A Review on Recent Advances in Implanted Medical Devices Security

César Brito
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
cesarbrito@estg.ipvc.pt

Luis Pinto
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
lfilipepinto@ipvc.pt

Victor Marinho
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
victormarinho@ipvc.pt

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

Pedro Pinto
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal
pedropinto@estg.ipvc.pt

Abstract — **The Implanted Medical Devices (IMD) industry has grown over the past few decades and is expected to grow in the coming ones. Being an asset for the health and quality of life of a patient, the availability of IMD-related products, their increasing complexity and advances in communication capabilities do not seem to have been seamlessly accompanied by cybersecurity concerns. Recent IMD can be integrated in the concept of IoT (Internet of Things) and thus, they are also exposed to attacks impacting on privacy and, above all, on the health and even the life of the device users. While in an early stage of the IMD development, the security procedures were based on the existing classic protocols and models and their functional capabilities were the focus of development, recent efforts have been made to address security from the start. In this paper we review the most recent contributions on the cybersecurity of IMD products and we highlight innovative ideas that represent new design and development paradigms of these devices next generations. In this review it is reinforced that the technological evolution and the progressive access of attackers to resources capable of exploiting multiple vulnerabilities can have a crucial impact in the IMD already implanted in the patient's body, designed to remain in operation for many years. Also, it brings the need to develop novel and robust protocols to guarantee security compatible with constrained computing resources and extremely low energy requirements to be feasible. Finally, the security and privacy concerns regarding this kind of devices should be addressed in the design phase and policies must move from damage mitigation to threat prevention.**

Keywords – Implanted Medical Devices; IMD Protocols; Internet of Medical Things; Medical Devices; Vulnerabilities; Security; Wireless communication attacks.

I. INTRODUCTION

The use of IMD (Implanted Medical Devices) can be an advance in the health and quality of life of patients. In general, the global Internet of Medical Things (IoMT) market is expected to swell to a $158 billion valuation in 2022, up from $41 billion in 2017 [1]. The perspective is that the continuous development of more efficient devices, with greater capacity for monitoring biological data and their transmission to decentralized applications or databases will lead to an exponential growth in the use of this device in the coming years. However, the risk of security threats to transmitted data and to the smooth functioning of IMD has also grown at an accelerated rate. Manufacturers of this type of products, as for most of the devices that have been integrated into the generic concept of Internet of Things (IoT), have put their focus and attention more on the development and improvement of the medical capabilities of these devices and less on security measures. In some situations, security measures are taken after the discovery of vulnerabilities, or even while or after the execution of an attack, while in this and other areas is relevant to adopt a preventive approach from the first step of product design and development.

This paper reviews the most recent contributions on solutions and mitigations of IMD security issues, using a defined methodology based on innovation and feasibility. The review provided herein intends to aid researchers and manufacturers to adopt a security-by-design while innovating and developing their products according to the most stringent and recent security strategies. Considering the interest of manufacturers in developing their software based on robust frameworks and protocols, that are also able to resist to increasingly sophisticated attacks, their work can benefit from the most recent studies and contributions published in this area.

This paper is structured as follows: Section II reviews IMD vulnerabilities and attacks. Section III presents the most recent contributions divided into two groups: the first, presenting a conceptual framework-type approach and complementary contributions to IMD security; the second introducing new technological approaches by reviewing the newest security protocols and procedures. Section IV presents the main conclusions of this work.

II. REVIEW ON IMD VULNERABILITIES AND ATTACKS

There are several academic studies, mentioned along this paper, news, and case reports of real attacks or, at least, discovery of vulnerabilities that become threats to a potential attack regarding IMD. The exploitation of these devices may negatively impact in (1) the confidentiality of the healthcare related data that belongs to the private forum of the device's user; (2) the authentication of health professionals who need access to the data and who can interact with the device either to health monitoring or to functional parameters configuration; (3) the availability of service of the device as it can be attacked in order to cause malfunction or even shutdown, endangering the health and, in extremis, the patient's own life. Deep analysis of the types of attacks, technologies involved and the damage they

2021 16th Iberian Conference on Information Systems and Technologies (CISTI)
23 – 26 June 2021, Chaves, Portugal
ISBN: 978-989-54659-1-0

can cause has been the subject of several studies, with different approaches, that may serve as a framework for a better understanding of the scope of this text.

