International Journal on Cybernetics & Informatics (IJCI) Vol.13, No.2, April 2024

Exploring Vulnerabilities and Attack Vectors Targeting Pacemaker Devices in Healthcare

Brad Chardenet[1], Jaycen Jamssens[1], Richard Cummins[1], and Tauheed Khan Mohd [1]

School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, United States

Abstract. This technical paper investigates the vulnerabilities and potential threats posed by emerging technologies, specifically Bluetooth-enabled patient pacemakers. With the advancements in healthcare technology, pacemakers now utilize Bluetooth connectivity for real-time monitoring and data transmission, offering patients and healthcare providers an important convenience. However, this technology also introduces significant security risks, leaving these life-sustaining devices susceptible to malicious attacks.

Through an in-depth analysis of existing research, real-life incidents, and vulnerabilities identified by experts in the field, this paper will underscore the critical vulnerabilities present in pacemaker systems. Examples, including findings from researchers such as Billy Rios, Jonathon Butts, and Marie Moe, demonstrate the potential severity of these vulnerabilities. From remote control manipulation to unauthorized access to sensitive medical data, the threats posed by these vulnerabilities are substantial and potentially life-threatening.

Moreover, this paper outlines advanced mitigation strategies essential for protecting patient pacemakers against these security risks. Recommendations include end-to-end encryption, whitelist device pairing, intrusion detection systems, and regular firmware updates, highlight the collaborative efforts required from patients, healthcare providers, and manufacturers to mitigate these risks effectively.

This paper's findings underscore the urgent need for robust cybersecurity measures in the design, implementation, and maintenance of pacemaker systems. Addressing these vulnerabilities is key for ensuring patient safety, maintaining privacy, and building trust in healthcare technology. The implications of this research extend beyond pacemaker security, emphasizing the broader importance of cybersecurity in medical devices and the importance of ongoing research and regulatory initiatives to protect patient health.

Keywords: Attack Vectors · Pacemaker · Healthcare

1 Introduction

This paper is about "The vulnerabilities and attacks on patient pacemakers". With today's technology, it is possible for people with pacemakers to see the

Bibhu Dash et al: NLPAI, IOTBC, CITE -2024
pp. 161-173, 2024. IJCI – 2024

DOI:10.5121/ijci.2024.130212

data regarding their heart health with Bluetooth. However, this can leave vulnerabilities to attackers. Bluetooth can be easily hacked, and data stolen from the patient without them knowing. Even worse attackers can hack the pacemaker to cause harm or even death to the patient. There are many ways an attacker can do this. They can insert malware into the patient's pacemaker to access files and erase the contents of the monitor memory of the patient's heart. They can also inject code into the pacemaker to shorten the pacemaker's battery life which can be life-threatening if the pacemaker is not operational with the patient knowing. [1]

Throughout this paper these aforementioned vulnerabilities will be discussed and dissected in great detail. Emphasis the risk of what could happen if a pacemaker were ever to be attacked individually or in mass. The solutions to mitigate and reduce the risks will also be outlined in detail as well to show where the opportunities for the manufacturers, doctors, and patients have the ability to take preventative measures to ensure the health and safety of those who wear these pacemakers to survive. Preventive measures like ease of access for security updates, ensuring the patient health readings are on a separation of patient data onto its own network to monitor traffic flow, developing a disaster plan if a breach were ever to occur through the pacemaker, and investing heavily in cybersecurity systems can help mitigate the overall risk for the patient's data and their health. Prior to going into further details about the risks involved and finding some solutions, a brief overview of the purpose of pacemakers and their functions will be discussed in the following section.[2]

Patient pacemakers have been developed to offer users useful information about their heart health via Bluetooth communication as technology advances. How- ever, this convenience has a unique set of weaknesses that could be used by bad actors to their advantage. We examine the pacemaker vulnerabilities and potential attacks in further detail through our research, highlighting the potential dangers that patients may not be aware of.

In recent years, pacemakers have increasingly used Bluetooth technology as a standard method of communicating critical health information to healthcare professionals. While this development makes pacemakers more convenient and allows for real-time monitoring, it puts them at risk for security lapses as well. With flaws like these that could be exploited by attackers with malicious intentions, allowing for disastrous results for the patients that use them.

Through our thorough investigation, we'll go over the flaws as well as the different ways that attackers can undermine the security of patient pacemakers. These will include the possibility to access pri- vate medical information without authorization, introducing malicious code to interfere with device operations, and potentially physically harming patients by interfering with pacemaker functionality. Our goal is to increase awareness of the seriousness of these vulnerabilities and how they could potentially affect patient safety.

