Advanced Science and Technology Letters
Vol.136 (ITCS 2016), pp.144-149
http://dx.doi.org/10.14257/astl.2016.136.34

The Study on Structure of IEEE 11073:20601 Agent for Protecting PHD

Doyoung Chung, Gaeil An, Sokjoon Lee, and Byungho Chung,

Electronics and Telecommunications Research Institute,
218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, KOREA
{thisisdoyoung, fogone, junny, cbh}@etri.re.kr

Abstract. In this paper, we suggest the structure of IEEE 11073:20601 agent for protecting user's healthcare information safely. Current IEEE 11073:20601 standard does not provide any method to ensure security of data exchange, and it assumes that data exchange is secured by other means. The suggested structrue of IEEE 11073:20601 agent includes mechanism for providing security of data exchange, and security of data storage. While providing those advantages, it also satisfies availability by effective encoding rules and data protecting algorithm.

Keywords: IEEE 11073:20601, PHD, Agent, PM-store

1 Introduction

Currently, the concern about health is increased, thus willingness for using healthcare device also increased. The development of ICT technology realizes wearable healthcare device, such as smart band, smart weight scale, and so on.

For interoperability between healthcare devices and healthcare services, some organizations, such as Continua, IHE, IEEE, etc., are establishing protocols, frameworks, and standards. Healthcare services usually treat sensitive information, such as biometic information, financial information, and some medical histories. Thus healthcare service requires high level of security, and it also applied to Personal Healthcare Device(PHD)s.

IEEE establishes standards for PHD, which named IEEE 11073 [1]. IEEE 11073 standards enable communication between medical devices and external computer systems. IEEE 11073 is composed of IEEE 11073:20601 and IEEE 11073:104zz. IEEE 11073:20601 align with, and draw upon, the existing clinically focuses standards to provide easy management of data from either a clinical or personal health device. And IEEE 11073:104zz standards define specific device specializations.

The system model of IEEE 11073:20601 is composed of Manager and Gateway. In this paper, we focused on the IEEE 11073:20601 agent and suggest the structure of IEEE 11073:20601 agent which protecting user's healthcare information safely.

ISSN: 2287-1233 ASTL

2 Related works

IEEE 11073:20601 standard depicts security of this standard as depends on other means, for example, a secure transport channel. Such depiction has drawbacks, for example, the medical is leaked by the vulnerability of transport layer, and inefficient power and computing resource management by seperation between (security) transport layer and IEEE 11073:20601.

To overcome those drawbacks, serveral reaserches are progressed. Egner et al. suggest mechanism [2] for mutual authentication between IEEE 11073:20601 agent and manager. However this mechanism does not provide protect mechanism for data exchange. Rubio et al. suggest mechanism [3] for mutual authentication between IEEE 11073:20601 agent and manager and protection mechanism for data exchange. Their suggestion also includes interworking with Hospital Information System(HIS), and classifies healthcare service by related components. Moreover they suggest sequrity requriements for each classification of healthcare services, and the methods for satisfy each sequrity requirement. However their suggestion assumes that Public Key Certification is available on PHD.

By the researchs [4], [5], [6] which measure power consumption and time spending on Symmetric key encryption and Assymetric key encryption algorithm on the MSP430 platform, it requires about 4.91s to using RSA-354 algorithm. Thus the assymetric key encyption algorithm which more secure than RSA-1024 is not avaiable on PHD, which usually using MSP430 platform.

On the other hand, symmetric key encryption algorithm, for example, AES-256 only consumes less than 1s for encrypt one block of plaintext. The secure hash algorithm, also consume 35ms(SHA1), and 71ms(HMAC-SHA1) [7]. Thus we suggest our mechanism based on symmetric key encryption and secure hash algorithm.

3 Secure IEEE 11073:20601 Protocol

The secure protocol which improve IEEE 11073:20601 has assumptions that the agent and manage share Pre-shared Key (PSK) in advance. It can be achieved by manufacutrers or the user of agent and manager. The secure protocol is composed of Key agreement part which based on IEEE 11073:20601 association and Data exchange protection part which based on IEEE 11073:20601 operating state.

