Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Cyberthreats on Implantable Medical Devices

Mohammed Nour A. Sabra*
Clinical Audit Department, King Fahad Medical City (KFMC), Riyadh, Saudi Arabia.

Received 25 Mar. 2021; Accepted 10 May. 2021; Available Online 01 Jun. 2021

Abstract

The significant and rapid technological development in the field of medical care, and Implanted Medical Device, clearly lead to improve the quality of care and effectiveness of treatment for numerous diseases that were previously difficult to be controlled. Technological growth has accompanied by a marked fear of academics and researchers during the past ten years from cyber threats that may lead to breaking the goal of creating these devices. Cyberspace risks and threats would expose many patients who use these devices to health complications and then endanger their lives. The risks and the vulnerability of these devices raised the curiosity to search and audit concerns that were purely theoretical and not associated with practical experience. The rapidity of change in the structure of the implanted medical device works as a barrier and reducing the possibility of their exposure to cyber threats. However, create comprehensive policy parallel with raising the awareness of the health care providers are the proactive steps to stop such threats and will be barriers from the cyber threats, therefore, no complete and comprehensive protection from cyberspace threats without ignoring that the Cyber threats will remain in places.

I. Introduction

Every aspect of modern life involves information technoloEvery aspect of modern life involves Information Technology and Computer Science (ITC) in such a way, it improves and increases the efficiency in medicine, education, industrial, transportation, entertainment, and more. Academic studies show interest in the cybersecurity of medical devices, particularly implanted medical devices. Some of them focused on insulin pumps [1], pacemakers [2], and brain stimulator device [3], or the medical field in general. The recommendation of the academic research was conflicting with the real number of vulnerabilities in real life. Absent of real threats that may affect and impact the implanted medical devices leads this paper to do more investigation and review in-depth research and paper that are study the medical device and cybersecurity to compare it with real-life—aiming to end with comprehensive and practical recommendations to protect the implanted medical device from the real threats and reducing the Reducing anxiety of the scientific community.

II. Background

Employing ITC science systems at the principal of the health care system already makes current knowledge accessible to patients, families,

Keywords: Implanted Medical Device, Cybersecurity, Medical Device, Health Care System.

Production and hosting by NAUSS

* Corresponding Author: Mohammed Nour A. Sabra
Email: msabra@kfmc.med.sa
doi: 10.26735/XVJR7905

and health care providers to reduce knowledge and experience challenges. New technology can assist the health care system in collecting more data about patient conditions, status, outcomes, and physician decisions to better and immediately support future health care planning decisions. Such medical devices are currently used, and we can find it in the market and are available for patients' treatment, such as the Deep brain stimulation (DBS) which used to deliver electrical impulses to treat a targeted some areas in the brain, and the configuration can be through the programmer or smart tablet, Insulin Pump devices System (IPD's) [4] used to treat Diabetes Mellitus (DM) patients, and it may be combined with Continuous glucose monitoring systems CGMS [1]. Heart devices (implanted cardiac devices ICD), helps to prevent any sudden heart attacks also to restore normal rhythms of the heart. Implantable heart devices interconnect wirelessly, using embedded computers and can sense an abnormal heart rhythm, provide a treatment shock in case of arrhythmias, and reports the events [5]. Finally, the Cochlear Implants (CI)[6], sophisticated technology that provides assistance aid to the person with a hearing loss.

The health care industry adopted new technology like wireless and networked medical devices, web-based applications, [7]. However, they also provide more opportunities for digital criminals to exploit the weakness for fun and profit. A good number of researchers that focus on cybersecurity and medical device, unfortunately, little of studies point to the real statistic of the attack on these devices and feasibility of putting effort with searching and focusing on offense[4].

