Advanced Science and Technology Letters
Vol.35(Security 2013), pp.50-53
http://dx.doi.org/10.14257/astl.2013.35.12

Embedded Authorization Identification Approach for Healthcare Networks Security

Ndibanje Bruce[1], Won Tae Jang[2], Hoon Jae Lee[2]
[1]Department of Ubiquitous IT, Graduate School of Dongseo University,
Sasang-Gu, Busan 617-716, Korea
bruce.dongseo.korea@gmail.com
[2]Division of Computer and Engineering Dongseo University
Sasang-Gu, Busan 617-716, Korea
jwtway@gdsu.dongseo.ac.kr,hjlee@dongseo.ac.kr

Abstract. With the rapid increase in the amount of information flowing across intranets and the Internet, security has become an essential part of today's computing world. With the emerging growth of embedded systems ranging from low-end systems such as PDAs, networked sensors and smart cards, to high-end systems such as routers, gateways, firewalls, and web servers, data availability service is now ubiquitously practical. This promise of universal connectivity for embedded systems creates increased possibilities for malicious users to gain unauthorized access to sensitive information. This paper presents a framework for HNS in which the embedded authorization credential scheme enables negotiation between entities to specify authorization requirements that must be met before accessing the network.

Keywords: Embedded; Authorization; Identification; Network Security; Authentication.

1 Introduction

Electronic healthcare is a promising paradigm that has drawn extensive attention from both academia and industry recently. It describes the application of information and communication technologies across the whole range of function that affect the patient's Personal Health Information (PHI).

The eHealth care system shows a high potential to improve the quality of diagnosis, reduce medical costs and help address the reliable and on-demand health care challenges posed by the aging society. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient body and allow to continuous monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical activities [1].

Conventional security solutions focus on one or more of the following areas: user authentication, secure communications and data protection, achieving varying levels of success. However, even in a network with well-implemented security, client devices are often poorly protected and may still represent a weak point – particularly when remote users attempt to log on to the corporate network.

This paper proposes an embedded authorization credential access control approach which allows the entities to provide their attributes embedded into the credential function where both user and device are strongly authenticated before accessing the network services. The remainder of this paper is organized as follows: Section 2 present the literature review while Section 3 describes the proposed solution. The security analysis is presented in Section 4 before concluding in Section 5.

2 Literature Review

The growing global interconnection and interdependency of embedded networks, in connection with increased sophistication of cyber attacks over time, demonstrate the need for a better understanding of the collective and cooperative security measures needed to prevent and respond to cyber security emergencies. Embedded network does have secure vulnerabilities. Parts of the network can be compromised. Compromised parts can make successful attacks. Security should be taken into account during the design phase. Proper security solutions should be found for Message authentication, Key management, Encryption. Access to the embedded networks should be restricted to a selected set of authorized users. Security functions implemented in an embedded system must be considered in both hardware and software, at all design abstraction levels, in communications between components, and in the manufacturing phase. Embedded system security requires a methodical documented approach of identifying the threat and mapping countermeasures and then verifying their effectiveness through a recognized process. Security will mean the embedded devices' ability to contain sensitive information and to hold down its end of a secure communication. Different solution has been proposed to prove the need of privacy and authenticity in a given network [2-5].

3 Embedded Secure Protocol

The proposed embedded secure protocol is software based which can be implemented in a wireless or wired device. In this paper we consider a case where a user with his devices performs 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 user with his wireless devices has to register to the Network Administration in order to distribute the IDs, PW and Nonce in a secure 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.

Figure 1 describes the proposed embedded security protocol that is based mutual authentication before entering network and enjoying data. The following is the description of the protocol:

Step-1: The user sends an authentication login request with his IDu and PW to his device. The device system checks if the use requires the conditions pre-registered by verifying his **"*CertAuth*".** If yes the algorithm moves to the next step otherwise block the user if he attempts more than 2 times and then the user gets a message to indicated him that he is not allowed to access to device. The system recommends him to visit the Network Administrator.

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, the gateway returns back the message to device.