In association stage, agent and manager generate session key based on the PSK. By modifying IEEE 11073:20601 to perform AARQ-AARE exchangement two times, 4-way handshake is performed betweeon agent and manager. By using Option-list field in AARQ, AARE in IEEE 11073:20601, we can transfer information related with key agreement 4-times. Thus it can be merged with existing key agreement mechanisms based on 4-way handshake, for example, handshake protocol in TLS [8], [9], [10]. While associating, the agent and manager perform agreement for two keys. One is session key, which for protecting data exchangement. The other is PM-store key, which for protecting data which store on PHD locally.

The PM-store key is used for encrypt medical data which located on PM-store object. Generally, the medical data which located on PM-store is stored on PHD

locally. Thus it is used for protecting medical data from data theft by local access. It is discarded from PHD, when the connection with manager is disconnected. In other words, data thief takes the PHD from original place then the PM-object key is discared. For example, the PM-store key is discared when the PHD is moved more than few tens of meter for Bluetooth connection.

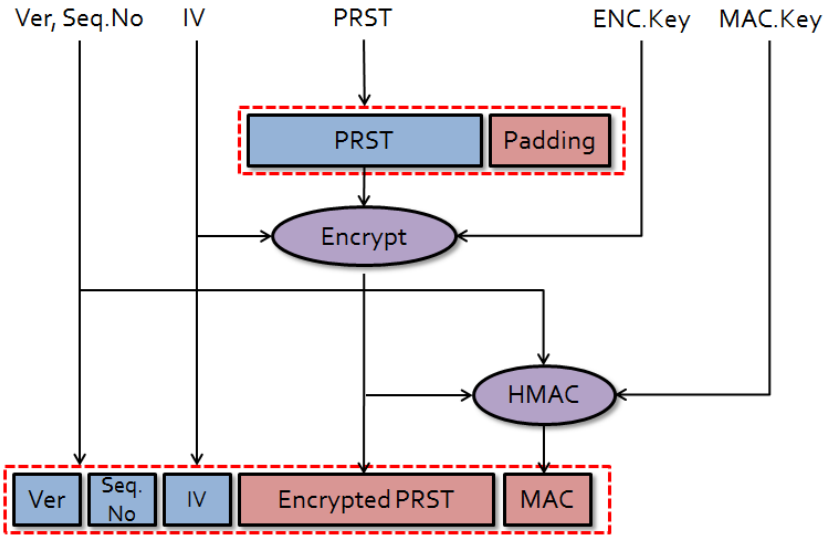

Fig. 1. The procedure of transformation PRST to Secure PRST

For exchanging data securely, the secure protocol follows Encrypt-then-MAC security mechanism [11], [12]. We use CBC-mode block cipher, such as AES-128-CBC, AES-256-CBC message encryption. This mechanism is depicted in Fig. 2. It transforms PRST message in IEEE 11073:20601 to protected form which named Secure PRST message. It is applied on operating state in IEEE 11073:20601.

3 Structure of Secure IEEE 11073:20601 Agent

The structure of Secure IEEE 11073:20601 is consist of legacy IEEE 11073:20601 agent, Secure Device Specification Block (SDSB), and Secure Message Exchange Block(SMEB).

SDSB, and SMEB hooking the message between Network Interface and Application Layer which is legacy IEEE 11073:20601 agent. This structure separates legacy IEEE 11073:20601 agent and suggested secure mechanism by layering. Thus it eases to apply secure mechanism on legacy PHDs.

Fig. 2 depicts the structure of SDSB. SDSB manages association and configuring state in Secure IEEE 11073:20601. Moreover it supports the protection mechanism which related with each device specification. For example, it supports the protection mechanism for PM-store Object. SDSB hooks the association and configuring state in

IEEE 11073:20601, and performs 4-way handshake by using modified AARQ-AARE exchangement two times.

