Security Vulnerabilities on Implantable Medical Devices

Ana Longras
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
ana.longras@ipvc.pt

Henrique Oliveira
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
henriqueoliveira@ipvc.pt

Sara Paiva
Instituto Politécnico de
Viana do Castelo, Portugal
sara.paiva@estg.ipvc.pt

Abstract — **Implantable medical devices are used for critical functions like diagnosis, prevention, control, treatment or life-enhancing patients with chronic diseases, through diagnosing and/or monitoring for better care and quality of patients' lives. Communication between medical devices and healthcare professionals is of utmost importance to treat health data and critical functions without the need for patient surgery. Increasingly, the development, implementation and use of security mechanisms that can provide the availability of information, the integrity of medical devices and the confidentiality of data are needed. Alteration of data, theft, improper access to this information, or even denial of service in a healthcare system can lead to the death of patients on devices such as these essential to life. This paper mainly contribution is a research on implantable medical device vulnerabilities and attack mitigation strategies.**

Keywords - Medical Devices; Security; Vulnerabilities; Attacks; Mitigation.

I. INTRODUCTION

The rapid aging of the world population is an undeniable fact. It is estimated that in 20 years, 20% of the world population is over 65 years old, according to the Population Reference Bureau [1]. For economic and public health reasons, ensuring quality and health care for the elderly is a priority. Wearables and implantable medical devices (IMDs) are a way to achieve this goal and today, given the advances in technology, it is perfectly possible to develop and make it accessible to everyone. Nowadays, there are several implantable medical devices, from hearing aids, pacemakers, neurostimulators, insulin pumps to retinal implants [2], as shown in Figure 1. They provide healthcare and quality services such as monitoring, memory enhancement, managing of home appliances, access to medical access and communication in emergency situations. The way these devices communicate between themselves and central servers and/or databases is something to have in mind as it is an aspect over which attacks can occur. The concept of telemetry arises in this context [3] as it refers to the communication process where measurement data is collected from remote or inaccessible locations and then made available at a receiving monitor [4]. Wireless communications are present on most devices nowadays.

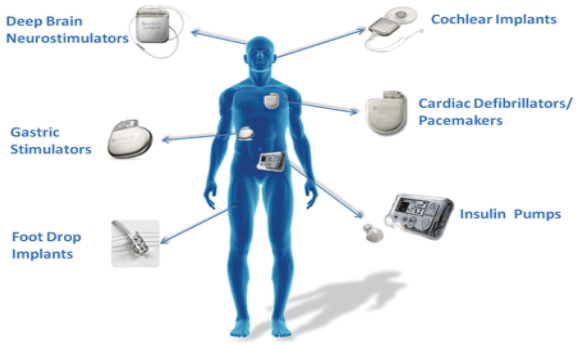

Figure 1. Wireless implantable medical devices (adapted from [14])

The end of wired devices eliminates restrictions on body positions, or on fragile structures such as the heart or spinal cord that would be damaged by moving wires, helps simplify surgical procedures and help minimize common surgical complications in implants when using wired connections [5]. Hence devices are increasingly equipped with wireless, Bluetooth or radio frequency telemetry (RF) communication capabilities. However, the evolution of medical device communication technologies has not been accompanied by increased security. The number of health safety incidents has been increasing, as shown in Figure 2.

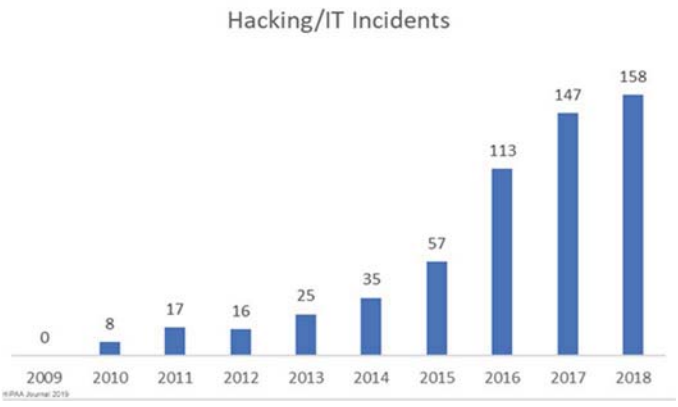

Figure 2 - Number of healthcare hacking incidents

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

Authorized licensed use limited to: b-on: Instituto Politecnico de Viana do Castelo. Downloaded on February 11,2022 at 17:01:27 UTC from IEEE Xplore. Restrictions apply.