In [2], authors describe, focused on IMD devices, the potential vulnerabilities of radio frequency communication, Wi-Fi connection and lack of authentication validation and how radio jamming, man-in-the-middle attack, replay attack and code injection can exploit these vulnerabilities. They present condensed information in a table evaluating, for each one, the probability of occurrence and the estimated impact. They concluded that the main risks come from unencrypted communications and the limited resources on devices.

Authors in [3] describe reports of real attacks or vulnerabilities of public exposure on various IMDs from different companies covering infusion pumps, insulin pumps and pacemakers, exposing the serious insecurities of many devices currently used by thousands of patients. The paper makes a factual and critical analysis of the manufacturers' behaviour regarding their products failures and the little attention and slowness related to cybersecurity, concluding that they only seem to act when pressed by the United States Food and Drug Administration (FDA) or when threatened with criminal prosecution for violation of medical product safety and patient medical information protection laws.

In [4], the authors describe attacks of resource-constrained part of IoT devices (including IMD) using short-range wireless communication technologies such as Wi-Fi, Bluetooth, ZigBee, and RFID. A taxonomy of attacks is proposed classifying them based on the fundamental security services, i.e., authentication, confidentiality, integrity, and availability. Each attack in the taxonomy is detailed and for each, authors propose possible countermeasures. The authors remark that most attacks were due to the flaws left on the authentication protocol, so, authentication is the most important and critical security service. Compromising it would, in most cases, lead to the compromising of the remaining security services. Therefore, if authentication is perfectly implemented, many attacks will be completely mitigated. As IoT is rapidly transforming the Internet into a Thing-to-Thing communication system (including IMD as smart healthcare devices), authors defend the need for new authentication protocols, thing-to-thing authentication protocols, avoiding that IoT can be exploited as a networking platform to conduct large scale, distributed, and devastating cyberattacks, using many heterogeneous devices which security configuration is unknow as bots.

There are reports of tampered data, which compromises the diagnosis and monitoring of the patient's disease and these changes often were made in the downstream computer system. As an example, in [5], a work dated 2019, an ethical hacking study was performed to an Intelligent Medical Diagnosis System (IMDS) in which the two most common web-based attacks (brute force and SQL Injection) were carried out and, with that, ECG data were changed affecting the correct diagnosis of the patient's heart disease. The authors also presented and evaluated prevention strategies for these attacks.

Security weaknesses that can lead to successful attacks on IMD and thus, a key factor is the robustness of the protocols and the associated encryption and authentication techniques to prevent intrusion and the theft or tampering of confidential data. Since IMD are usually implemented in humans, data privacy issues are also important to be addressed. The increasingly widespread use of IMD and the need to securely access data from different users of the healthcare system (doctors, nurses, therapists, device programmers, etc.) raises concerns. Simple authentication can be complemented with adequate user privileges policies so each one accesses data according to their role to protect the patient's privacy.

The integration of IMD devices in the IoT global network as a smart healthcare system brings new threats and security concerns. The communications between IMD and remote servers or users may involve an intermediate device, typically a smartphone or smartwatch, making use of different wireless communication technologies in the entire process. This means that an attacker has more attack vectors to achieve his goals. On the other hand, the fact that there is a proximity between the IMD and the intermediate device, also allows innovative approaches. Therefore, IMD security needs attention regarding privacy, authorization, authentication, trust, accountability, auditability, confidentiality, and key management.

The design stage in the development of IMD is of crucial importance. Instead of using tools and methods of general application adapted to medical devices to address their security, the IMD manufacturers are urged to use up-to-day knowledge and methods in the design stage. These devices are increasingly miniaturized, they make use of wireless interfaces, and the battery power is limited which means that the impact of DoS attacks with successive attempts to authenticate, a virtually impossible situation in previous generations of IMD, can now seriously endanger the health and lives of patients. Even in older devices, it becomes necessary to balance the need to ensure privacy, availability, authenticity and other security requirements, with the demand of computing and power consumption to keep usability and battery life at an acceptable level. In view of all this, some innovative ideas have been proposed bringing to light new approaches and the use of innovative concepts. Ethical hacking is often done by researchers to anticipate the detection of vulnerabilities and propose corrections before damages can occur. The security of medical data must be seen globally in the entire communication system and not just in the IMD device itself.

