Architecture for Monitoring Security State of ISO/IEEE 11073 Healthcare User Domain

Gaeil An, Doyoung Chung, and Byungho Chung
Information Security Research Division
Electronics and Telecommunications Research Institute (ETRI)
Dajeon, Korea
e-mail: {fogone, thisisdoyoung, cbh}@etri.re.kr

***Abstract*— With an increase in concern about one's health, Ubiquitous healthcare (U-health) service industries are getting more and more developed. Because the health data is very important one, security should be essentially applied to healthcare area. This paper proposes a healthcare security architecture, which can monitor the security state of a healthcare user domain and evaluate its security level. Through the proposed architecture, healthcare providers can determine trust or distrust of health data received from healthcare user domain by checking its security level.**

Keywords-Heahthcare; security state; monitoring; trust;

I. INTRODUCTION

With an increase in concern about one's health, U-health service industries are getting more and more developed. Through U-health service, users can conveniently measure their own health status at home or fitness center without need to go to the hospitals and receive medical services in remote diagnostics.

Continua Health Alliance (CHA), an international healthcare organization, has proposed an end-to-end healthcare architecture for enabling end-to-end connectivity of devices and services for personal health management and healthcare delivery and for providing interoperability among various kinds of healthcare devices [1]. The Continua healthcare architecture consists of a healthcare user domain where the health data (i.e., bio-data) of users is measured through personal healthcare devices and a healthcare provider domain where the health status of users is diagnosed by analyzing the health data.

Because health data is very important and sensitive one, security should be essentially applied to healthcare area. Accordingly, the CHA uses security standards such as TLS to protect health data in the healthcare provider domain. To protect health data in the healthcare user domain, the CHA employs link layer security standards. Because the link layer security standards do not sufficiently support security requirements of healthcare service, there has been research for applying security function to the ISO/IEEE 11073 protocol which is a health data transport protocol [2]-[4].

Even if the healthcare architecture considers security function, there is a problem that healthcare providers cannot determine trust or distrust of the health data received from a healthcare user domain because they have no information about how the health data has been handled in the user domain.

To address the health data trustworthiness issue, this paper proposes a healthcare security architecture, which can monitor the security state of a healthcare user domain and evaluate its security level. Through the proposed architecture, healthcare providers can determine trust or distrust of health data received from a healthcare user domain by checking its security level.

II. HEALTHCARE END-TO-END ARCHITECTURE

Fig. 1 shows the healthcare end-to-end architecture which has been proposed by CHA. The architecture defines a Personal Healthcare Device (PHD), Aggregation Manager (AM), Tele-health Service Center (TSC), and Health Records Network (HRN).

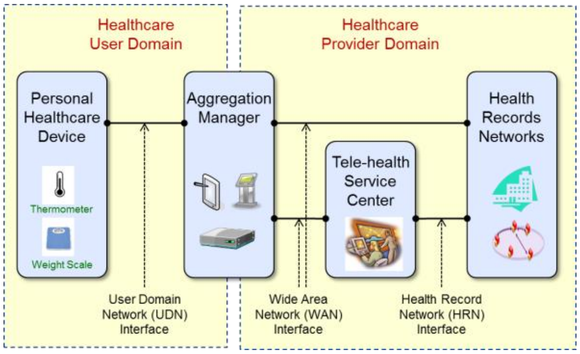

Healthcare User Domain
Healthcare Provider Domain
Personal Healthcare Device
Thermometer
Weight Scale
Aggregation Manager
Tele-health Service Center
Health Records Networks
User Domain Network (UDN) Interface
Wide Area Network (WAN) Interface
Health Record Network (HRN) Interface

Figure 1. Continua architecture: healthcare end-to-end architecture.

The PHD is a personal device which measures the health status of users. An example of PHDs includes a thermometer, a pulse oximeter, a weight scale, a glucose meter, and so on. The AM is a communication gateway which collects health data from PHDs and transmits them to a TSC or a HRN. An example of AMs includes smart-phone, PC, and so on. The TSC is a healthcare server which provides healthcare service such as a chronic disease management and an old people health care. Finally, the HRN indicates a hospital medical information system such as hospital Enterprise Health Record (HER), physician Electronic Medical Record (EMR), or Personal Health Record (PHR).

In the Continua architecture, there are three kinds of interface: User Domain Network (UDN), WAN and HRN.

The UDN interface is one between PHD and AM. It uses the ISO/IEEE 11073 protocol [5] as data transport protocol. As link layer protocol it employs Bluetooth, BLE, USB, ZigBee, and NFC. The WAN interface is one between AM and TSC or between AM and HRN. It uses the IHE HL7 protocol as data transport protocol. The HRN interface is one between the TSC and the HRN and uses the IHE HL7 protocol [6].

