EPiC Series in Health Sciences
Volume 4, 2020, Pages 65–68
CAOS 2020. The 20th Annual Meeting of the International Society for Computer Assisted Orthopaedic Surgery

Secure Knee Prosthesis – Processing of Encrypted Data and User Authentication

Anass Elmoadine[1], Maxime Pistono[1], Reda Bellafqira[1] and Gouenou Coatrieux[1]
[1] Institut Mines-Telecom Atlantique Bretagne Pays de la Loire Atlantique ; Unité INSERM 1101 LaTIM, Technopole Brest-Iroise, CS 83818, 29238 Brest, Cedex 3 France
anass.el-moadine@imt-atlantique.fr, maxime.pistono@imt-atlantique.fr, reda.bellafqira@imt-atlantique.fr, gouenou.coatrieux@imt-atlantique.fr

Abstract

Today, Implemented Medical Devices (IMDs) are key elements of the healthcare system being more and more complex with connectivity facilities. Participating to data collecting, they contribute to improve patient follow-up as well as medical practices. However, with such a connectivity security threats are significant and can be the cause of decision errors, patient privacy concerns and so on. This is why, international and national regulations make mandatory to consider security when developing new IMDs. In the context of resource constrained connected Knee Prosthesis (KP), we present: 1) a solution to securely process data emitted by KP on untrusted Human Machine Interface (HMI) and implementation times; 2) an authentication protocol for installing trust between the different entities involved in the process.

1 Introduction

In this work, we are interested in securing a connected knee prosthesis (KP) to be compliant with regulations like GDPR (Bussche, 2017) and HIPAA (Mercuri., 2004)). In our framework and as

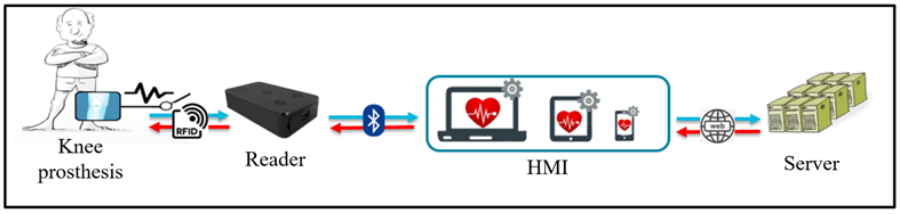

Figure 1: Project framework.

depicted in Figure 1, KP sends sensors' samples to a reader (RE) for transmission to a Human machine interface (HMI) so as to process data for patient monitoring and relay data to a server (Server) for storage purpose. Herein, HMI filters sensors' samples and raises an alarm if necessary. Based on a STRIDE security risk analysis (Carmen Camara, 2015), we identified various threats and security objectives while making the following assumptions: HMI is honest but curious - it may try to infer information about KP data but it will not tamper them; KP and RE are considered as honest proprietary devices. To ensure IMD data confidentiality, solutions like Cloaker (Tamara Denning, 2008) or IMDguard (Fengyuan Xu, 2011), use an external device to open secure channel with IMD. However, to process data, HMI has to decrypt them and if an attacker takes the control of the HMI device data privacy can be endangered. (Pistono Maxime, 2019) proposes a solution for securely processing data based on homomorphic encryption. In this work, we illustrate how it can also be used to reinforced entities authentication.

2 Solution

To secure communications against eavesdropper, KP uses a low computational complexity Combined Linear Congruential Generator (CLCG). Thanks to a cryptosystem conversion algorithm, CLCG encrypted data are turned into data homomorphically encrypted with the Damgard-Jurik (D-J) cryptosystem. By doing so, a smartphone integrated HMI can filter homomorphically encrypted data and raise an alarm without accessing to the data real values. We first come back of this process before presenting how its functionalities can be used to reinforce KP, RE and HMI authentication.

2.1 Secure processing

In our system, HMI linearly filters KP data: $A = \sum_{i=0}^{M-1} w_i d_i$, where: $\{d_i\}_{i=1..M-1}$ are the sensors' samples and $\{w_i\}_{i=1..M-1}$ the filter weights. HMI emits an alert if *A* is greater than a threshold *S*.

