MOBiSEC

The 5th International Symposium on Mobile Internet Security

MobiSec 2021

October 7 – 9, 2021
Jeju Oriental Hotel,
Jeju Island, South Korea

Organized by

KIISC Research Group on 5G Security

Hosted by

Korea Institute of Information Security and Cryptology (KIISC)

Sponsored by

Huawei Korea

Electronics and Telecommunications Research Institute (ETRI)

한국정보보호학회
Korea Institute of Information Security & Cryptology

HUAWEI

ETRI

Poster: Toward Hourglass-Concepted Memory Data Leakage Protection with Capacitor-Based Timer

Ahn Sung-Kyu[1], Ji-Won Kang[2], and Ki-Woong Park[1]*
[1]SysCore Laboratory, Sejong University
yiimfn@gmail.com, jwkang@sejong.ac.kr
[2]Dept of Computer Engineering, Sejong University
woongbak@sejong.ac.kr

Abstract

Technological advances in the medical field are experiencing new leaps. In the past, medical innovations were achieved by developments in fields such as medicine, pharmacy, and biotechnology. However, recent medical innovations are expanding applications through the convergence of advanced digital technologies with medical and healthcare technologies [3]. As the medical paradigm shifts towards digital medical technologies and digital healthcare models, the core values in the medical field have changed to patient-centered medical practices rather than disease-centered practices. Hence, the digital medical device industry has accelerated the development of medical software and hardware as well as development of traditional hardware and advanced-technology-based fusion medical devices. However, rapid developments in medical software and hardware have posed digital threats to conventional medical devices[2][4]. Among these threats, the most significant are attacks on embedded medical devices incorporating Internet of Things (IoT) technology. Recently, owing to accelerated developments in IoT-based medical devices, the diversity of embedded medical devices has increased, and users can maintain their health with improves quality of life through IoT-based medical and healthcare devices [5]. However, IoT-based medical devices that are in close contact with users often store or use sensitive information, such as personal information about the users regarding their medical activity records as well as location, physical, and medical data [1][5]. In this work, we propose a solution to minimize the threat of data leakage by physically limiting the available period during which data is allocated to the memory of the embedded medical device. The structure of the proposed system is presented in Figure 1. The system memory is separated into specific areas, and each area is connected to a capacitor-based power supply. The charging management module supplies power to each capacitor. In medical practice with IoT-based medical devices, a specific portion of the operating system or the processes for operating the device are allocated to the memory. The operating system then assigns a time limit according to the importance of the data in the memory allocation process. Based on the time limits set according to priorities, the charging management module supplies current to and stores the charge in the capacitor. In the case of high-priority data, such as the user information and data concerning the medical sensor, the time limit is short, and the capacitor connected to the memory area in which the corresponding data are allocated is charged for a short period of time to ensure a small capacitance value. After the charging management module completes charging, the charge held by the capacitor is drained in accordance with leakage current characteristics. When the amount of charge held by the capacitor is reduced to below a certain capacitance value that cannot be measured, the corresponding memory power unit of the memory area is connected to the ground of the device; this causes the data allocated in that memory area to be physically volatilized. When power is cut off by grounding, the data and calculations in the medical device related to user information that are allocated in the corresponding memory are volatilized to block leakage. When such a scheme is applied to a general embedded system such as a medical device, it is expected that resource consumption can be minimized and data leakage can be prevented compared with existing solutions. As a further study, the system proposed herein will

H. Cho, J. Kim (eds.), *The 5th International Symposium on Mobile Internet Security (MobiSec'21)*, Jeju Island, Republic of Korea, October 7-9, 2021, P-Article No. 9, pp. 1-2

*Corresponding author: Dept of Computer Engineering, Sejong University be manufactured in hardware form, and the actual data leakage prevention effects of the embedded medical device will be evaluated experimentally.

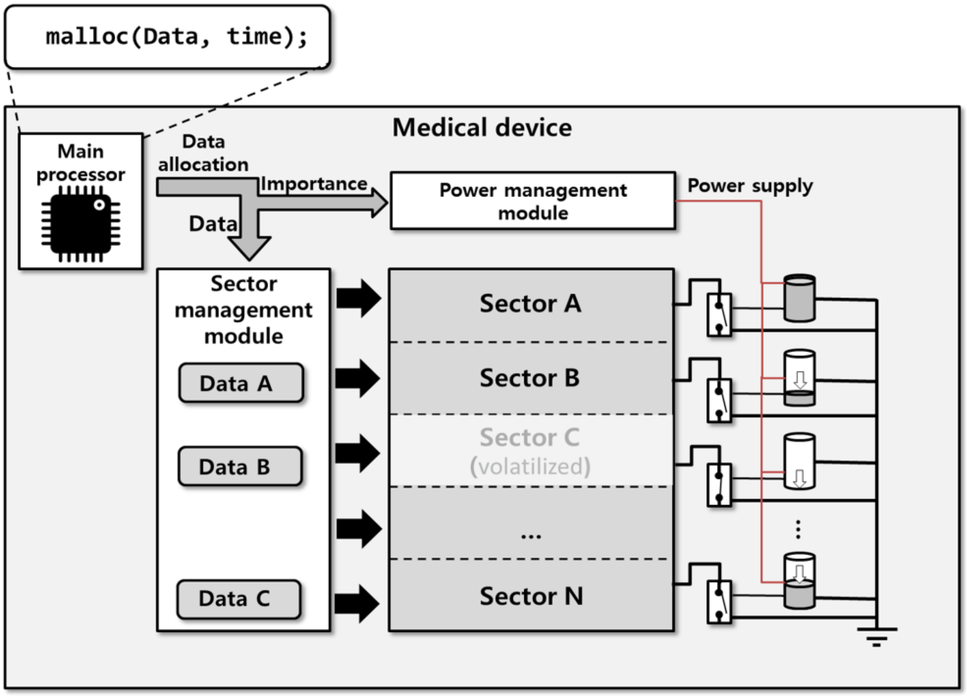

Figure 1: Conceptual Architecture of the Hourglass-Concepted Memory

Keywords: Embedded system security, IoMT, Medical device

Acknowledgments

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2019-0-00426,Development of active kill-switch and biomarker based defense system for life-threatening IoT medical devices, 20%) and National Research Foundation of Korea (NRF) (NO.NRF-2020R1A2C4002737, Intelligent Incident Investigation Platform for IoT CERT, 80%)

References

[1] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, Q. Mohammad, and S. Alrabaee. Security vulnerabilities detected in medical devices. In *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, pages 1–6. IEEE, 2020.

[2] C. Camara, P. Peris-Lopez, and J. E. Tapiador. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of biomedical informatics*, 55:272–289, 2015.

[3] A. Chacko and T. Hayajneh. Security and privacy issues with iot in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, 4(14), 2018.

[4] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn. Internet of things (iot): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, pages 321–326. IEEE, 2016.

[5] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem. Ideas and challenges for securing wireless implantable medical devices: A review. *IEEE Sensors Journal*, 17(3):562–576, 2016.