III. Recent Advances on IMD Security

Responding to the increasing use of IMD and to the identification of their vulnerabilities, studies and solutions have been proposed to prevent attacks or mitigate their consequences. In this section the recent proposals and approaches reviewed are divided in two categories: (A) new or improved layered models and frameworks, with the proposals to ensure security in each protocol and stack to guarantee the security of the system as a whole; and (B), with new or adapted protocols or procedures that can be applied in IMD to enhance their security.

A. Security Mechanisms and Models for IMD

In the context of new devices development, in [6] it is proposed a model of a Secure IMD (SIMD), consisting of a specific firmware that can be applied in new or existing

ISBN: 978-989-54659-1-0

devices, intended to solve known firmware vulnerabilities, some with a few years of operation. According to the authors, the model is applicable to any type of medical device and is characterized as "risk mitigation" model. The firmware added to devices includes procedures that maintain a whitelist of medical devices approved to interact with the medical devices. Then, before any action is executed, the device checks the whitelist and verifies that any data (request, update, or command) is digitally signed prior to processing it. The authors argue that these new features do not interfere with the device operation and, although they introduce additional processing cost, the security level of the device is enhanced. Even when applied to an older generation system, SIMD can verify that all commands are within accepted parameters and come from a trusted source, except in emergency mode where a reduced operational mode is maintained.

In 2020, a model for a lightweight implementation of data security is presented in [7] intended to guide the software development of IMD while meeting specific security requirements for this type of devices. The proposed model is based on three protocol layers (as presented in Fig. 1). Layer 1 is the most basic layer and includes data integrity and mutual authentication (i.e., only the commands/data received from authenticated parties are processed). Layer 2 includes the properties of Layer 1 and the privacy of data. Layer 3 includes the properties of both previous layers and the confidentiality of data.

Network integrated technologies can be used to complement and improve the security of IMD. Authors in [8] propose the use of an Intrusion Detection Systems (IDS) for IMD running on a mobile phone/PDA. Being a relevant line of defence, the use of this type of technology implies a permanent monitoring of communication in search of abnormal patterns that may consist of suspicious activity but may generate false alerts. As a drawback, it requires significant energy consumption, processing and bandwidth which strongly limits its use generally.

The reviewed works consists of different approaches to enhance IMD security. While the goal of [6] is to enhance security in new and existing devices, in [7] a more complete approach is proposed by suggesting a model to implement in development stage. The IDS presented in [8] highlights that the protection of IMD can be performed in the device or in a perimeter involving it.

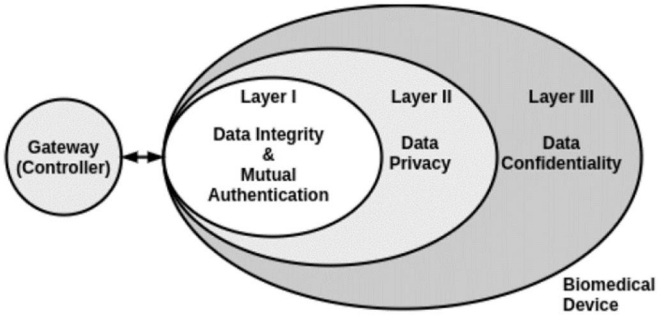

Figure 1. Three-layer model for the lightweight implementation of data security (extracted from [7]).

B. *Secure Protocols and Procedures for IMD*

In [9], it is proposed IMDfence, a Secure Protocol for IMD. The authors carried out an in-depth research of multiple proposals that emerged in recent years, assessed their strengths and weaknesses, and based on the assessment output, the authors proposed a more complete protocol. The final assessment of all proposals is presented in a table in which they identified compliance or not compliance with nine safety requirements, named basic security services, covering different aspects.

In the IMDfence proposal, the introduction of a smart card and a trusted third party, was taken as relevant to meet IMD particular security requirements such as access control, confidentiality, integrity, availability, non-repudiation, authentication, and emergency access. At the same time, the developed protocol also covers other requirements that are not so common but are important for the most recent and future generations of IMD, such as the bedside-reader operation, the multi-manufacturer support and flexibility/scalability. The bedside-reader operation is an IMD feature which is a bedside reader that sends data over the internet of the patient's treatment status when he is sleeping, allowing remote monitoring. The multi-manufacturer support allows IMD-security system to be manufacturer-independent because it is not possible to pre-emptively stock all the readers from all the manufacturers for emergencies (e.g., an ambulance should use one generic reader regardless of the IMD manufacturer and type). The flexibility/scalability where pre-shared secrets between the reader and IMD are not used and the device should not be limited to communicating with only a fixed number of readers limiting portability during emergencies, when there is a need for treatment outside home or in travels. Algorithms, rules, and protocol primitives were also developed by authors of this proposal to respond to all requirements allowing access to the IMD during emergencies without compromising security or patient safety.