One can secure such operations with additive homomorphic encryption (HE) like D-J. D-J allows to compute addition over encrypted data with the guarantee that the decrypted result equals to the one carried out with unencrypted data: $E_h[m_1]E_h[m_2] = E_h[m_1+m_2]$ and $E_h[m_1]^{m_2} = E_h[m_1 m_2]$ where m_1, m_2 are two plain texts and $E_h[\cdot]$ is the DJ-encryption function. Based on these properties: $E_h[\mathrm{A}] = \prod_{i=0}^{M-1} E_h[d_i]^{w_i}$.

To summarize our solution:

1. KP CLCG encrypts d_i as follows: $d_i + Z_i$ (eq.a), where Z_i is the i^{th} CLCG output.
2. HMI DJ-encrypts $d_i + Z_i$ and gets $E_h[d_i + Z_i]$. It computes $E_h[Z_i]$ based on the DJ-encrypted version of CLCG (see (Maxime Pistono, 2019)) and denoises homomorphically encrypted data samples calculating: $E_h[d_i] = E_h[d_i + Z_i] \times E[Z_i]^{-1}$ (eq.b)
3. HMI calculates $E_h[A] = E_h[\sum_{i=0}^{M-1} w_i d_i]$, and uses the procedure in (Reda Bellafqira, 2017) to conclude if A is greater than S or not without decrypting $E_h[A]$ and $E_h[S]$.

We implemented this protocol on a microcontroller of *8 MHz*, using the Mini-GMP library. The CLCG execution time is about *920 ms* for *100* samples.

2.2 Authentication protocol based on HE

Before all entities communicate, they need to authenticate each other. If it is mandatory that KP and RE authenticate each other, there is an interest that HMI authenticates both KP and RE in order to be sure that the good KP is behind RE.

In the case of IMDs, three main strategies can be distinguished in order to verify the identity of an entity (Roudier, 2001): by means of a secret only known from this entity (secret key); by means of an electronic device owned by the entity (USB key (Tarak Nandy, 2019)); through biometric information (*e.g.* fingerprint). Solutions based on secret keys use symmetrical or asymmetrical protocols and do not require additional material. As our KP microcontroller includes the symmetrical AES cryptosystem, we opted for the AES-XCBC-MAC-96 (Herbert, 2003) for dual KP-RE authentication Figure 2.. The proposed method is secure against replay and man in the middle attacks.

In order HMI authenticates KP and RE at the same time, we propose a 4 step protocol that takes advantage of the HMI homomorphic capabilities (see section 2.1): 1) KP, RE store two secret keys while Server stores the addition of these keys; 2) KP and RE send their keys CLCG encrypted to HMI (eq.a); 3) Server sends the key sum homomorphically encrypted to HMI along with CLCG-DJ conversion parameters; 4) HMI converts the two CLCG encrypted keys from KP and RE in D-J encrypted key (eq.b), computes their homomorphic addition and comparison with the Server sum to conclude if KP and RE are the good ones.