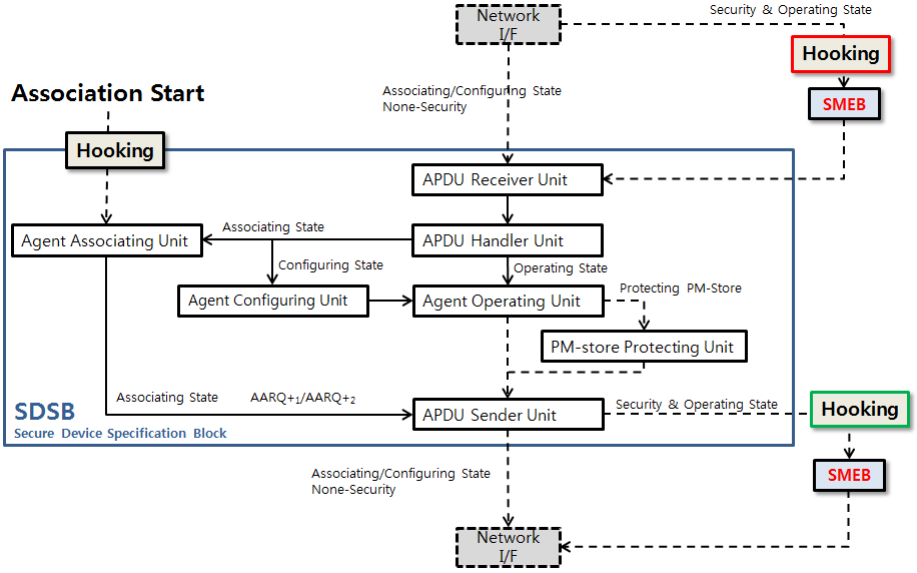

Fig. 2. The structure of Secure Device Specification on Block (SDSB)

In operating state, Secure IEEE 11073:20601 Agent provides two secure mechanisms. One is protection of PM-Store Object, and the other is protection of message exchange. The protection of PM-Store Object is achieved by encrypt medical data in PM-Store by PM-Store key, and store it on local storage. The protection of message exchange is performed by SMEB.

Fig. 3 depicts the structure of SMEB. SDSB and SMEB have to interwork, and the interworking point is depicted in Fig.2 and Fig.3. SMEB hooks PRST message generated by legacy IEEE 11073:20601 agent. Then it transforms the PRST message to Secure PRST message as depicted in Fig.1. SMEB is consists of Secure PRST unit, HMAC unit, Symmetric Encryption/Decryption Unit, and Validation Unit.

Fig. 3 depicts the structure of SMEB. SDSB and SMEB have to interwork, and the interworking point is depicted in Fig.2 and Fig.3. SMEB hooks PRST message generated by legacy IEEE 11073:20601 agent. Then it transforms the PRST message to Secure PRST message as depicted in Fig.1. SMEB is consists of Secure PRST unit, HMAC unit, Symmetric Encryption/Decryption Unit, and Validation Unit.

The role of HMAC unit and Symmetric Encryption/Decryption unit is obvious. The Secure PRST unit receives HMAC, encrypted message which generated by above units. Then it assembles Secure PRST message with protocol version, sequence number of messages, and initial vector for CBC-mode block cipher. The initial vector should be generated randomly for every message. When the Secure PRST message is received, Secure PRST unit parses it and separates each element.

The Validation unit performs comprehensive validation on each Secure PRST message. It validates each Secure PRST message with HMAC, and checks whether

decrypted message is PRST or not. Currently, the main role of Validation unit is detection of replay attack using sequence number in Secure PRST message. However we expect that the role of Validation unit is expanded in further works, and the availability of detecting attack is improved.

