Security Concerns on e-Healthcare System with Countermeasures Applied

Ndibanje Bruce* ·김현호* · 박제훈** · 김창균** · 이훈재*
*동서대학교, **부설연구소
Ndibanje Bruce* · Hyun-Ho Kim* · JeaHoon Park**· ChangKyun Kim**· HoonJae Lee*
*Dongseo University, **ETRI Attached
E-mail : ndibabruce@gmail.com, jobok@dongseo.ac.kr, hjlee@dongseo.ac.kr

ABSTRACT

Data and network security for e-Healthcare Systems are a primary concern due to the easiest deployment area accessibility of the sensor devices. Furthermore, they are often interacting closely in cooperation with the physical environment and the surrounding people, where such exposure increases security vulnerabilities in cases of improperly managed security of the information sharing among different healthcare organizations. Hence, healthcare-specific security standards such as authentication, data integrity, system security and internet security are used to ensure security and privacy of patients' information. This paper discusses security threats on e-Healthcare Systems where an attacker can access both data and network using masquerade attack. Moreover, an efficient and cost effective approach for countermeasures is discussed for the delivery of secure services.

키워드

e-Healthcare, data security, network security, vulnerabilities

Ⅰ. 서 론

The recent advances in Information and Communication Technology domain have given rise to many networks and application as well. The efforts done by different researchers have produced huge and beneficial technologies, devices, and services adhering to them. Those devices are typically designed for specific tasks such as sensing, data processing and communication purposes. With this regards, security is primary concern to ensure the whole communication between the devices passing through networks systems. Following the problem statement, many novel challenges ore offered by the growth of the application's wireless healthcare offers, like, reliable data transmission, node mobility support and fast event detection, timely delivery of data, power management, node computation and middleware [1-3]. In addition though, deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very *sensitive* (*i.e.*, if a patient has some embarrassing disease), so any leakage of individual disease data could makes him/her embarrassed. In fact sometimes revealing disease information can result in a person losing his/her job, or make it impossible for him/her to obtain insurance protection. The latter trend marks an ever-growing and clamant need for protecting the confidentiality and integrity of health-care information, whilst at the same time ensuring its availability to authorised health-care providers. However, one has to acknowledge the fact that complete protection of data is, in practice, neither feasible nor possible. This paper deals with data and network attacks on healthcare system by masquerade attack and we describe a countermeasure protocol based against this attack. The remainder of this paper is organized as follows: Section 2 present related work while

Section 3 describes the attack countermeasure applied. Finally Section 4 concludes the paper.

Ⅱ. RELATED WORK

For the trustworthy of data and network security of the eHealthacare systems, a large number of protections techniques have been addressed. In the following, we provide an overview of some existing security implementations for eHealthcare systems. A solution to unsure the communication among wireless sensor network to support eHealthcare systems has been proposed in [4]. A classification level based has described where the information among the system is leveled from level 5 to level 1. Level 5 is the data which do not comprise any sensitive information and allow public access. Along with the security level increases, to access the data becomes more and more critical. For the data marked as level 1, they are extremely sensitive and only allow few people to access. Different users are assigned to a predefined level. If the users involved in the communication belong to the same level, the communication is at the same level. If the users involved in the communication do not belong to the same level, the communication will be happened at the lower value level. When the communication level is determined, different strength encryption algorithms are applied to the communication using keys from 80 bits up to 192 bit or longer. To provide security for online systems (PCASSO), a scheme based implementation of patient centered access has been proposed by Masys et al. [5]. Initially, it aims to permit patients and health care providers to access health information, even the sensitive data. Their access scheme combines role-based access control, mandatory access control and discretionary access control. The implementation is a patient-centered and centralized approach that stores all the data on a single server.

Ⅲ. Attack Description and Countermeasure

A. Masquerade Attack describtion

In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The Fig.1 shows an overview of a hospital environment within an attacker trying to access the network by masquerade attacks. In generally, the attempt may come from within the hospital, for example, from a medical staff; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the patient's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete patients 'records from the data base, make changes to network configuration and routing information. Moreover, in any eHealthcare Wireless Sensor Network, a masquerade node can apply easily denial-of-service attacks, and can disrupt the application operation. It can even defeat the purpose of wireless healthcare. Thus, masquerading nodes can be very dangerous for healthcare applications. More important, if a masquerade relay node captures the patient physiological data, later, these captured messages can pose replay threats to the real-time healthcare application. Obviously, the patient treatment depends on fresh received messages from medical sensor networks. If masquerade nodes replay the old messages again and again, this could cause of mistreatment and overtreatment (*i.e.*, medicine overdose) of the patients. Thus, masquerade and replay threats endanger real-time healthcare applications using wireless medical sensors.