In order to protect against these risks, we will also suggest mitigation methods and preventive measures that manufacturers, healthcare providers, government agencies such as the Food and Drug Administration, and patients can all use. We will go into more technical depth, share insights from related research, and suggest methods to effectively minimize these risks in the sections that follow. By the time this paper is finished, we expect to have emphasized the significance of cybersecurity in the context of patient pacemakers and equipped stakeholders to take proactive measures to ensure patient security and welfare. [3].

1.1 *What is a Pacemaker?*

The purpose of a pacemaker is to help treat individuals with cardiac issues such as arrhythmia or a weak heart. An arrhythmia is an issue where a heart is not beating at a normal pace (either slower or faster), or a heart that beats at an erratic rhythm. The purpose of the pacemaker once implanted through an outpatient surgery, is to send electrical pulses to the patient's heart in order to correct the rhythm it beats to correct it to a normal rhythm.

There are a few types of pacemakers that can be implanted within a patient, which all serve the same purpose. There are Transvenous, Wireless, and Surface. The former two types are the pacemakers that require surgery to be placed within the body, and the surface is placed over the body. They all serve the same function, and all have similar vulnerabilities. [2][4]

Pacemakers work through a few basic functions; these functions are extremely important for pacemakers to work properly and to ensure the patient's health. Pacemakers are comprised of a battery for power, a computerized generator for operations of the system, and sensors connected to wires that are called electrodes. All these pieces work together to monitor and transmit data which allows them to function properly and correct the rhythms of the patient's heart. Other functions of pacemakers can include the monitoring of breathing, blood temperatures, and can even adjust the heart rate based on the activity of the patient's activities.

All of this data from the use of the pacemaker is stored by the device and with the newer technology today can be transmitted right to the doctor for them to monitor. This transmission is typically done with Bluetooth technology, which as mentioned above, can be ripe with vulnerabilities. To ensure the safety, security and privacy of patient's and healthcare professionals, these vulnerabilities must be discussed along with risk mitigation measures.[5]

2 Related Work

The vulnerabilities that are inherent in Bluetooth-enabled patient pacemakers have escalated into a cause of massive and life-threatening concern within both the cybersecurity and medical fields. The evolving landscape of this type of technology has witnessed several notable incidents that underscore the severity and the potential risks associated with Bluetooth technology. Given the importance of patient health and safety, the emerging issues have caught significant attention from researchers, governmental agencies, healthcare providers, and other stakeholders.

There have been several alarming incidents related to Bluetooth technology that have come to the surface, which illuminate the vulnerabilities that are embedded within medical devices, particularly Bluetooth pacemakers. These incidents serve as stark reminders of any potential threat posed by malicious exploitation of Bluetooth connections that are in life-sustaining devices. These incidents have triggered a heightened sense of urgency within the medical and cybersecurity communities, which has emphasized the need for immediate action to address these vulnerabilities.

In response to these escalating concerns, researchers, governmental bodies, and regulatory agencies such as the Food and Drug Administration have been quick to acknowledge and address the vulnerabilities that are prevalent in Bluetooth-enabled pacemakers. Their concerted efforts have prioritized patient safety and their well-being. This proactive stance has led to a series of comprehensive studies and experiments aimed at identifying, analyzing, and mitigating these vulnerabilities.

As a direct response to some of the identified vulnerabilities, there have been recalls and warnings that have been issued to patients equipped with susceptible Bluetooth-enabled pacemakers. These measures, that were taken by regulatory bodies and healthcare institutions, have emphasized the importance of addressing the identified risks promptly. Such actions are pivotal in alerting patients to potential threats and ensuring necessary precautions have been taken to safeguard their health and well-being.

2.1 *Marie Moe's Pacemaker Hacking Project:*

Marie Moe created a compelling initiative, the Pacemaker Hacking Project, which was created in 2015, stemming from her genuine concerns surrounding the possibility of security vulnerabilities of her implanted Bortnick Cardiomessenger II model. Her groundbreaking study was a pioneering effort focused on a detailed analysis of the security capabilities inherent in her implanted medical device.

The purpose of Marie Moe's endeavor was driven by a determination to scrutinize and comprehend the security measures that were embedded within the Bortnick Cardiomessenger II pacemaker device. The project sought to delve deeper into the intricacies of the device's security infrastructure, aiming to evaluate its strength and to try to identify potential weaknesses or vulnerabilities that could compromise patient safety.

Through Marie Moe's exhaustive research and analysis, it was discovered that there were alarming security flaws within the Cardiomessenger II model that were brought to light. Her detailed investigation revealed a trio of critical vulnerabilities:

Improper Authentication: The study uncovered a weakness in the authentication mechanisms of the Cardiomessenger II device. This type of vulnerabilities could potentially allow unauthorized access to the pacemaker's functionalities, this discovery raised alarming concerns about the device's susceptibility to malicious manipulation.