Because health data is very important and sensitive one, security should be essentially applied to healthcare area. Accordingly, the CHA uses security standards such as TLS and IHE (Integrating the Healthcare Enterprise) XDM (Cross-Enterprise Document Media Interchange) to protect health data in the healthcare provider domain. To protect health data in the healthcare user domain, the CHA employs link layer security standards such as Bluetooth health device profile and ZigBee healthcare application profile. The link layer security standards do not sufficiently support security requirements of healthcare service. For example, the link layer security does not support user authentication. To directly protect health data in the healthcare user domain, there has been research for providing security function to the ISO/IEEE 11073 protocol which is a health data transport protocol [2]-[4]. But currently any of those research results has not been accepted as international standard.

Even if the healthcare architecture can protect the health data from cyber-attack by using security function such as confidentiality, integrity, and availability, there is still a health data trustworthiness issue. Namely there is a problem that the healthcare providers cannot determine trust or distrust of the health data received from a healthcare user domain because they have no information about how the health data has been handled in the user domain.

III. SECURITY STATE MONITORING ABOUT HEALTHCARE USER DOMAIN

This section proposes the architecture for security state monitoring and explains in detail about security state data collection and security level evaluation.

A. *Architecture for security state monitoring*

In this paper, we propose five steps in order to determine trust or distrust of the health data received from a healthcare user domain as shown in Fig. 2. The five steps are as follows:

① Raw security state information collection step: collect raw security state information by monitoring PHD and AM, such as communication security state, healthcare protocol state, healthcare environment, and AM security state.

② Abnormal behavior detection step: detect abnormal behavior by analyzing the raw security state information which was collected in the previous step and by using security software installed in the AM.

③ Security state information normalization step: normalize the collected security state information by removing duplicated or useless data. As a result, it is generated security state information about communication security, cyber-attack detection, healthcare environment, and AM security.

④ Security level evaluation step: evaluate the security level of a healthcare user domain by using the security state information acquired through the previous steps.

⑤ Security response step: determine trust or distrust of the health data received from the healthcare user domain. If it is regarded as unreliable data, it is ignored and the communication from its sender is refused.

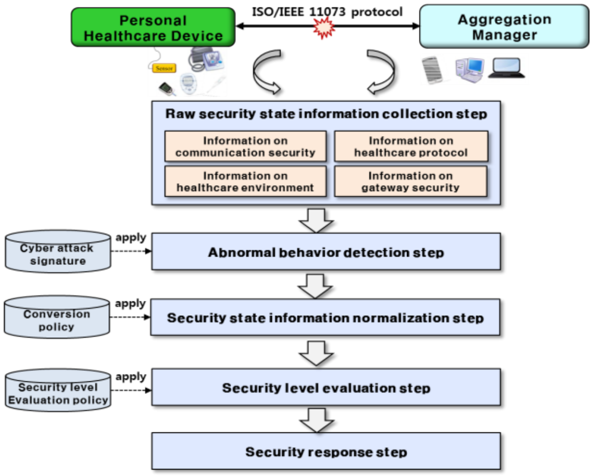

Personal Healthcare Device
ISO/IEEE 11073 protocol
Aggregation Manager
Sensor
Raw security state information collection step
Information on communication security
Information on healthcare protocol
Information on healthcare environment
Information on gateway security
Cyber attack signature
apply
Abnormal behavior detection step
Conversion policy
apply
Security state information normalization step
Security level Evaluation policy
apply
Security level evaluation step
Security response step

Figure 2. Five steps for determining trust or distrust of health data received from healthcare user domain

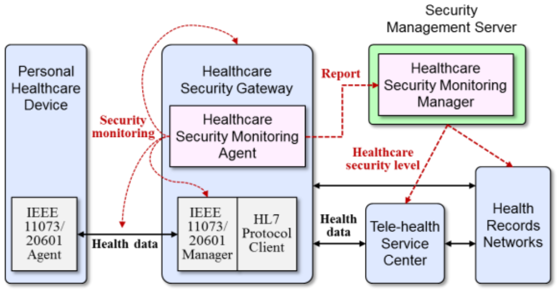

Security Management Server
Personal Healthcare Device
Healthcare Security Gateway
Report
Healthcare Security Monitoring Manager
Security monitoring
Healthcare Security Monitoring Agent
Healthcare security level
Health Records Networks
IEEE 11073/ 20601 Agent
Health data
IEEE 11073/ 20601 Manager
HL7 Protocol Client
Health data
Tele-health Service Center

Figure 3. Architecture for security state monitoring about healthcare user domain

Fig. 3 shows architecture for security state monitoring about the healthcare user domain. In the architecture, we propose two core components for security state monitoring: a healthcare security monitoring (HSM) agent and a HSM manager. The HSM agent operates as a component of the AM and the HSM manager resides at a separated system such as security management server.

The HSM agent operates as follows. Firstly, it collects security state information. And then it detects cyber-attacks (e.g., Denial service of attack) by analyzing the collected security state information or by using security software installed in the AM. Finally, it summarizes the collected or analyzed security state information (i.e., communication security state, cyber-attack state, health data collection environment, and AM security state) and reports them to the HSM manager.

The HSM manager operates as follows. First of all, it determines the security level of the healthcare user domain by analyzing the security state information received form the

HSM agent. Lastly, it provides the security level of the healthcare user domain to TRC or HRN so as to help them determine trust or distrust of the health data received from a PHD.