The most widely used wireless communication is now Wi-Fi, a mechanism that is widely exposed to vulnerabilities and a mean to conduct security attacks. This paper describes the results of research on implantable medical device vulnerabilities, highlighting the radio frequency and wi-fi communications used to send packets between the device and the monitoring system. Introducing key security concerns associated with device architecture and deployment and usage, listing possible system failures, threats, attacks, and mitigation measures for device vulnerabilities.

This paper is structured as follows. Section II consists of a brief introduction to the topic of medical and implantable devices. The most common vulnerabilities of these devices are presented in section III, while Section IV presents models of possible attacks that affect systems where medical devices are used. Section V is based on presenting measures to mitigate vulnerabilities by preventing the success or at least decreasing the severity of potential attacks. Finally, we present conclusions of this work.

II. MEDICAL DEVICES OVERVIEW

As afore mentioned, many IMDs use telemetry which consists of measuring medical devices data and remotely transmitting this data to a central monitoring point to track the control, maintenance and performance of medical devices. In this scenario, there are two main aspects concerning security and safety in the architecture of solutions of IMDs: the medical device and the monitoring system. Regarding the medical device, it contains confidential patient data and information, and also provides access to sensitive medical information [6][7], facts that require big security concerns. IMDs are also deployed to control substances in the body, insert treatments, and other vital functionalities so assuring they are not attacked can be a matter of serious health conditions or even life or dead situations. On another hand, insurance companies are a major stakeholder in accessing IMD data. If, on the one hand, they are interested in having access to the information in order to refuse to make or renew or increase the insurance amount based on the patient's risk; on the other hand, they are the providers of equipment to patients, when they are aware of the vulnerabilities, they can claim compensation. Regarding monitoring systems, they keep a history of transmissions, vital signs, device battery longevity, a symptom diary, device information and other useful information depending on the type of the device. Many of them run on operating systems like windows XP, with several known vulnerabilities which compromise the monitoring system of these solutions and hence the entire solution.

III. VULNERABILITIES

There are several vulnerabilities associated to the usage of IMDs that will be described in this section, namely radio frequency communication, Wi-Fi connections and the lack of authentication validation.

A. Radio Frequency Communication

Devices that use radio frequency (RF) to communicate has a low probability that attacks are successful as the attack needs to be done at close range from the patient. Radiofrequency function is activated in the hospital during follow-up appointments [8]. There is a need for short-range patient access with active RF functionality for an attach to be executed. The frequency of any wireless device is publicly available online and is easily obtained from the Federal Communications Commission ID (FCC ID). On some devices, it is also available on the back of the device [9]. The result of successful radio frequency scanning may include the ability to read and write any valid memory location on the device [10].

B. Wi-Fi Connection

In addition to radio frequency communication, attacks can occur during a period when the device is connected to the internet, over Wi-Fi communication to send or receive data. Packet exchange is through clear text, so an attacker could capture data exchange packets and extract sensitive information such as device serial numbers. There are several models of medical devices with this vulnerability, such as the example identified in CVE-2018-10634 [11]. This vulnerability undermines the integrity and confidentiality of data obtained from insulin pumps and most devices that use Wi-Fi communications [12].

C. Lack of authentication validation

Pacemakers and Implantable cardioverter defibrillator (ICDs) devices that transmit heartbeat load data or heart failure metrics, contain a magnetic switch (or sensor) that is activated by strong magnetic fields [13]. Current magnetic key-based access does not require any authentication system and is therefore insecure. Table 1 presents a summary of what was previously explained in relation to the severity of the risk, the description of the risk as well as examples of how the attack can be carried out.

TABLE 1 – Level of vulnerability of medical devices.

Security	Description	Examples
Low - 0	Neither vulnerabilities nor malware on device	Device with upgraded software version
Moderate - 1	Vulnerabilities on device, no exploits yet	Weakness in protocol Potential buffer overflow
High - 2	Vulnerabilities on device with known exploits	Protocol weakness or buffer overflow can be used for unauthorized access
Very High - 3	Malware on device	Hardware Trojan or software backdoor on device

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

Authorized licensed use limited to: b-on: Instituto Politecnico de Viana do Castelo. Downloaded on February 11,2022 at 17:01:27 UTC from IEEE Xplore. Restrictions apply.