Finally, particular attention was paid to providing the protocol with sensitivity and mechanisms able to deal and protect against battery Denial-of-Service (DoS) attacks. This involved security in all elements of the IMD ecosystem, that is, the communications between IMD and data readers (smartphone, smartwatch, etc.) and from those to the trusted third party such as an hospital server, providing for the use of various communication technologies (radiofrequency, Bluetooth, wireless). One of the most interesting aspects of this study is that the proposed solutions were simulated in several possible scenarios (combinations involving honest or malicious users, hacked, stolen or forged readers and attackers.). The impact of IMDefence system on the device overall performance was calculated in order to certify its real applicability from the perspective of the additional hardware necessary in IMD manufacturing to integrate this system, and to ensure the safety for the patient during its use. Indeed, additional energy consumption, system response delays, extra memory requirements, computational overhead, etc. were evaluated parameters to verify that patient safety is never jeopardized in what is the basic functioning of the IMD.

ISBN: 978-989-54659-1-0

In [10], a role-based hierarchical protocol for data access and encryption for IMD is presented. This work dated from 2019 introduced a role-based encryption and the access distribution within the same function to improve the security of the data while using the least possible resources, an important issue considering the constraints of IMD devices. This scheme ensures the security of the stored medical data and limits its access to the authorized entities in a hierarchically way based on their roles. It can be used by different kinds of IMD devices and ensures the protection of wireless communication against replay attacks by using a pseudo-random chaotic key generator and an algorithm system to generate distribution keys and data encryption respectively (as presented in Fig. 2). Even if an attacker intercepts and captures the logs sent, and if also he identifies several counter tags and their output from the chaotic generator, he is still unable to decipher the data logs.

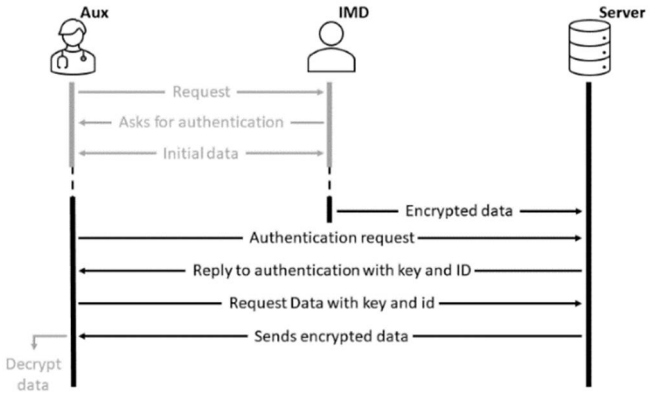

Figure 2. Block scheme of encryption/decryption process and communication protocol description (adapted from [10]).

In [11] it is proposed a secure protocol for data transmission between IMD and the receiving computer reinforcing protection in the user authentication to access the IMD data. In fact, authentication is not only verified at the beginning of the session but continuously, using facial recognition. This is important if an authorized user, as a doctor in the hospital, is receiving data from the patient device in his computer and, during the session, leaves the computer unattended making the data accessible to a malicious person. The procedure is divided in two phases: in the first, the authentication is done using an SHA-256 hash function in the user ID. The IDs of authorized users are not stored in clear text in the computer's memory preventing cache attacks and the ID is processed by the hash function to authenticate. After this phase, facial recognition techniques are used to assign predefined permissions to that user and manage their interaction with the IMD (sending commands, collecting data, etc.) ensuring that facial recognition is done permanently during the open session. If at any time this recognition fails, the session is immediately disconnected (for example, if the user leaves and leaves the computer alone). The transmission protocol uses nonce (number just used one time) to prevent replay attacks in which the messages are either repeated or delayed. The purpose of a nonce is to make each request unique so an attacker cannot replay a request in a different context, i.e., to ensure that old communications cannot be reused in replay attacks. The protocol design also prevents battery-depletion attacks. If an attacker tries to drain the IMD's battery by sending many invalid messages they are discarded since an invalid ID or invalid nonce is used.

