ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Enhanced Access Control Scheme for Implantable Medical Devices

Perla Krishnakanth
Department of Embedded Systems,
Nova College of Engineering and Technology,
Hyderabad, Telangana – 501512, India.

Abstract:
Implantable medical devices (IMDs) are electronic devices implanted within human body for diagnostic, monitoring, and therapeutic purposes. It is imperative to guarantee that IMDs are completely secured since the patient's life is closely bound to the robustness and effectiveness of IMDs. Intuitively, we have to ensure that only the authorized medical personnel and IMD programmer can access the IMD. However, in recent years, several attacks have been reported which can successfully compromise a number of IMD products, e.g., stealing the sensitive health data and issuing fake commands. Up to now, there is no commonly agreed and well-recognized security standard and the protection of IMD is still an open problem. In this paper, we present a comprehensive survey of the existing literature on IMD security, with a focus on the access control schemes to prevent unauthorized access. Specifically, we first reviewed the security incidents, IMD threat model and the development of regulations for IMD security. Next, we classified existing IMD access control schemes based on architecture, type of keys used, access control channel and logic. We also analyzed how different access control models can be adopted to secure IMD. Besides, we particularly discussed the viability of online authentication and low/zero power authentications in the IMD context.

INTRODUCTION:

Nowadays, the lives of millions of patients rely upon IMDs implanted within their bodies to treat a variety of diseases and conditions such as cardiac arrhythmias, diabetes, Parkinson's disease, or for cosmetic purposes.

According to the Transparency Market Research's report [1], the U.S. implantable medical devices market is expected to be worth $73,944.3 million by 2018. The IMDs [2] [3] are small in size and thereby resource constrained in terms of computational power, storage and battery. Unlike other electronic devices, the battery recharge or replacement for IMDs requires invasive surgery. Some researchers have been seeking the feasibility to incorporate the wireless charging technology (e.g., magnetic resonance) into IMDs, but it is in the very early stages and still faces significant regulatory hurdles [4]. Despite being very promising, the wireless charging enabled IMD product will not be released to the market, without many years of reliability testing (e.g. interference with other metal devices) and clinical trials (e.g. effect on human organs and tissues).

Hence, at the current stage, reducing energy consumption is still one of the top priorities in IMD design. Usually, IMD batteries should last from 5 to 10 years, which greatly limits the complexity of security mechanisms to be performed. For example, complicated cryptographic computations and long-range wireless transmissions are all considered unaffordable. The IMDs are facing a range of malicious attacks launched by external adversaries and unintentional mistakes in software or firmware design. Modern IMDs are equipped with a radio transceiver to communicate with an external device generally known as "Programmer". An authorized IMD programmer can issue commands to change the IMD configuration settings (e.g., parameter, dosage) and extract the medical data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Some IMDs are connected to the hospital networks or the Internet hence can be remotely monitored and operated by the doctors. However, the wireless communication and networking capabilities in IMDs are the major source of security risks. Due to the openness of the wireless channels, all transmitted packets can be captured by nearby eavesdroppers. This can not only expose patient privacy like the presence of IMD and its model, but also lead to other classic wireless attacks such as forging, tampering, and replying the messages. Additionally, if the IMD supports remote access by the doctor or the hospital, cyber attacks targeted at the hospital network/server may steal the patient data or the credentials.

Therefore, the development of lightweight but effective access control scheme for IMDs is highly desired. Security and privacy issues have been reviewed in several existing works. In this article, we conduct a comprehensive survey specifically on the access control scheme for IMDs. We also studied some authentication schemes for resource-limited body area networks (BANs) and secret key sharing methods for smart phones, which can potentially be adopted for IMD access control. The paper first summarizes the IMD security incidents of unauthorized access reported in recent years, and discusses the threat model IMD is facing and the current regulations on IMD security.

Then, the existing IMD access control schemes are classified into four categories in terms of the access control architecture and the type of keys being used, including direct access control with pre-loaded keys, direct access control with temporary keys, indirect access control via a proxy, and anomaly detection based schemes. Next, we present how different types of access control models can be applied to the IMD context. Finally, we discuss the viability of using online authentication server and embedding low-power (zero-power) authentication in IMD.

IMD Security Incidents:

Halperin et al [10]. Presented the vulnerabilities of a commercial implantable cardioverter defibrillator (ICD). Equipped with an oscilloscope and a software radio, they managed to reverse-engineer the ICD's communications protocol and obtain the personal information of the patient and the ICD. Furthermore, they also launched active attacks to change the therapy settings and drain the battery more rapidly. Similarly, eavesdropping attacks and active attacks can also compromise commercial glucose monitoring and insulin delivery system. After reverse-engineering the communication protocol and packet format, they were able to impersonate the doctor and alter the intended therapy by replaying and injecting messages with a software radio. A security professional Barnaby Jack has also revealed serious security flaws in IMDs, and demonstrated how an adversary can remotely take full control of insulin pump, pacemaker and ICD [7].

Even though IMD manufacturers are supposed to take responsibility for the security incidents and vulnerabilities in their products, they are unwilling to include strong security mechanisms since these changes will result in additional cost and time to the market. In 2014, an independent security researcher Billy Rios discovered 100 vulnerabilities in the communications system in the PCA 3 Life care infusion pump software by medical device company Hospira (HSP), which allows a hacker to tap into the pumps and change the amount of medication they've been set to dispense. Rios notified Hospira, but the company failed to respond to him.