III. Research Questions

In reality, a few vulnerabilities reported and not reaching to level of aggression or threats, especially for the IMD. The following question related to this issue raised:

1. Is the Scientific community express the real situation for IMD and related equipment against cyber threat, what is the difference between the theoretical IMD cyber-attacks and real cyber-attacks?
2. What are cybersecurity measures and governmental regulations not already in place for implanted portable medical devices or accessories that connected and how to improve it to maintain the CIA in patients' safety?
3. How much can extend the level of recognizing the healthcare professional the risks, vulnerability, and threat, that may impact the implanted medical devices and to improve the importance of reporting the threats?

IV. Literature

IMD are embedded systems inside the human body, inserted under the supervision of highly qualified medical staff [8]. When IMD has a wireless feature, IMD manufactories developed these functions so that health care staff and patients can get control, monitor devices data, and report the analysis wirelessly either by directly connecting via Bluetooth or connecting via the network [9]. Although there are advantages of the wireless connection of the IMDs, there is still an expanding risk of IMD function disabled by attackers [10]. Wireless access control features can permit attackers to manipulate IMD settings and entering values from beyond the immediate location of the patient. Successful attacks could lead to significant harm to patients, or disabled cybersecurity policy in the organization network and the devices connected that may be used in the home setting [11].

The healthcare infrastructure is part of critical infrastructure in any country, and it should be part of any national plan of the Critical Infrastructure Protection plan (CIP) [12]. Therefore, it is challenging to protect the healthcare ecosystem without a good acknowledge of what the vulnerabilities are. Stakeholders should understand the threat and risk of vulnerabilities, risks, and vulnerabilities that can affect the healthcare ecosystem. Also, they have to be aware of technical vulnerabilities including human factors [9].

The existing connection of the health care system to networks experienced some security concerns; from a cybersecurity point of view, the network connection exposed the whole system to cybersecurity vulnerabilities [13]. The healthcare area has many vulnerable related beliefs of tradi-

tional people that no one would have the motivation to attack hospital network or medical systems, and defensive measures are not necessary [14] Medical devices still are easily accessible to attackers, who can use any device to support a potential entry point to health care networks, bypassing the firewalls software and protection system as an example.

The health care system sometimes is targeted for financial or political gains. And we can classify this attack motivation into three primary types; thief wants to steal data, intellectual property, or password, the vandal who seek to destruct via DOS (Denial of Service) to stop the hospital service and soldier who goes think to control over any system. World wild, the health care system complains from threats and consequences of vulnerability, results in impact negatively on the quality of patient care. Hackers have been distribution "Ransomware called Wanna-Cry" (Wana-Crypt). The whole system will lock up the medical record and encrypts them in a way that the hospital cannot access [15]. However, hospitals and clinics have become an easy target to hackers.

Such research show interest in the confidentiality of information concerning the patient and it is a principle respected by health care professionals from ancient times [16] and allowed the strengthening of physician-patient relations. Literature focused on the health care system data that stored and transformed in digital form and it will be under risk, for example [14], Disrupting attacks to shut down health care systems, critical kit or tools, lab machine, changing configuration settings of devices (e.g., insulin infusion pumps), or rebooting life-saving devices such as ventilators. Loss the log of the medical information which is considering very serious for treating patients with severe illnesses and access to controlled laboratory devices.

Access control restriction needed in the health care system by encrypting data to prevent any leakage for medical information. Malfunctions of computer networks that can cause errors in diagnosis, risk of medical errors, or financial losses [13]. The importance of networking health care is communication to exchange data between healthcare applications, and this indicates to vulnerability inherited from IT integration. Such Attacks that may internal or external of an organization may be targeting communication networks. Other research focused on the cybersecurity in the medical device's system such as equipment, tools, implant, including a part or accessory [17] used in the identification of disease and patient's conditions.

Medical devices are unique because of its attributes such as regular evolves, sensitivity accuracy, lightweight, and security which could directly affect treatments, safety, and may lead to endangering of patient life [18]. The consequences of any vulnerabilities may be exploited and potentially high impact on patients' safety. The modern medical device contains personal information stored in the main memory, also operational data, such as the simulation settings, rate of battery drain, and biometric parameters. An attacker could utilize any of the above information to facilitate attacks relying on specific pathological states [4].

