International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.139-144
http://dx.doi.org/10.14257/ijsia.2014.8.2.14

An Embedded Encryption Protocol for Healthcare Networks Security

Ndibanje Bruce[1], Won Tae Jang[2] and Hoon Jae Lee[2]

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

Abstract

Data availability service is now ubiquitously practical from the high-end systems such as routers, gateways, firewalls, and web servers to the low-end systems such as smart phone, tablet, etc…with the emerging growth of the embedded systems, there is parallel rapid increase in the amount of information flowing across intranets and the Internet. Hence, security has become an essential part of today's computing world. 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 an embedded encryption protocol scheme enables negotiation between entities to specify authorization requirements that must be met before accessing the network and data.

Keywords: *Healthcare; Credential, Embedded; 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.

ISSN: 1738-9976 IJSIA

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]

A solution to unsure the data protection has been proposed in [5]. In this context, Sylvain et al. proposed a embedded security based on device. The Secure SoC provides physical protection to secret keys by keeping the components like Secure ROM, which is handling the secret keys, inside the Secure SoC. During execution time, the protected secure keys from the Secure ROM has to be loaded to the RAM in clear text and during that time the bus from the Secure ROM to the RAM can be monitored to access the secret keys. This can be prevented by allocating buffers for secret keys or intermediate values of cryptographic operations involving secret keys in the Internal RAM of the Secure SoC. This prevents the protected keys being available to any bus outside the Secure SoC. The Secure Bootloader in the Secure SoC ensures that the device boots up with the genuine OS or firmware with right process privileges. The Memory Management Unit (MMU) configured by the OS permits the access to the buffers in the Internal RAM that involves secret key operations only to the secure processes with special OS privileges. In the case where the Secure ROM is limited or preprogrammed by the hardware manufacturer, the Secure ROM is limited or preprogrammed by the hardware manufacturer, the Secure ROM can be programmed with a master key. This master key can be used to encrypt and store the device secret keys in the internal ROM. In ideal case of a Secure SoC:

- The Secure ROM cannot be physically accessed to retrieve the secret keys.
- Buses inside the Secure SoC cannot be monitored to obtain protected data or keys.
- The removal or replacement of any components in the Secure SoC should be impossible or should prevent the SoC from working.

The level of physical protection varies depending on the value of the protected content. The protection can be just tamper detection of SoC to zeroing of all the stored content in the SoC when a physical access attempt is made. Tamper detection protection method does not prevent a attacker from obtaining the data from the chip but will only makes it possible to know whether the chip is tampered or not. The zeroing requires special power supply and hardware support that makes the chip costlier.

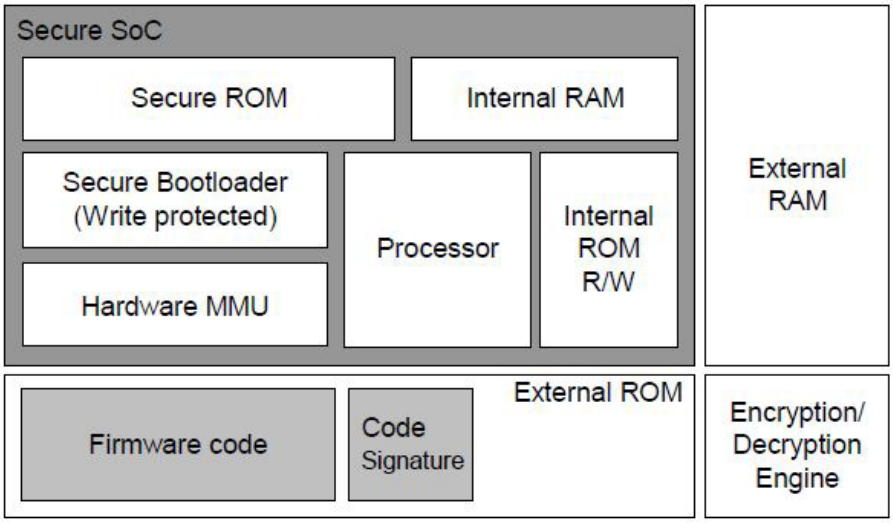

Figure 1. Secure SoC Components

3. The Proposed Embedded Encryption Protocol

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 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 Figure 2 describes the proposed embedded security protocol that is based mutual authentication before entering network and enjoys data. The proposed embedded security protocol gives a secure manner to the user and devices to process the mutual authentication before entering to the network and exchanging message. Thus, the data and network security are supported to be in security and if anyone tries to breach the network security, this protocol will easily detect him. The following is the description of the protocol:

Step-1: The user sends an authentication login request 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 3 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 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 well 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 embedded authorization credential.