Controlling which devices can read from or send commands to the IMDs is the focus of the access control protocol called ACIMD [12], proposed in 2020. It implements a distance bounding mechanism based on physiological signals, particularly electrocardiograms. The proposed scheme allows verifying the proximity between an IMD and a programmer (distance checking) where each entity can verify the identity of the other involved party and be sure of her/his presence during the protocol execution (mutual authentication). The authors state that the ACIMD protocol is more efficient than their predecessors regarding the number of exchanged messages and the computation cost (time and energy) and is able to operate in the normal and emergency operation modes typical for IMDs. The main contribution is the use of a short-range and secure channel for the transmission of a session key such as photobiomodulation. It allows short-range communications and needs line-of-sight between the transmitter and the receiver. Photobiomodulation (also known as Low-Level Light Therapy, LLLT) consists in the emission of light by a diode or laser in the spectral range of 600–1000 nm and at a low-power (<500 nW). Usually, session keys are used several times. Under this assumption, every time we need to renew the session key (including the first time) a key agreement protocol through the LLLT channel is executed before for distance checking and authentication verification. The feasibility of the proposal protocol was evaluated with an ECG (electrocardiogram) dataset of 199 subjects. An attacker having control over the mobile phone through malware, ransomware or physical possession can force the IMD to execute malicious actions without the user's knowledge. Cryptographic-based authentication protocols are not sufficient to prevent such attacks since the IMD cannot distinguish whether it has received a command from a legitimate user or an adversary. If the mobile phone is also used to wake up the IMD through the BLE (Bluetooth Low Energy) connection, an adversary having control over the mobile phone can also attempt to wake up the system repeatedly and drain its energy.

In [13], it is proposed a dual-factor authentication scheme where cryptographic authentication is complemented with a voluntary response from the user to consent the execution of the desired action such as an automatic drug delivery or data transfer. The protocol authors had chosen a touch-based voluntary response where the user taps on their skin near the IMD. Since most implants are subcutaneous, they can easily detect the tap-pattern and authenticate using this second-factor response. It is difficult or even impossible for an attacker to make this second-factor response to the IMD providing higher security guarantees. In addition to second factor authentication, the human voluntary factor (human touch) is also used for waking up the system protecting against energy-drainage attacks. An illustrative image of this protocol is presented in Fig. 3.

ISBN: 978-989-54659-1-0

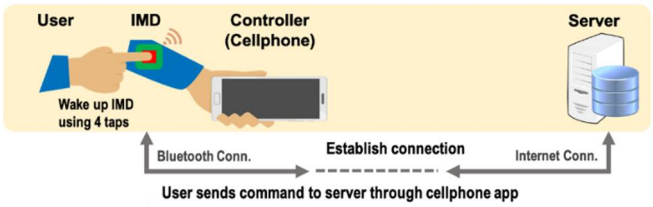

Figure 3. Proposed dual-factor authentication protocol to secure internetconnected implantable medical devices (adapted from [13]).

The study in [14] exploits the special characteristics of the Received Signal Strength (RSS) ratio between a wearable proxy devices (WPD) and IMD in wireless body area networks (WBANs) to distinguish legitimate users and attackers. The use of RSS for localization and attack detection purposes is quite common. However, considerable variations may result from body structure, environment dynamics and interference in the WBAN. An attacker can easily forge the information that results from simple RSS analysis by making changes in transmission power. However, if the analysis is made based on proportions between two RSS, the reliability and predictability are increased. This was the focus of this proposal, studying various scenarios for the nodes to be considered to implement the solution based on the proportion between the two RSS. The option was to use an indirect access control using a WPD. The analysis is now done by the ratio of IMD and WPD RSS. Moreover, based on the idea of proposed Authentication Request Filtering (ARF), two corresponding light-weight security protocols are presented to defend the Forced Authentication (FA) attacks and enhance the accessibility of IMD in emergency mode, respectively. The authors mathematically analysed the RSS ratio between WPD and IMD (Fig. 4), testing several distances and scenarios proving that it is possible to use this ratio to distinguish legitimate users and attackers due to the proximity to IMD.