Med-jack (Medical Device Hijack) new concept exploit medical devices by injects malware into unprotected medical devices to create weak links in hospital security software defenses [18], including therapeutic kit (e.g., infusion pumps), diagnostic and monitoring equipment (e.g., MRI machines), and life support devices (e.g., ventilators). The typical examples for possible risks on Medical devices that result in an impact on the CIA include flawed software or defective in the design of firmware during composing the codes of the software, which is free of protection measures.

Accessing by unauthorized persons of a medical device could lead to full control by the hacker [3]. Identify critical vulnerabilities that may face the medical device, especially when it comes to the cybersecurity side include accessing to internet through mechanisms that connected to medical networks internally or externally by default password of admin [13].

Many articles described the importance of cybersecurity in the implanted medical device's which adapted the "Nano-medicine" that minimizing the size to be small, which could meet body requirements and measuring body vital signs. Also, performing accurate analyses by Wireless Sensor Network (WSN). IMD can realize long-distance signal

transmission that facilitates health care providers to follow up patients' health conditions remotely [7]. An innovative embedded system and lightweight technical solution support connectivity, productive performance with the efficient cost of components.

Newly, the concept referred to the illegal command of an electronic brain implant [19]. With the widespread adoption of DBS technology comes a more significant opportunity for high technical competence, hackers to use the new technology for malicious purposes. Some of the scientists have demonstrated the potential for exploitation of the security constraints of implantable medical devices with possibly severe consequences. There are several options for brain jacking, such as altering the stimulation parameters such amount of the voltage, frequency, pulse width, current, and electrode contact [13].

Some studies focusing on battery consumption of IMD. Any repeated attacks on the system can reduce the battery prematurely, this type of implanted device is non-rechargeable, and this will result in decreased device lifetime [13].

Radcliffe is a researcher in the cybersecurity. He is one of the DM patients; he has proved his capability of hacking and accesses his insulin pump [20]. Such attacks on medical devices are expecting to be very rare, but theoretical, it is a possibility and could not ignore. June 28, 2019, The (U.S. Food and Drug Association) FDA has recalled several Medtronic insulin pumps, because there is a risk of them to hacked [21]. This incidence highlighted the vulnerable that many medical devices are exposing to cyber-attacks.

Vulnerability in CIEDs would be possible for a hacker if he operates his attacks in the same radiofrequency that used by CIEDs so that he can disturb the CIED RF. Disturbing the CIED would inhibit the value of monitoring and allow the loss of reading of the events that go to be undetected by the system. In a pacing-dependent mode, the patient's heart is dependent on the pacemaker, overseeing may inhibit pacing so the heart muscle will suddenly stop or may result in inappropriate pacing and even life-threatening shocks [6].

October of 2018, the FDA released a safety communication regarding potential vulnerabilities in the Care Link from Medtronic devices for (CIED). The programmers allow the health care providers to check battery status, obtain device performance information, and adjust settings from a CIED. An exterior researcher was able to identify a technique that allowed an unauthorized hacker to manipulate the programmer's settings during remoting installing a software update [22].

V. Methodology

The argument designed to follow the exploratory facts or information that already available in the digital library, international database and analyze these findings to make a critical evaluation of the current status of the implanted medical device and accessories related to cyber threats. The investigation of the previous researches supports developing policy and raising the awareness level for healthcare providers. We explored studies and papers from reliable sources and global databases that are the basis for all companies and sectors interested in cyber research. Highly selective for the survey research that adequately interested in the health sector and the systems used in the health field. Some excluded from the thesis plan that is older than ten years since health care is considered to be long-term modernization and renewal in the field of medical devices. Secondly, studies related to medical files or the documentation process were also excluded to reduce distribution out of the scope.