IV. ATTACKS ON IMPLANTABLE MEDICAL DEVICES

Until now, security attacks on medical devices have been relatively rare, but IMDs are being increasingly common, thereby increasing the incentives to attack them for profit. A modern pacemaker has the capability to collect information about patient and transmit it via Wi-Fi to an access point or medical devices used during hospital checkups. The access point devices, which collect information about the patient's health while at home, sends the data to remote servers. Pacemakers that can send data via the internet can help patients with mobility issues. However, the communications protocols used when sending the data to remote servers is very trivial and is susceptible of being hacked [14]. Concern about the vulnerability of medical devices like as pacemakers, ICDs, insulin pumps, defibrillators, fetal monitors and scanners is growing as healthcare facilities increasingly rely on devices that connect with each other, with hospital medical record systems and with the internet. Already in 2015, two security researchers discovered over 68,000 medical systems that were exposed online, and 12,000 of them belonged to one healthcare organization [15]. The major concern with this discovery was that these devices were connected to the Internet through computers running very old versions of Windows XP, a version of the OS which is known to have lots of exploitable vulnerabilities. These devices were discovered by using Shodan, a search engine that can find IoT devices online that are connected to the Internet. These are easy to hack via brute-force attacks and using hard-coded logins. Attacks can cause failures such as exposing confidential patient information, mishandling, poor monitoring, access to the equipment system, changing device scheduled tasks, creating battery swings or even administering inappropriate stimuli or disabling alarms. As afore mentioned, implantable medical devices (IMDs) have very limited power resources, are powered by a non-rechargeable battery, and replacing the battery requires surgery, processing, and information storage. Due to limited resources, they are very vulnerable to resource exhaustion attacks.

The exploitation of Wi-Fi communication for not demanding proximity to the victim is the most used for attacks. The ease of deploying backdoors in hospital networks, and with medical devices connected to the same hospital network, multiple systems can be infected with malware, including the possibility of twenty-four insulin pump and pacemaker failures allowing remote control [16].

Attacks such as a resource exhaustion attack, known as a forced authentication attack, is a type of denial of service attack (DoS). This attack applies to IMDs that communicate wirelessly with external readers or monitors. When an external reader attempts to connect to an IMD, the first step is the authentication between the IMD and the reader. If the authentication is not successful, the IMD will discontinue the communication with the reader. However, the authentication process itself requires IMD to make some communications, which consume a considerable amount of power and if an unauthorized reader repeatedly attempts to connect to an IMD, it will cause the IMD to perform multiple authentications and thus expend a lot of the required battery power. In addition, this type of attack generates a large amount of security logs, overloading IMD storage. By reducing battery life, damage can render the device inefficient. Next we summarize some types of attacks to medical devices, such as radio jamming, main-in-the-middle attack, replay attack and code injection.

Radio Jamming: this type of DoS occurs when communication is blocked, and interference is created. The attacker abuses system resources by repeatedly sending valid or invalid messages [17].

Man-in-the-middle attack: The attacker listens to gain access to sensitive health information, neither interrupting nor altering communications. Another situation will be that the attacker may choose to intercept data or code from a medical device while radio frequencies are active, to relay altered data to the monitor or alarm system [17].

Replay attack: this attack also consists of the intersection and representation of the medical device or a monitoring system, represented by a network attack in which valid data is manipulated. Such an attack can be used not to receive treatment, for example, by mixing the order of packets arriving at IMD or worse, continuously sending the same message to medical devices to the monitoring system.

Code injection: occurs when the attacker modifies the source code on a medical device, monitor or even a possible alarm system to perform an undefined operation, for example, modifying the pacemaker software to constantly provide electric shocks.

Table 2 summarizes potential vulnerabilities with their attacks, likelihood of attack, and system impact.

TABLE 2 – List of vulnerabilities.

Threats	Attack	Probability	Impact
Radio Frequency Communication	Scanning	Low – need to be done at close range	-Read and write any valid memory location on the device; - Data corruption.
Wi-Fi Connection	Capture/ Sniffing	Medium – need the device connect to the internet. But packets are in clear text	-Undermines the integrity and confidentiality of data obtained
Lack of authentication validation	DoS	Low – need strong magnetic fields	-System Availability

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

Authorized licensed use limited to: b-on: Instituto Politecnico de Viana do Castelo. Downloaded on February 11,2022 at 17:01:27 UTC from IEEE Xplore. Restrictions apply.