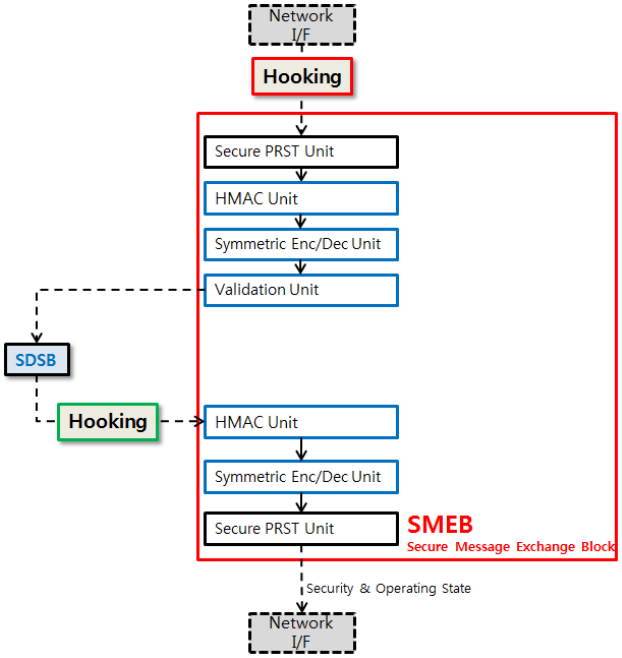

Fig. 3. The structure of Secure Message Exchange Block(SMEB)

4 Conclusion

In this paper, we present the structure of IEEE 11073:20601 agent for protecting PHD. Previous works on protecting IEEE 11073:20601 agent, manager, or connection have difficult to apply on low power, low performance devices. Unfortunately most of PHD is based on MSP430 platform, and this platform is hard to support Public Key based crypto primitives.

In our mechanism, we suggest secure mechanisms for protecting medical data which stored on PHD locally, and protecting data exchange between IEEE 11073:20601 agent and manager. Our mechanism based on Symmetric Key based crypto primitives. Thus it satisfies availability.

The advantage of this approach is to provide secure mechanisms for local stored data, while protecting data exchangement. Moreover it is reasonable to apply on actual PHD, which has low power and low performance. Currently, we are planning to improve secure mechanisms for local stored data, for example, restoring PM-store Key by resuming previous Session.

Acknowledgement. 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. IEEE Std 11073-20601™-2014, Health informatics – Personal health device communication – Part 20601: Application profile – Optimized Exchange Protocol. (2014)
2. Egner, A., Soceanu, A., Moldoveanu, F.: Managing Secure Authentication for Standard Mobile Medical Networks: Computers and Communications (ISCC), 2012 IEEE Symposium on, July 2012. (2012)
3. Rubio, O.J., Trigo, J.D., Alesanco, A., Serrano, L., Garcia, J.: Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility. In: Journal of Biomedical Informatics. vol.60, pp.270-285. (2016)
4. Buhrow, B., Riemer, P., Shea, M., Gilbert, B., Daniel, E.: Block Cipher Speed and Energy Efficiency Records on the MSP 430: System Design Trade-Offs for 16-Bit Embedded Applications: Progress in Cryptology – LATINCRYPT 2014 (2014)
5. Hyncica, O., Kucera, P., Honzik, P., Fiedler, P.: Performance Evaluation of Symmetric Cryptography in Embedded Systems: The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (2011)
6. Quirino, G.S., Moreno, E.D., Matos, L.B. C.: Performance Evaluation of Asymmetric Encryption Algorithms in embedded platforms used in WSN: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2013)
7. Lee, H.R., Choi, Y.J., Kim, H.W.: Implementation of TinyHash based on Hash Algorithm for Sensor Network. In: Proceedings of world academy of science, engineering and technology. vol. 10. (2005)
8. Dierks, T., Allen, C.: The TLS Protocol Version 1.0: IETF RFC 2246 (1999)
9. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1: IETF RFC 4346 (2006)
10. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2: IETF RFC 5246 (2008)
11. Eronen, E.P., Tschofenig, E.H.: Pre-shared Key Ciphersuites for Transport Layer Security (TLS): IETF RFC 4279 (2005)
12. Gutmann, P.: Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS): IETF RFC 7366 (2014)