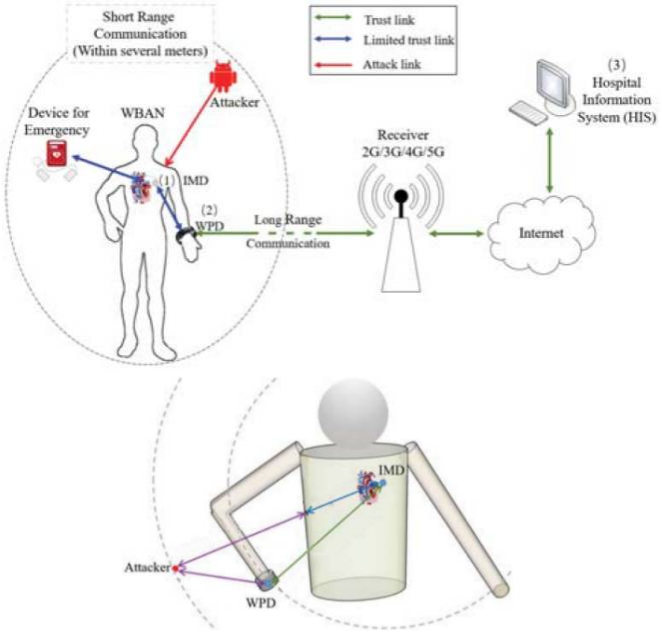

Figure 4. WBAN architecture of a personal healthcare system and schematic diagram of the variables involved in the calculation of the IMD and WPD based RSS ratio (extracted and adapted from [14]).

Table I presents a summary of the security requirements proposed in [9] and their correspondence with the papers reviewed. The security requirements are described as follows: (1) access control, so that user access and privileges are based in the type of user; (2) authentication to make sure that device access is always identified; (3) authorization to ensure that only valid privilege levels are assigned; (4) availability, to ensure that IMD is available whenever needed; (5) confidentiality to restrict access to legitimate entities; (6) emergency access because patient safety must always be more important than device security; (7) integrity consists of making sure the data is not tampered in any way; (8) non-repudiation to ensure that in case of a medical mistake the sender of the message is not able to deny it; (9) privacy to safeguard personal data; and (10) multi manufacturer support to make sure that in emergency situations the medical team does no need to know the make and model of the equipment; bedside reader which consists in an equipment that is placed by the bedside and reads IMD data when the user is resting; flexibility/scalability so that the IMD can communicate with a large number of readers increasing portability.

TABLE I. SUMMARY OF CONTRIBUTIONS ON PROTOCOLS FOR SECURITY REQUIREMENTS

Security requirement	Protocol					
	[9]	*[10]*	*[11]*	*[12]*	*[13]*	*[14]*
Access Control	√		√	√	√	√
Authentication	√	√	√	√	√	√
Authorization	√	√	√			
Availability	√	√				
Confidentiality	√	√	√			
Emergency Access	√			√		√
Integrity	√	√	√			
(8) Non-Repudiation	√	√				
(9) Privacy	√		√			
(10) Multi manufacturer support, bedside reader and flexibility/scalability	√					

IMDfence [9] is the most complete protocol, being the only one that deals with all the security requirements mentioned. Some of the protocols in the table ([12], [13] and [14]) focused in specific IMD security requirements, assuming that all the other requirements were already taken care. References [10] and [11] tried to take a more complete approach focusing in the more common security requirements.

IV. CONCLUSION

The development of new IMDs and their integration into the IoT require new security challenges and precautions. The addition of technologies and features also brings new threats. In older IMD that are still in use, updates must also be made due to new threats that keep appearing. In any case, the constraints of low computation, low energy consumption, small size, and difficulty of access for replacement, typical of IMD,

ISBN: 978-989-54659-1-0

remain. Therefore, this topic has been the subject of several research in the last years where different proposals are being made.

Currently, a myriad of attacks to IMD are possible due to the wireless technologies involved and the growing resources available to attackers. Encryption and authentication techniques considered secure for years can no longer be considered as being safe. Sniffing and packet analysis or data tampering became possible through Wi-Fi network. Denial-of-Service attacks that deplete the battery are easy to do. Fortunately, ethical hacking is often done by researchers to anticipate the detection of vulnerabilities and propose corrections before damages can occur. In addition, it must be considered that security of medical data must be seen globally in the entire communication system and not just in the IMD device itself.