V. Attack Mitigation

A successful attack can alter the behavior of a medical device. One thing to be done is to validate the security of the device firmware implementation as sources cannot be modified without authorization. It is also important to encrypt the firmware installed on medical devices to prevent decryption of content. Another measure will be to improve the authentication process by limiting the number of requests to the system to prevent system overloading and therefore to prevent denial of service. Another way to mitigate attacks is to encrypt all communication packets, make data integrity checking, anti-replay features and usage restrictions. Also, implementing a smart device traffic monitoring system to control system logs, monitor power variations and process, prevent anyone from listening on the network to "play back" data and then modify for malicious purposes. Finally, have the entire monitoring system in high availability to ensure availability and access control to validate the entity to access.

VII. Conclusion

Medical devices increasingly use wireless communication and internet connections. In this paper, we discussed the security of communications of medical devices, centered on the security of communications with other systems, such as the monitoring system, very important because it interferes with people's health, namely with life itself. Therefore, it is essential to prioritize "safety". We analyzed several vulnerabilities in these systems, possible forms of attacks and how to mitigate them. The analysis revealed potential security risks arising primarily from unencrypted communications and the limited resources on devices. As we mentioned, it is a system that endangers human life. Thus, there is no margin for failures or errors. These systems will continue to have new challenges in the coming years and new solutions and proposals will have to be made. Future work we intend to do includes the proposal of a secure architecture that includes medical devices and monitoring systems.

References

[1] Kinsella, K.; Phillips, D.R. Global aging: The challenge of success. Pop. Bull. 2005, 60, 1-42.

[2] Darwish A, Hassanien A. Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors (Basel). 2001;11(6):5561-95.

[3] Moravejosharieh A, Lioret J. Performance evaluation of collocated ieee 802.15.4-based wireless body sensor networks. Annals of Telecommunications. 2016; 71(9/10):425-40.

[4] R. Ritter, J. Handwerker, T. Liu and M. Ortmanns, "Telemetry for Implantable Medical Devices: Part 1 - Media Properties and Standards," in IEEE Solid-State Circuits Magazine, vol. 6, no. 2, pp. 47-51, Spring 2014.

[5] Ferguson JE, Redish AD. Wireless communication with implanted medical devices using the conductive properties of the body. Expert Rev Med Devices. 2011;8(4):427–433. doi:10.1586/erd.11.16.

[6] Hei Xiali, Du Xiaojiang. Security for wireless Implantable Medical Devices, 2013. doi:10.10077978-1-4614-7153-0.

[7] K. Fu, "Inside risks: reducing risks of implantable medical devices", Communications of the ACM, vol. 52, pp: 25-27, Jun. 2009.

[8] D. Panescu, "Emerging technologies: wireless communication systems for implantable medical devices," Engineering in Medicine and Biology Magazine, vol. 27, pp: 96-101, Mar.-Apr. 2008.

[9] "FCC ID Search." Federal Communications Commission, 2 Nov. 2017, https://www.fcc.gov/oet/ea/fccid.

[10] "Medtronic Conexus Radio Frequency Telemetry Protocol: CISA." Medtronic Conexus Radio Frequency Telemetry Protocol | CISA, https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01.

[11] National Vulnerability Database. NVD, https://nvd.nist.gov/vuln/detail/CVE-2018-10634.

[12] "Insulin pumps - global pipeline analysis, opportunity assessment and market forecasts to 2016, GlobalData." [Online]. Available: http://www.globaldata.com.

[13] Medtronic, Inc., "Implantable pacemaker and defibrillator information: magnets," www.medtronic.com/rhythms/downloads/3215ENp7magnetsonline.pdf.

[14] Chacko, Anil & Hayajneh, Thaier. (2018). Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. 4. 155079. 10.4108/eai.13-7-2018.155079.

[15] C. Catalin, "Thousands of IoT Medical Devices Found Vulnerable to Online Attacks," 29 September 2015; http://news.softpedia.com/news/thousands-of-iot-medical-devices-found-vulnerable-to-online-attacks-493144.shtml.

[16] Storm, Darlene, and Darlene Storm. "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks." Computerworld, Computerworld, 8 June 2015, https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html.

[17] D. Raymond and S. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," IEEE Pervasive Computing, vol.7, pp: 74-81, Jan.-Mar. 2008.

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

Authorized licensed use limited to: b-on: Instituto Politecnico de Viana do Castelo. Downloaded on February 11,2022 at 17:01:27 UTC from IEEE Xplore. Restrictions apply.