VI. Findings and Discussion

By identification 160 records from multi-resource[1]. Literature shows many of the suggested vulnerability. Those vulnerabilities compared to real threats status in the international[2] . The researches from 2010 till 2019, excluded related to Medical device newly concept and annually the manufactory's released versions of the tools, NVD database

[1] National Center for Biotechnology Information advances science (NCBI), Research Gate, ProQuest Library database, King Fahad Medical City Digital Library database, King Saud University Digital Library Database. (KSU), Naïf Arab University for Security Sciences Digital Library (NAUSS), IEEE Explore Digital Library and ELSEVIER Database.

[2] the National Vulnerability Database NVD from NIST8, Recalls of Medical Devices database from FDA

has poor documentation before 2010, Update for new treatment and devices every short period, and Most of the vulnerability came from the health care system (such hospital network and other medical facility or user, not from the medical device itself.)

History of IMD shows that IMD was continuously evolving, even in its basic structure as we see in the market, many kinds and types every day released to market that gives many choices for the health care providers. Every IMD model has different specifications, and some time has a different operating system which is ignored by the literature. The health care system and patient needs are continually developing and keep changing over time to achieve the wishes of health care requirements and human needs. IMD is improving and growing in security structures, where many of manufactory adopt the cyber-security protection models[23]. Every year the manufactories released many new versions and new devices, where this variation the models and versions are working as a robust shield for protecting the IMD from the attackers or any cyber threats or even manufacturing vulnerability even with an internet connection. It will be hard to identify and track all the versions of product vulnerabilities, and that leads to being tough for someone to consume time and effort for such attacks with a very low probability of success as we see in the NVD [23] reports database.

First, the human is dynamic living, unstoppable, and IMDs such attached devices will be continuously moving from one location to another according to the location of the patients, and this finding is considered one of a substantial obstacle for many kinds of cyber threats. The distance that created between the patient who hold the device and suspected attackers or the cyber threats considered a safe zone from any threats or at list decreases the probability of threats; with little assistance from the manufactory who provide some instruction card to instruct the patient and his family regarding the device used on how to use, distance, also security options.

The reviewed literature recognized that security issue in the device software is not usually present on medical devices related to first the power consumption that needed by an encryption process in case of need to protect the IMD by the encrypted process, some of the recommendations in the literature suggest the Advanced Encryption System (AES) system and offer a study of the feasibility of use. However, in reality, the smallness of the operating system, size, and maintaining battery consumption with the limit as required are challenges for manufactory and costing, on the other hand, a few reporting for vulnerability and the threat that may impact the IMD still challenging to convince the manufactories to focus on the cybersecurity concerns specialty in a low rate of reporting the incidence of events.

IMD's are devices systems needed by manufacturer application intervention for adjustments or reconfigurations. The manufacturers are responsible for technical problems, maintenance, and supporting security concerns—some time the IMD from the health care provider to have control over the devices. So, with appreciate awareness and educate the staff will support proactive security to protect the IMD.

All of the IMDs subjected to stringent laws such as FDA and European EMA, as a consequence, any IMDs have to pass the verification and examination process, including the penetrating test which it has done in the lab or registered international laboratories to maintain CIA concepts and kept out of security breaches.

However, manufacturers are working to withdraw any model that has any inappropriate behaviors for patient's use, as we see in the recall communication from FDA. FDA database contains Medical Device Recalls classified since November 2002 also includes correction or removal actions initiated by the FDA. Any violation in the medical device, the work is recalled communication and classification may occur after the secure recalling.