In this paper, a review was made on the most common vulnerabilities and attacks on IMD, as well as on recent advances that have emerged in the last two years for solutions and mitigations of IMD security issues. The analysis of the proposals presented throughout this paper highlighted some important aspects to keep in mind. First, the need to design IMD security models and protocols that are increasingly robust and able to predict and deal with increasingly sophisticated attack threats. Then, new communication technologies and the growing integration of IMD in the IoT world require improved security standards, not only for the fundamental services of confidentiality, integrity, and availability, but also covering privacy, non-repudiation, and hierarchical access control. Old models of IMD were accessible only by one person (physician). Today we also have nurses, therapists, programming technicians, paramedics, etc. therefore, user accountability must be added to the system. Finally, all this need to be done with the usual constraints of IMD. Perhaps because of this, some researchers try innovative approaches by studying and using concepts, such as multi-factor authentication by touch patterns in an implant under the skin or telecommunications signals strength ratio as function of distance, that allow enhancements in IMD security without significant computing and energy additional impact.

REFERENCES

[1] 'IoT in Healthcare 2021: IoT Medical Devices & Companies'. https://www.businessinsider.com/iot-healthcare (accessed Jan. 15,2021).

[2] A. Longras, H. Oliveira, and S. Paiva, 'Security Vulnerabilities on Implantable Medical Devices', *Iber. Conf. Inf. Syst. Technol. Cist.*, vol. 2020-June, no. June, pp. 24–27, 2020, doi: 10.23919/CISTI49556.2020.9141043.

[3] D. Zaldivar, L. A. Tawalbeh, and F. Muheidat, 'Investigating the Security Threats on Networked Medical Devices', *2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020*, pp. 488–493, 2020, doi: 10.1109/CCWC47524.2020.9031212.

[4] K. Lounis and M. Zulkernine, 'Attacks and Defenses in Short-Range Wireless Technologies for IoT', *IEEE Access*, vol. 8, pp. 88892–88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[5] Y. He, H. Soygazi, C. Luo, and H. Janicke, 'Security Defense Strategy for Intelligent Medical Diagnosis System (CMDS)', *Comput. Cardiol. (2010).*, vol. 2019-Septe, pp. 3454–3457, 2019, doi: 10.23919/CinC49843.2019.9005775.

[6] C. Easttom and N. Mei, 'Mitigating Implanted Medical Device Cybersecurity Risks', *2019 IEEE 10th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2019*, pp. 0145–0148, 2019, doi: 10.1109/UEMCON47517.2019.8992922.

[7] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, 'Minimum On-the-node Data Security for the Next-generation Miniaturized Wireless Biomedical Devices', *Midwest Symp. Circuits Syst.*, vol. 2020-Augus, pp. 1068–1071, 2020, doi: 10.1109/MWSCAS48704.2020.9184564.

[8] M. Darji and B. Trivedi, 'IMD-IDS a specification based Intrusion Detection system for Wireless IMDs', *Int. J. Appl. Inf. Syst.*, vol. 5, no. 6, pp. 19–23, 2013, doi: 10.5120/ijais13-450926.

[9] M. A. Siddiqi, C. Doerr, and C. Strydis, 'IMDfence: Architecting a Secure Protocol for Implantable Medical Devices', *IEEE Access*, vol. 8, pp. 147948–147964, 2020, doi: 10.1109/ACCESS.2020.3015686.

[10] T. Belkhouja, S. Sorour, and M. S. Hefeida, 'Role-based hierarchical medical data encryption for implantable medical devices', *2019 IEEE Glob. Commun. Conf. GLOBECOM 2019 - Proc.*, 2019, doi: 10.1109/GLOBECOM38437.2019.9014192.

[11] V. H. Tutari, B. Das, and D. R. Chowdhury, 'A continuous role-based authentication scheme and data transmission protocol for implantable medical devices', *2019 2nd Int. Conf. Adv. Comput. Commun. Paradig. ICACCP 2019*, 2019, doi: 10.1109/ICACCP.2019.8883012.

[12] C. Camara, P. Peris-Lopez, J. M. De Fuentes, and S. Marchal, 'Access Control for Implantable Medical Devices', *IEEE Trans. Emerg. Top. Comput.*, vol. 6750, no. c, pp. 1–13, 2020, doi: 10.1109/TETC.2020.2982461.

[13] S. Maji *et al.*, 'A low-power dual-factor authentication unit for secure implantable devices', *arXiv*, pp. 1–4, 2020.

[14] Z. Zhang, X. Xu, S. Han, Y. Liang, and C. Liu, 'Wearable Proxy Device-Assisted Authentication Request Filtering for Implantable Medical Devices', *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2020-May, 2020, doi: 10.1109/WCNC45663.2020.9120856.

ISBN: 978-989-54659-1-0