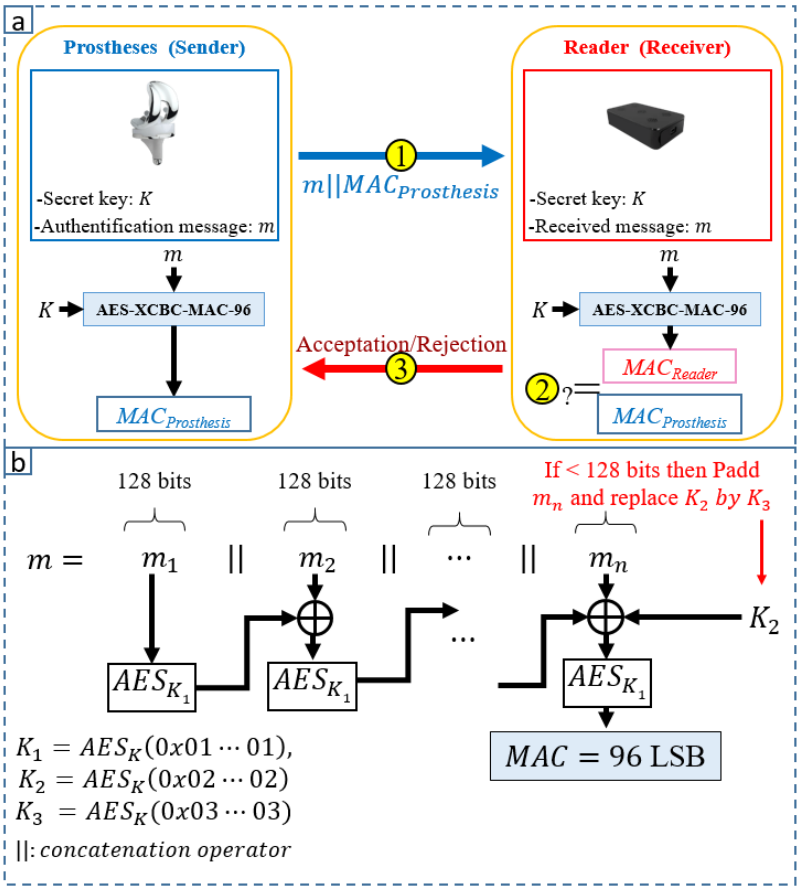

Figure 2: AES-XCBC-MAC-96: (a) authentication protocol (b) implementation with AES.

3 Conclusion

We proposed a secure protocol that allows the entities involved in an IMD communication chain to authenticate each other. Its originality stands on the reuse of the homomorphic functionalities of HMI (encryption conversion, secured filtering operations and thresholding) in order to allow HMI to authenticate both KP and RE while only talking with RE and Server. Moreover, regarding KP-RE dual authentication, we proposed the AES-XCBC-MAC-96 implementation.

4 Acknowledgment

"This work benefited from State aid managed by the National Research Agency under the future investment program bearing the reference ANR-17-RHUS-0005"

References

Bussche, P. V. (2017). *The eu general data protection regulation (gdpr).* Springer International Publishing.

Carlisle, D. (2010, April). *graphicx: Enhanced support for graphics.* Retrieved from http://www.ctan.org/tex-archive/ help/Catalogue/entries/graphicx.html

Carmen Camara, P. P.-L. (2015). Security and privacy issues in implantable medical devices: Acomprehensive survey. *Journal of biomedical informatics*, 272-289.

Fengyuan Xu, Z. Q. (2011). Imdguard: Securingimplantable medical devices with the external wearable guardian. *proceeding IEEE INFOCOM*, 1862-1870.

Herbert, S. F. (2003, Septembre). The aes-xcbc-mac-96 algorithm and its use with ipsec. *Technical report,RFC 3566*.

Maxime Pistono, R. B. (2019). ure processing of stream cipherencrypted data issued from iot: Application to a connected knee prosthesis. *41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, (pp. 6494-6497).

Mercuri., R. T. (2004). The hipaa-potamus in health care data security. *Communications of the ACM 47(7)*, (pp. 25-28).

Reda Bellafqira, G. C. (2017). Proxy re-encryption based on homomorphic encryption. *Proceedings of the 33rd Annual ComputerSecurity Applications Conference*, (pp. 154-161).

Roudier, R. M. (2001). Protocole d'athentification. *REVUE DE L ELECTRICITE ET DE L ELECTRONIQUE* , 41-44.

Tamara Denning, K. F. (2008, july 29). Absence makes the heart grow fonder: Newdirections for implantable medical device security. . *HotSec*.

Tarak Nandy, M. Y. (2019). Review on security of internet of things authentication mechanism. *IEEE Access*, 151054-151089.

Voronkov, A. (2004). *EasyChair conference system*. Retrieved from easychair.org

Voronkov, A. (2014). Keynote talk: EasyChair. In *Proceeedings of the 29th ACM/IEEE International Conference on Automated Software Engineering* (pp. 3-4). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2643085&dl=ACM&coll=DL

Voronkov, A., & Hoder, K. (n.d.). *Templates.* Retrieved from Templates for proceedings: https://easychair.org/proceedings/template.cgi?a=12732737

Wikipedia. (n.d.). *EasyChair.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/EasyChair