Also, the medical device product conducts and communicates with its patients or health care facility about the recall. As we mention in the previous point, we found that the number of recalls is low, and for some of IMD is not presents and absents at all, Recall percentage for insulin pump from 2011 to 2019 was 8 (total) out of 83138 total insulin pump (FDA recall Database), And the vulnerability that found solved by the recall process for removal or

correction. Pacemaker Recall statistics from 2011 till 2019, the total Recall for pacemaker 2013 to 2019 was 12 out of 73700 total Pacemaker devices (FDA recall Database). Another device that under our focus, we did not find any recall for it or any vulnerability report. The analysis from the low number recalling report in the FDA database has two probability:

4. There are no reports received from the health care provider, patients, or users, and this helps us to circulate awareness models of cyber dangers that threatening IMD and it needs to create an educational and awareness session for IMD.
5. There are no vulnerability reports from the manufacturing company and hiding the fact related competition issue, and this supports the effort to create a policy that forced the manufacturer to disclose all the results obtained during the manufacturing life cycle period.
6. The results are real and that fears of security breaches on IMDs is very few and enough to alert the stakeholder to improve the awareness and creat police as proactive steps to protect the devices.

The major recall reason as per FDA related to software failure, may this one of the warning indicators draw the research community's attention. Software weaknesses can come in forms of flaws and bugs, so attackers have the opportunity to use these weaknesses to access the devices.

Literature has found that use of IMD frequently ignore security warnings, especially if the security warnings are frequent or difficulty in the user interface. Moreover, this is very important in ensuring IMD safety and security involves the user contributing to their safety and security.

Cybersecurity needs to deploy the pool of tools, security perceptions, policies, procedures, guidelines, security precautions, risk controlling approaches, best practices training, assurance, and technologies that can be used to protect and secure the data within the cyber environment to achieve the desired outcome for ensuring the organization and user's assets safety.

However, in the information security field, the human factor considered the most vulnerable agent that unpredictable and element characterizing as challenging to be controlled. Therefore, patients and health care providers should have an adequate level of cybersecurity awareness on implanted medical devices and how to protect themselves against the increased cyber threats. Technical solutions alone cannot provide comprehensive protection.

VII. Conclusion and Recommendation

Any attack has constrained, and limitation; whatever the preparation or hacker experience, to answer this assumption, we have to explore such constrains that are create restriction boundary on such attacks, for example, Physical range constraints were most of IMD with wireless technology has limited capabilities that can communicate with device programmers or terminal over less than 1-meter. So, the assumption that adversaries need to be within a few meters' distances from the targeted IMD to be able to capture or transmit messages is very challenging, particularly moving patients to multi-locations such as a hospital or home. All of IMD comes with a close system that configured only by the company, which is another constraint to the advertiser to capture the information on the operating system, which makes it hard to prepare for such attacks. Healthcare providers have to fulfill the pre-marketing Essential Principle that requires the manufacturer to minimize the cyber threat and risks related to IMD using. Also, the sponsor of the medical device must demonstrate compliance with the Essential Principles. The health care provider has to knowledge that dealing with IMD that does not fulfill with the Essential Principles may have enforcement of penalties.

References

[1] G. Cocha, et al. "Intelligent insulin pump design," in *2018 Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación (CACIDI)*, Buenos Aires, 2018, pp. 1-4, doi: 10.1109/CACIDI.2018.8584364.

[2] E. Marin, et al. "On the (in)security of the latest gener-

ation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl. (ACSAC '16)*, New York, USA, pp. 226-236, doi: 10.1145/2991079.2991094.

[3] J. Pugh, L. Pycroft, A. Sandberg, T. Aziz and J. Savulescu, "Brainjacking in deep brain stimulation and autonomy," *Ethics Inf. Technol.*, vol. 20, no. 3, pp. 219-232, July 30, 2018, doi: 10.1007/s10676-018-9466-4.

[4] J. Finkle, "J&J warns diabetic patients: Insulin pump vulnerable to hacking," Oct. 4, 2016. [Online]. Available: https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

[5] A. Baranchuk, *et al.* "Cybersecurity for cardiac implantable electronic devices: what should you know?," *J. Am. Coll. Cardiol.*, vol. 71, no. 11, pp. 1284-1288, Mar. 20, 2018, doi: 10.1016/j.jacc.2018.01.023.

