization are also defined. This appointment should be approved by the chief executive officer. [Policy document]

- Security training for system operations personnel and pledge

Evaluation method: For handling of personal health information by u-health system operating staff, a security training plan and pledge form should exist. [Policy document]

- Establishment and documentation of information access policy

Evaluation method: Make sure that the policy document exists for the rights and responsibilities of personal health information handling staff. [Policy document]

- Security incident response system

Evaluation method: Make sure that systemic organization for security accident reporting and a response system are built. [Policy document]

- Backup and recovery policy

Evaluation method: Checking that the system server program, data backup, recovery method, period, staff are defined. [Policy document]

3.6.2 Physical Security Elements

- Physical protection zone settings of the server operating space

Evaluation method: Server system should be installed in the access controlled position, (1) IDC or (2) independent area with locks. [Document][Actual inspection]

- Interior equipment of the server operating space

Evaluation method: Verify that the equipment is located in a spaces prepared for a disaster, such as fire and power outage. [Document][Actual inspection]

3.6.3 Technical Security Elements

- Firewall installation

Evaluation method: Make sure to submit the license for installed firewall to block the intrusion of the outside and confirm through inspection. [Attached document] [Actual inspection]

- Anti-malware

Evaluation method: Make sure to submit the license for installation of malware response software and confirm through inspection. [Attached document][Actual inspection]

- Separation of DB server

Evaluation method: Ensure to be disconnected

between DB server and application program such as web service by disconnection of external interface between server and DB server. [Technical document][Actual inspection]

3.7 Overall Evaluation Procedure for the Security Level of U-Health System (Figure 1)

- Determination of pass or fail in the security evaluation of the u-health system is conducted as illustrated in the flowchart (Figure 1).

4. Discussion

This study extracted security requirements applicable to real-world situations in u-health environments. In addition, the factors that might be the sine qua non of more rigorous personal medical information protection schemes in the future are also included.

A variety of information security standards, guidelines, related statutes, certification programs, and the like have been analyzed in this study, at the same time suggesting new assessment criteria and methods that had been collected and developed after extracting security requirements. The individual assessment items for each component of a u-health system including hardware, software, and operational aspects, which has been prepared over the course of such research processes, may help increase security levels in terms of the design of u-health medical equipment.

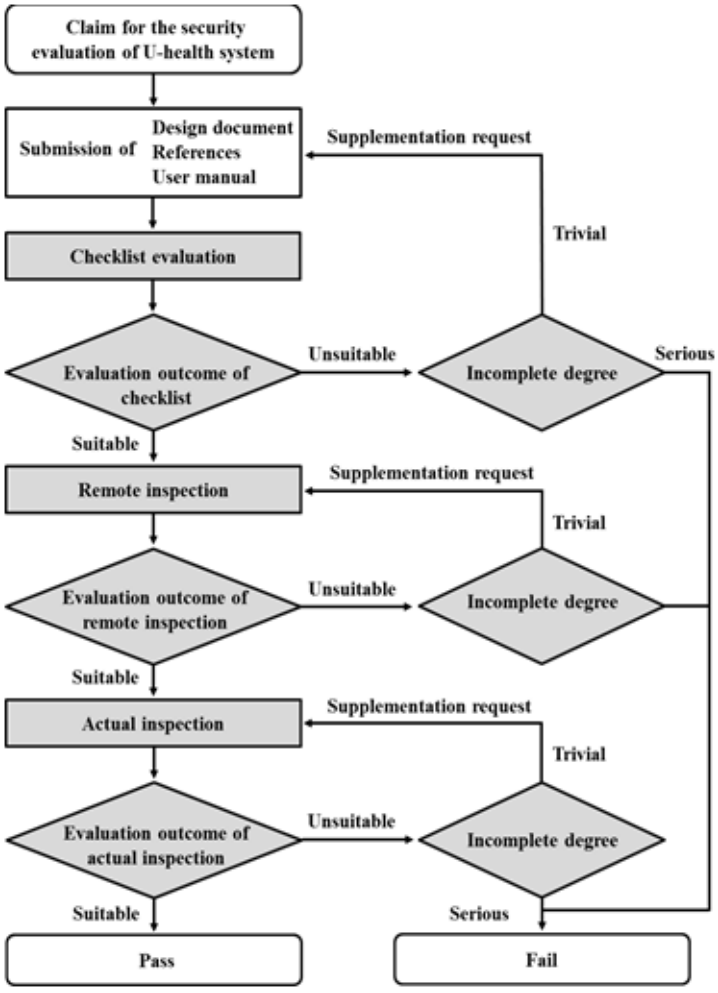

Figure 1. Flow chart of evaluation procedure for u-health security system.

Ultimately, it is believed that more sustainable studies should be carried out in line with the ontogeny of the u-health market.

5. Conclusions

The individual elements to be assessed for the security levels of each component of u-health system including hardware, software and operational aspects may help increase the security levels in terms of the design of u-health medical equipment and contribute to the authentication process by authorization authorities.

6. Acknowledgment

This study is the result of a u-health project (10172 u-health 461) supported by the Korean Food and Drug Administration (KFDA).

7. References

1. Ministry of Health and Welfare. 2009 National Health Statistics. Administrative publication no. 11-1351159-000027-10. Korea. 2010.
2. Ministry of Health and Welfare. 2010-2020 Long term estimation for national health expenditure. Korea. 2011.
3. Samsung Economic Research Institute. A new era of u-Health. Korea. 2007.
4. Korea Food and Drug Administration. u-Healthcare item-wise medical device permission and evaluation guideline. Korea. 2010.
5. Coera E. Guide to Health Informatics. 2nd ed. A Hodder Arnold Publication; 2003.
6. ISO/IEC 27000. Information technology - Security techniques. Information security management systems - Overview and vocabulary. 2009.
7. IEC 60601-1-4 Consol. Ed. 1.1 (incl. am1) Bilingual. Medical electrical equipment - Part 1-4: General requirements for safety - Collateral Standard: Programmable electrical medical systems. 2000.
8. Soo JH. Tracking analysis of user privacy damage using smartphone. Journal of Convergence Society for SMB. 2014; 4(1):13 –8.
9. Lim J-S. Design of fusion multilabeling system controlled by Wi-Fi signals. Journal of the Korea Convergence Society. 2015; 6(1):1 –5. 1. Introduction