Unencrypted Storage of Medical Data: Marie Moe's research highlighted the dangerous practice of storing sensitive patient medical data without a strong encryption measure in place. This was a significant security lapse that rendered patient information vulnerable to interception and exploitation, posing risks to patient privacy and confidentiality.

Credential Reuse: Another worrying discovery was the negligent practice of credential reuse within the Cardiomessenger II model. The oversight posed a significant threat, that could potentially enable unauthorized parties to exploit reused credentials to gain access to critical systems, which again would compromise patient safety and data integrity.

2.2 *Research by Billy Rios and Jonathon Butts:*

A couple security experts from WhiteScope and QED Secure Solutions, Billy Rios, and Jonathon Butts, conducted an expansive examination of Medtronic's pacemaker infrastructure. Their meticulousness in their research unearthed critical vulnerabilities embedded within these medical devices, which triggered serious concerns within the medical and cybersecurity realms.

Billy Rios and Jonathon Butts started an extensive investigation focusing on dissecting the architecture of Medtronic's brand pacemakers. Their analysis took a deep dive aiming to uncover potential weaknesses or loopholes within the Bluetooth pacemaker's infrastructure that could potentially compromise the security and integrity of these life-sustaining devices.

Significant Vulnerabilities Uncovered: Their research findings revealed a number of vulnerabilities within Medtronic's Bluetooth pacemaker infrastructure that could be a cause for alarm. The vulnerabilities in question posed substantial risks, as they could potentially grant malicious parties' remote access and control over pacemaker functions. The identified vulnerabilities were of particular concern due to their potential to:

1. **Enable Remote Access:** One of the vulnerabilities discovered by Rios and Butts was which had the capability to enable unauthorized remote access to the pacemaker systems. This was a troubling prospect that raised serious concerns, as it could allow external parties to gain access and manipulate crucial pacemaker functions from a distance.
2. **Pose Life-Threatening Risks:** The critical nature of the vulnerabilities uncovered was highlighted by the potential life-threatening risks posed to patients. The ability for attackers to gain control over pacemaker functionalities raised alarming concerns about the impact on patient safety and well-being.

2.3 *FDA Recall and Vulnerability Discovery (2017):*

In an important move, the Food and Drug Administration in 2017 identified a massive vulnerability within a Bluetooth pacemaker system. This was an alarming revelation that had emerged as the Food and Drug Administration uncovered over 500,000 pacemakers that were vulnerable to potential cyber-attacks.

The severity of this discovery prompted an important and unprecedented action within the medical community.

The gravity of the situation propelled the Food and Drug Administration to start a voluntary recall of the vulnerable Bluetooth pacemakers. This recall, unseen in this scale, underscored the imminent threats posed by vulnerabilities in Bluetooth-enabled implantable medical devices. The recall highlighted the urgent need for heightened vigilance and enhanced security measures to protect patient safety.

2.4 *FDA's Action and Collaborative Initiatives (2018):*

Subsequent to the vulnerability discoveries, the Food and Drug Administration took a very proactive approach in addressing these critical issues. With the formation of the CyberMed Analysis board in 2018, this board exemplified the Food and Drug Administration's commitment to strengthening cybersecurity measures within the medical fields. The strategic move aimed to provide comprehensive guidance not only to manufacturers but also to medical facilities and regulatory bodies. With the vision of creating a collective effort that would help elevate the security standards of Bluetooth-enabled pacemakers.

2.5 *Advancements in Mitigation Strategies (MIT Research)*

MIT's Innovative Approach: MIT's continued research has been a key factor in pioneering innovative solutions to mitigate potential threats targeting patients' Bluetooth pacemakers. Through the development of external encryption devices signifies a groundbreaking approach to strengthen security measures. These cutting-edge devices, equipped with advanced encryption and authentication features. This acts as a strong shield against unauthorized access by malicious parties that seek to exploit any vulnerabilities in Bluetooth-enabled pacemakers.

Safeguarding Patient Well-being: The emergence of these external encryption devices represents an important step in safeguarding the well-being of patients reliant on Bluetooth-enabled pacemakers. MIT's groundbreaking research highlights the critical role of advanced encryption technologies in stopping potential attackers from carrying out malicious activities. This helps ensure patient safety and bolsters the security resilience of Bluetooth-enabled medical devices.

3 Research/Findings

Pacemakers' vulnerability to hacking started to raise significant concerns within the medical community over the years. Back in 2017, the Food and Drug Administration discovered something very disturbing, there are more than 500,000 pacemakers susceptible to potential cyber-attacks. Consequently, the Food and

Drug Administration issued a voluntary recall for individuals equipped with these vulnerable pacemakers to prevent potential security breaches.