Hospira stayed silent on the issue until another researcher Jeremy Richards publicly disclosed the vulnerability in April 2015. The U.S. Food and Drug Administration (FDA) and the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team sent out advisories notifying hospitals of the danger of Hospira pumps, and encouraging the transition to alternative infusion systems.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IMD Threat Model:

Two types of adversaries can be involved in an attack targeted at IMD: (i) Passive Adversary. A passive adversary can only eavesdrop on the wireless channel and listen to the messages exchanged between the IMD and the IMD programmer. Given an unencrypted radio channel, a passive attack can break the confidentiality and the authentication. Specifically, it can determine whether a person is carrying an IMD or not; obtain the type, model, and serial number of the IMD; intercept the unencrypted data and disclose private information about the patient, such as the name, age, conditions, ID, health records, etc. (ii) Active Adversary. After analyzing and reverse-engineering the communication protocol between the IMD and the programmer, an active adversary is able to tamper their messages and send unauthorized commands to the IMD (e.g. changing the configurations and parameters). The active attack could result in fatal threat to the patient.

A standard assumption in current literature is that the adversary will not approach the patient or make physical contact, deterred from leaving criminal evidence such as fingerprint, witness, or video taken by the surveillance camera. In this sense, the simple proximity-based access control scheme plus a lightweight key generation mechanism (generate a shared key between the IMD and the programmer to encrypt the communication) is sufficient to secure the IMD. However, Rushanan et al. Remark that this adversarial model neglects subtle classes of attacks by people known to the victim. We also consider that the attack can be launched automatically through the wireless channel without manual operation and physical contact, which means the adversary, can pretend to be a pedestrian happened to walk by. Besides, the adversary in the close range may be just a colluder collecting the basic information of the IMD (e.g. model, serial number) or amplifying the wireless signal, while the active adversary is launching sophisticated attack far away.

Existing access control schemes for IMD have been focusing on two general attack models. In the first type of attacks, an unauthorized programmer aims to obtain access to medical data stored in the IMD, send malicious commands, or change the device configurations. In the second type of attacks, an unauthorized programmer repeatedly connects with the target IMD, triggering the continuous execution of authentication computations in order to drain its battery. In addition, this may also result in the denial-of-service (DoS) which can prevent authorized emergency treatments.

IMD Regulations on Cyber security:

The U.S. Food and Drug Administration (FDA) is the governmental agency that supervises and regulates the medical device industry. FDA has been keeping an eye on the security incidents of medical devices. In order to improve the IMDs security and ensure that patients are safe, FDA has provided guidelines regulating medical device cyber security. In Oct. 2014, FDA released the guidance on the Premarket Submissions for Management of Cyber security in Medical Devices, and the more recent draft guidance of Post market Management of Cyber security in Medical Devices is released in Jan 2016 [6].

The premarket submission guidance provides recommendations to consider and document in FDA medical device premarket submissions to provide effective cyber security management and to reduce the risk that device functionality is intentionally or unintentionally compromised. To guard against vulnerabilities, the FDA urges manufacturers to consider cyber security during the design and development phase of the medical device. It also recommends manufacturers establish a cyber security vulnerability and management approach as part of their software validation and risk analysis. The draft guidance of post market management in cyber security encourages manufacturers to implement an effective cyber security risk management program for both premarket and postmarked lifecycle phases.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Specifically, it highlights that manufacturers should maintain an ongoing process of monitoring, identifying and addressing cyber security vulnerabilities in medical devices once they have entered the market. Additionally, it outlines the steps manufacturers should take to continually address cyber security risks with their devices.

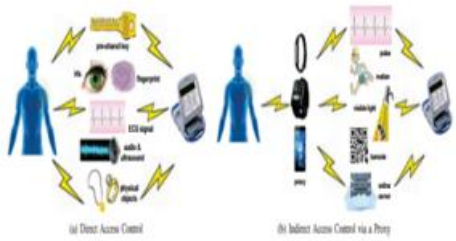

Fig. 1: IMD Access Control Architecture

However, these guidelines are mostly only recommendations and not legally binding. There is no validation and verification of the new IMD products (software and hardware) and their cyber security documentations by a trusted agency. The protection of IoT devices still relies on the research and development team of each individual manufacturer.

Conclusion:

This paper surveys the state-of-art approaches to enforce access control on IMDs. We roughly classified them into 4 different groups: direct access control with pre-loaded keys, direct access control with temporary keys, indirect access control via a proxy, and anomaly detection based schemes. For each group, we presented the affiliated related works together with their advantages and deficiencies. Additionally, we studied how various access control models can be used to protect the IMD. Finally, the viability to use online authentication server and low-power (zero-power) authentication techniques are discussed.

References:

[1] Transparency Market Research, "Implantable medical devices market - u.s. industry analysis, size, share, trends, growth and forecast 2012 2018," 2013.

[2] R. F. Xue, K. W. Cheng, and M. Je, "High-efficiency wireless power transfer for biomedical implants by optimal resonant load transformation," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 60, no. 4, pp. 867–874, April 2013.

[3] K. M. Silay, C. Dehollain, and M. Declercq, "A closed-loop remote powering link for wireless cortical implants," IEEE Sensors Journal, vol. 13, no. 9, pp. 3226–3235, Sept 2013.

[4] B. Boston, "Wireless power supplier witricity expands medicalindustry footprint," http://www.betaboston.com/news/2015/08/26/wireless-power-supplier-witricity-expands-medical-industry-footprint/, 2015.

[5] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks," in 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 524–539.

[6] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices," Journal of Biomedical Informatics, vol. 55, no. C, pp. 272–289, Jun. 2015.

[7] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), Nov 2014, pp. 246–249.

[8] 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, vol. 17, no. 3, pp. 562–576, Feb 2017.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[9] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," IEEE Access, vol. 4, pp. 959–979, 2016.

[10] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in Proceedings of the 49th Annual Design Automation Conference, ser. DAC '12, 2012, pp. 12–17.