[6] W. F. House, "Cochlear implants," *Ann. Otol. Rhinol. Laryngol.*, vol. 85, no. 3_suppl, pp. 3-3, May 1, 1976, doi: 10.1177/00034894760850S303.

[7] D. Arney, K. K. Venkatasubramanian, O. Sokolsky and I. Lee, "Biomedical devices and systems security," in *2011 Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Boston, MA, 2011, pp. 2376-2379, doi: 10.1109/IEMBS.2011.6090663.

[8] S. Aram, R. A. Shirvani, E. G. Pasero and M. F. Chouikha, "Implantable Medical Devices; Networking Security Survey," *J. Internet Serv. Inf. Secur. (JISIS)*, vol. 6, no. 3, pp. 40-60, Aug. 2016, doi: 10.22667/JISIS.2016.08.31.040.

[9] L. Pycroft and T. Z. Aziz, "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks," *Expert Rev. Med. Devices*, vol. 15, no. 6, Jun 13, 2018, doi: 10.1080/17434440.2018.1483235.

[10] Y. A. Bangash, Q. Abid, A. A. Ali and Y. E. A. Al-Salhi, "Security issues and challenges in wireless sensor networks: a survey," *IAENG Int. J. Comput. Sci.*, vol. 44, no.2, pp135-149, 2017.

[11] A. Saklecha, "Will doctors finally accept technology? Yes. Here's how," Feb. 20, 2014. [Online]. Available: https://techonomy.com/2014/02/will-doctors-finally-accept-technology-yes-heres/

[12] MDISS, "Cyber Vulnerabilities and Risks in the Healthcare Ecosystem," 2017. [Online]. Available: https://www.mdiss.org/

[13] C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technol. Health Care*, vol. 25, no. 1, pp. 1-10, Feb. 21, 2017, doi: 10.3233/THC-161263.

[14] S. G. Langer, "Cyber-Security issues in healthcare information technology," *J. Digit. Imaging*, vol. 30, no. 1, pp. 117-125, Feb. 2017, doi: 10.1007/s10278-016-9913-x.

[15] C. Graham, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history," May 20, 2017. [Online]. Available: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

[16] D. Sabău-Popa, I. Bradea, M. Boloș and C. Delcea, "The information confidentiality and cyber security in medical institutions," *Ann. Univ. Oradea Econ. Sci.*, vol. Tom XXIV-2015, no. 1, pp. 855-860, July 2015.

[17] P. A. Williams and A. J Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Med. Devices (Auckl)*, vol. 8, pp. 305-316, Jul. 2015, doi: 10.2147/MDER.S50048.

[18] A. J. Burns, M. E. Johnson, and P. Honeyman, "A brief chronology of medical device security," *Commun. ACM*, vol. 5, no. 10, pp. 66–72, Oct. 2016, doi: 10.1145/2890488.

[19] C. Li, A. Raghunathan and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th Int. Conf. e-Health Netw., Appl. Serv.*, Columbia, MO, 2011, pp. 150-156. doi: 10.1109/HEALTH.2011.6026732.

[20] L. Pycroft, et al. "Brainjacking: Implant Security Issues in Invasive Neuromodulation," *World Neurosurg.*, vol. 92, pp. 454-462, Aug. 2016, doi: 10.1016/j.wneu.2016.05.010.

[21] FDA Safety Communication, Potential Cybersecurity Risks, 2019, USA.

[22] B. Alexander, S. Haseeb and A. Baranchuk, "Are implanted electronic devices hackable?," *Ternds Cardiovasc. Med.*, vol. 29, no. 8, pp. 476-480, Nov. 2019, doi: 10.1016/j.tcm.2018.11.011.

[23] https://nvd.nist.gov/