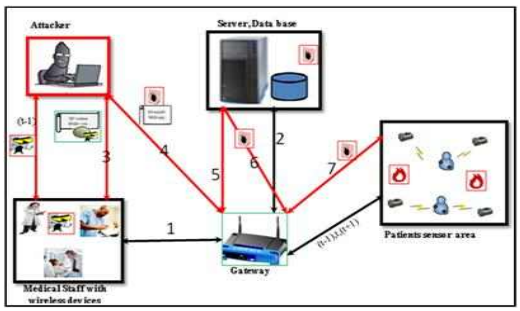

fig1.Masquerade attack on eHealthcare Sytem

(t−1) The attacker try to steal passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. Here (t−1) stands for “previousely” or “earlier” befere active attack, the attack may come from within hospital or outside.
(t−1, t, t+1) At any time (with a given frequency) the sensors devices regularly exchange message with data base where medical staff can find them
(1−2) The medical staff are using their wireless sensor for logging into the server or database through gateway.
(3) The attacker gets the victim's account ID and password for further privileges authentication
(4-5) The attacker send a login request to the netwotk using privileges of stolen ID and PW of the victim user
(6−7) While the attacker has access to server , data bse, and all network, he can now interact(pretending to be the legimate member of the network) with either staff medical or sensors'patients. Also, he can modify and delete patients ‘records from the data base, make changes to network configuration and routing information.

B. Proposed countermeasure

The proposed countermeasure is protocol based where a medical staff and all devices perform a mutual authentication process before accessing network and data. Before detailed discussion of the proposed scheme, some assumptions are made and are not supposed to be violated before mutual authentication starts.

● The medical staff with their daily wireless devices has to register to the Network Administration in order to distribute their IDs, PWs and Nonce in insecure manner

● Registration and verification phase between user and wireless devices, Server and wireless devises are supposed to be honest without compromising each other. After registration phase is done, all components can start the mutual authentication process.

The Fig.2 describes the proposed countermeasure that is based mutual authentication before entering network and enjoys data.

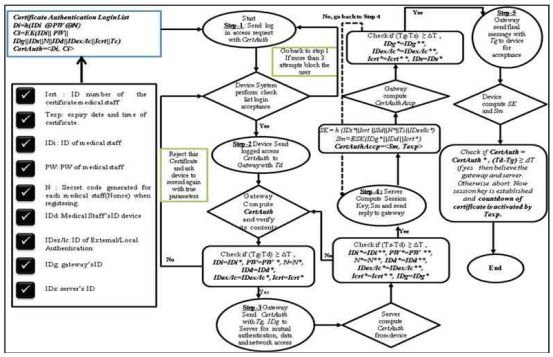

Fig. 2. Proposed countermeasure protocol based

The proposed method to counter the masquerade attack is protocol based where user, devices are mutual authentication before exchanging message. Thus, the data and network security are supported to be in security and if anyone tries to breach the network sec, this protocol will easily detect him. The following is the description of the protocol:

Step−1: The user send the certificate authentication request list to the wireless device if the required list is verified, then go to next step otherwise back to the center of the network.

Step−2: The wireless device sends now the request to the gateway for network accessibility. If the verification is true, then the gateway sends the message to the server to perform the other tasks of authentication. If not gateway returns back the message to device.

Step−3: While receiving the message from the gateway, sever performs mutual authentication by checking the content of the *CertAuth* and if everything is alright then reply positively to gateway or abort the process and send back the message to gateway as well.

Step−4: Upon receiving the reply from server, the gateway perform the mutual authentication and check if it the legitimate server, if yes the gateway send an acceptance certificate to device in order to access both data and network, if not gateway will reject the message from server and will return back to him.

Step−5: When the device gets the acceptance certificate message, it also performs the mutual authentication by checking different secrets parameters. If they match, then the session starts with session key and time of the current session. This is the end the countermeasure.

C. Security Analysis

In this section, we present the security

analysis vis-à-vis at masquerade attack and a comparison with recent secure communication scheme with our proposed protocol is done for the sufficient qualities

Masquerading user attack : The protocol is against this attack in its concept. Suppose an attacker steal the certificate, CertAuth=<Di, Ci>, he will try to login to the network but t cannot pass the stolen certificate because the device system will check and will remark an attempt to re-use the certificate, then measure can be taken (i.e. unlock the device).

Masquerading gateway attack : Suppose that the attacker bypass security device, now the gateway will see that Td , and others IDs are already used, then measure can be taken (i.e. an alert can be generated to the server, and track process can start to localize the user device.

Ⅳ. CONCLUSION

This paper discussed the security concern and countermeasure applied in healthcare applications using medical sensor networks. It has been shown that a masquerade attack can be launched to the system and patients 'data are in danger. We proposed a countermeasure against this kind of attack where a user and all devices into the healthcare network are mutual authenticated. Finally a performance analysis has been done with regard to masquerade attack and the result reveal the efficient and of the countermeasure.

참고문헌

[1] Koch, S.; Hagglund, M. Health Informatics and the Delivery of Care to Older People. Maturitas 2009, 63, 195-199.

[2] Chung, W.Y.; Yan, C.; Shin, K. A Cell Phone Based Health Monitoring System with Self Analysis Processing Using Wireless Sensor Network Technology. In Proceedings of 29th Annual International Conference on the IEEE EMBS, Lyon, France, 23-26 August 2007.

[3] Gravina, R.; Guerrieri, A.; Fortino, G.; Bellifemine, F. Giannantonio, R.; Sgroi, M. Development of Body Sensor Network Application Using SPINE. In Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC 2008), Singapore, 12-15 October 2008.

[4] R. Sulaiman, D. Sharma, Ma Wanli, and D. Tran. "A Security Architecture for e-Health Services", in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on. 2008.

[5] D. R. Masys and D. B. Baker. "Patient-Centered Access to Secure Systems Online (PCASSO): A Secure Approach to Clinical Data Access Via the World Wide Web". 1997.