B. *Collection of raw security state data*

The raw security state data which is collected by the HSM agent is as follow.

- Communication security state: indicates whether or not the communication security mechanisms such as authentication, confidentiality, and integrity are applied to the UDN interface (e.g., ISO/IEEE 11073 over Bluetooth)
- Healthcare protocol state: indicates information about protocol warning/error messages and protocol connection on the UDN interface
- Health data collection environment: indicates information on PHD and AM (e.g. product name and model), whether or not a PHD is shared by people, whether a PHD is installed in open or private area, and so on
- Gateway security state: indicates whether or not security software or chipsets are being performed on the AM, such as a firewall, an anti-virus, a Trust Platform Module (TPM), and so on.

A HSM agent can detect abnormal behavior by analyzing healthcare protocol state information. An example of abnormal behavior includes a denial of service attack which requests communication connections so excessively as to exhaust the computing resources of an AM.

C. *Evaluation of security level*

If a HSM manager receives security state information about a healthcare user domain, it evaluates the security level of the domain by analyzing the received information based on its own local policy. The following is a simple example of such policy-based security level evaluation algorithm.

① Extract security state attributes from the security state information which is received from the HSM agent

② Convert the value of security state attribute to numeric one. (e.g., if authentication function is supported at the UDN interface, its value is 1. Otherwise its value is 0)

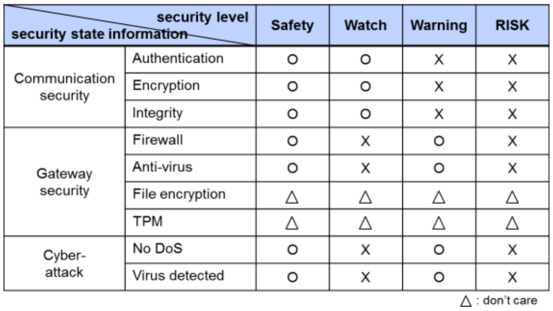
③ Normalize the value of security state attributes by applying different weight to them. The weight value by security state attribute is determined by a user-defined policy

④ Calculate a total security state score of the healthcare user domain by adding all the values of security state attributes

⑤ Finally determine the security level of the healthcare user domain by using the security state score. The relation between security state score and security level is set by a user-defined policy.

In this paper, we define four kinds of security level: Safety, Watch, Warning, and Risk. The security level is determined by a user-defined policy. An example of such policy is described in Table. 1. According to Table 1, if all the security state of a healthcare user domain is perfect, then its security level becomes 'Safety'. If the security state is good in the communication security but bad in the gateway security or the cyber-attack, then its security level becomes 'Watch'. If the security state is bad in the communication security, then its security level becomes 'Warning'. Finally if all the security state is bad, then its security level is 'Risk'.

TABLE I. AN EXAMPLE OF USER-DEFINED POLICY FOR DETERMINING SECURITY LEVEL



security level / security state information		Safety	Watch	Warning	RISK
Communication security	Authentication	○	○	X	X
	Encryption	○	○	X	X
	Integrity	○	○	X	X
Gateway security	Firewall	○	X	○	X
	Anti-virus	○	X	○	X
	File encryption	△	△	△	△
	TPM	△	△	△	△
Cyber-attack	No DoS	○	X	○	X
	Virus detected	○	X	○	X

△ : don't care

IV. CONCULSION AND FUTURE WORK

In this paper, we have proposed a healthcare security architecture which can monitor the security state of a healthcare user domain and evaluate its security level. Our architecture can help healthcare providers determine trust or distrust of health data received from the healthcare user domain by checking its security level. Our future work is to implement and verify the proposed architecture.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.B0713-15-0007, Development of International Standards Smart Medical Security Platform focused on the Field Considering Life Cycle of Medical Information)

REFERENCES

[1] ITU-T, "Interoperability design guidelines for personal health systems," ITU-T Recommendation H.810, Dec. 2013.

[2] Rubio ÓJ, Trigo JD, Alesanco Á, Serrano L, and García J, "Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility," Journal of Biomedical Informatics, pp 270-285, April 2016

[3] A. Egner, Florica moldoveanu, N. Goga, A. Moldoveanu, V. Asavei, and A. Morar, "enhanced communication protocol for iso/ieee 11073-20601," U.P.B. Sci. Bull., Series C, Vol. 75, Iss. 2, pp. 3-16, 2013

[4] A. Egner, A. Soceanu, and F. Moldoveanu, "Managing secure authentication for standard mobile medical networks," IEEE Symposium on Computers and Communications (ISCC), pp. 390-393, 2012

[5] The Institute of Electrical and Electronics Engineers, "ISO/IEEE 11073-20601 Standard for Health Informatics - Personal health device communication - Application profile-Optimized exchange protocol," ISO/IEEE 11073-20601, 2014

[6] Health Level 7 Inc., "HL7 Resource Library," 2005, http://www.hl7.org.