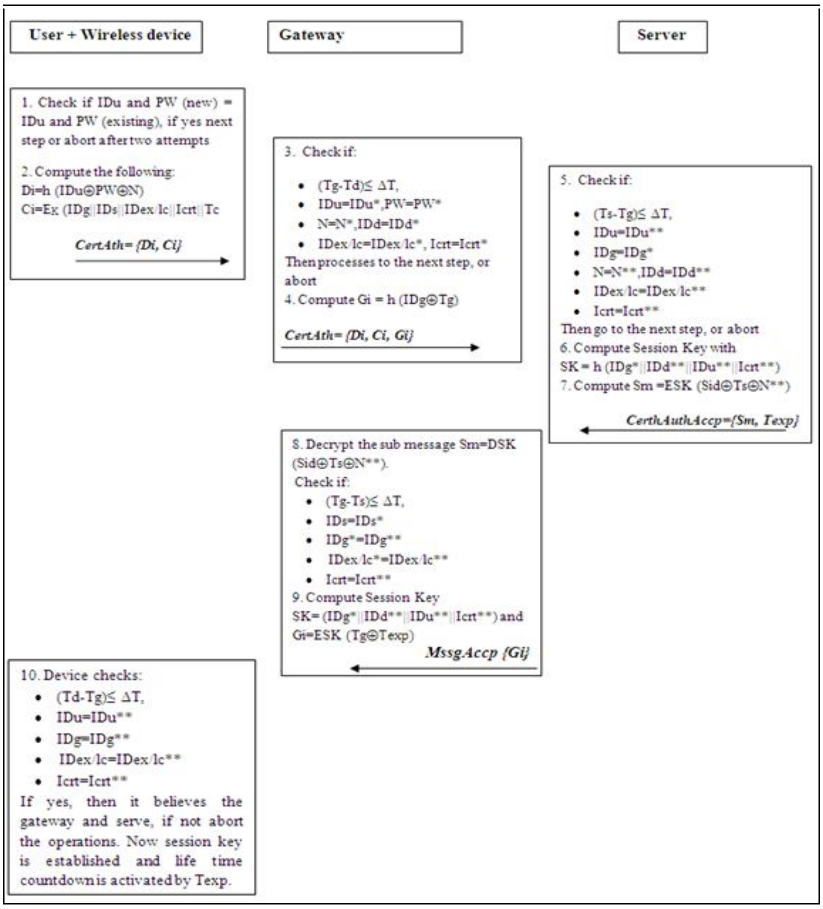
User + Wireless device
Gateway
Server
1. Check if IDu and PW (new) = IDu and PW (existing), if yes next step or abort after two attempts
2. Compute the following:
Di=h (IDu⊕PW⊕N)
Ci=Ex (IDg||IDs||IDex/lc||Icrt||Tc
CertAth= {Di, Ci}
3. Check if:
• (Tg-Td)≤ ΔT,
• IDu=IDu*,PW=PW*
• N=N*,IDd=IDd*
• IDex/lc=IDex/lc*, Icrt=Icrt*
Then processes to the next step, or abort
4. Compute Gi = h (IDg⊕Tg)
CertAth= {Di, Ci, Gi}
5. Check if:
• (Ts-Tg)≤ ΔT,
• IDu=IDu**
• IDg=IDg*
• N=N**,IDd=IDd**
• IDex/lc=IDex/lc**
• Icrt=Icrt**
Then go to the next step, or abort
6. Compute Session Key with
SK = h (IDg*||IDd**||IDu**||Icrt**)
7. Compute Sm =ESK (Sid⊕Ts⊕N**)
CerthAuthAccp={Sm, Texp}
8. Decrypt the sub message Sm=DSK (Sid⊕Ts⊕N**).
Check if:
• (Tg-Ts)≤ ΔT,
• IDs=IDs*
• IDg*=IDg**
• IDex/lc*=IDex/lc**
• Icrt=Icrt**
9. Compute Session Key
SK= (IDg*||IDd**||IDu**||Icrt**) and
Gi=ESK (Tg⊕Texp)
MssgAccp {Gi}
10. Device checks:
• (Td-Tg)≤ ΔT,
• IDu=IDu**
• IDg=IDg**
• IDex/lc=IDex/lc**
• Icrt=Icrt**
If yes, then it believes the gateway and serve, if not abort the operations. Now session key is established and life time countdown is activated by Texp.

Fig. 1. Proposed Embedded Security Protocol

Step-4: Upon receiving the reply from server, the gateway perform the mutual authentication and check if it is the legitimate server, if yes the gateway send a message of acceptance with *MssAccp* 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 message, it also performs the mutual authentication by checking different secrets parameters. If they are matching, then the session starts with session key and the countdown of the life time of the current session. This is the end the embedded authorization identification.

4 Security Analysis

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 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, N* , 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).

Mutual authentication*:* The proposed protocol provides the mutual authentication protocol for the whole communication process between all entities (*user, gateway and server).* This security feature is against known attack like compromised devices or replay and both they are sure that they are the legitimacies ones.

Session key establishment*:* A session key, *SK* is established between the communicating entities after authentication process. This key is different in each session and cannot be replayed after the session expires.

5 Conclusion

This paper discussed the embedded authorization credential in a Healthcare Network for data and network security where user and devices are mutual authenticated before accessing the network. The known attacks can be launched to the system in this regards; data and network are in danger. The performance analysis has been done with regard to those attacks and the result reveals that the protocol is efficient and resilient.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: 2013-071188). And it also supported by the BB21 project of Busan Metropolitan City.

References

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. Barua, M., Alam, M.S., Liang, X. and Shen, X. (2011) “Secure and quality of service assurance scheduling scheme for wban with application to ehealth”, *Wireless Communications and Networking Conference (WCNC), 2011 IEEE,* Cancun, Quintana-Roo, Mexico, pp.1–5.
5. G. Sylvain; P. Renaud.” SoC security: a war against sidechannels” GET /Telecom Paris, CNRS LTCI, Département de Communication et Électronique.