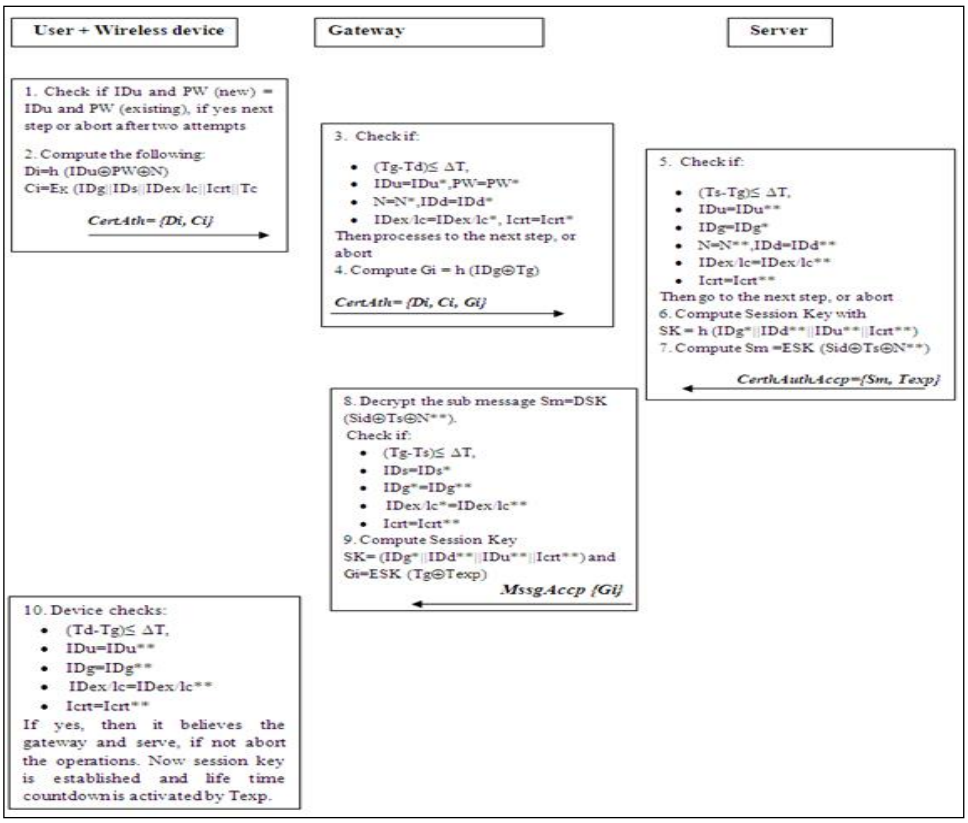

Figure 2. Steps of the Proposed Embedded Encryption Protocol

4. Security Analysis

4.1. 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).

4.2. 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).

4.3. 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.

4.4. 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.

Acknowledgements

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 was also supported by the BB21 project of Busan Metropolitan City

References

[1] S. Koch and M. Hagglund, "Health Informatics and the Delivery of Care to Older People", Maturitas, vol. 63, **(2009)**, pp. 195-199.
[2] W. Y. Chung, C. Yan and K. Shin, "A Cell Phone Based Health Monitoring System with Self Analysis Processing Using Wireless Sensor Network Technology", Proceedings of 29th Annual International Conference on the IEEE EMBS, Lyon, France, **(2007)** August 23-26.
[3] R. Gravina, A. Guerrieri, G. Fortino, F. Bellifemine, R. Giannantonio and M. Sgroi, "Development of Body Sensor Network Application Using SPINE", Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC 2008), Singapore, **(2008)** October 12-15.
[4] M. Barua, M. S. Alam, X. Liang and X. Shen, "Secure and quality of service assurance scheduling scheme for wban with application to ehealth", Wireless Communications and Networking Conference (WCNC), IEEE, Cancun, Quintana-Roo, Mexico, **(2011)**, pp. 1-5.
[5] G. Sylvain and P. Renaud, "SoC security: a war against sidechannels", GET /Telecom Paris, CNRS LTCI, Département de Communication et Électronique, Ann, Telecomm., vol. 59, no. 7-9, **(2004)**.