Researchers Billy Rios and Jonathon Butts from the security firms WhiteScope and QED Secure Solutions played a pivotal role in uncovering a series of vulnerabilities within the Medtronic brand of pacemakers. During their testing and investigating, they identified vulnerabilities within Medtronic's infrastructure that could allow an attacker to penetrate the pacemaker system thereby allowing an attacker to install malicious software, which would allow them to gain remote control over the device. This unauthorized access could lead to life-threatening situations, enabling attackers to administer unnecessary shocks to a patient's heart—a harmful and potentially fatal scenario.

Marie Moe, who is another significant figure in the realm of pacemaker security, had a Bortnick Cardiomessenger II model surgically implanted in her. Marie was driven by curiosity about the security measures in place, so she started the Pacemaker Hacking Project in 2015. Marie's main goal for her project was to scrutinize the security capabilities of the device implanted within her. In July 2020, Marie unveiled her findings, she highlighted five major security vulnerabilities they were improper authentication, transmission of credentials in clear text before encryption, credential reuse, unencrypted storage of medical data, and incorrect storage procedures on the device.

To address these critical security flaws, the Food and Drug Administration took action in 2018 by coming up with and introducing a comprehensive plan of action. The plan encompassed the development of a new medical safety device and started the creation and the establishment of a CyberMed Analysis board, which is a collaborative platform involving public-private partnerships. This board was envisioned to offer resources and guidance to device manufacturers, medical facilities, and the Food and Drug Administration itself.

The Food and Drug Administration recognized the urgency of enhancing cybersecurity measures for medical devices, they have committed to implementing more robust practices and safety measures. Plans are underway to fortify the system for identifying threats to pacemakers and formulating effective strategies to mitigate these risks as they arise.

There have been further advancements in this domain, they have emerged from researchers at MIT, who are actively working on an external encryption device designed to prevent potential attackers. This device's innovation, intended to be worn around the neck or wrist, is equipped with advanced encryption and authentication features. The goal is to disrupt nearby transmissions operating at the same frequency as the pacemaker, which would effectively shield the medical device from unauthorized access and potential harm to the patient.

3.1 *Bluetooth Vulnerabilities in Pacemakers: An In-Depth Look*

Through the integration of Bluetooth technology medical devices have undeniably enhanced their capabilities, this is particularly prevalent in devices like pacemakers. However, this technological advancement has concurrently created a series of significant security concerns for pacemakers. One of the most critical vulnerabilities lies in the unsecured cryptographic key exchange process that is inherent in Bluetooth pairing. This vulnerability exposes pacemaker devices to potential interception, posing a severe threat to their security.[6]

Compounding this issue is the inconsistency among encryption standards used on Bluetooth devices, this heightens the risk of an attacker deciphering transmitted data, thereby compromising the confidentiality of sensitive information.[7] Furthermore, vulnerabilities like the BlueBorne attack vector can pose a grave threat to pacemaker functionality. These vulnerabilities can empower attackers to seize control of a device or disseminate malware, all without requiring any user intervention.[6][8]

Expanding on the security risks associated with Bluetooth technology in medical devices such as pacemakers, it's imperative to delve deeper into the potential consequences of these vulnerabilities. Notably, the susceptibility to interception during key exchanges. This not only compromises the privacy of patient data but also jeopardizes the integrity of vital patient medical information. The varied encryption standards further exacerbate this situation, creating a series of potential entry points for attackers or malicious parties to exploit. The threat posed by the BlueBorne attack vector opens up the frightening possibility of not just pacemaker compromises but also this manipulation could directly impact a patient's well-being.

3.2 *Securing Pacemakers: Advanced Strategies for Mitigating Bluetooth Vulnerabilities*

Enhancing the security measures against Bluetooth vulnerabilities in pacemakers necessitates a comprehensive and secure approach. Robust techniques are essential to counter data interception and tampering, mandating the implementation of end-to-end encryption within communication protocols.[9] Using augmentations to security further involves adopting a whitelist methodology for device pairing. This will effectively restrict connections solely to pre-approved devices, which will fortify the systems against unauthorized access.[10]

Furthermore, using proactive measures entail the incorporation of an intrusion detection system and regular firmware updates in order to promptly address emergent vulnerabilities and monitor for any irregular activities.[11][12] This multifaceted approach will serve as a critical defense mechanism to safeguard pacemaker systems from potential threats and ensure ongoing security resilience.

However, the effectiveness of these risk mitigation strategies heavily relies on the collaborative efforts of patients, healthcare providers, and pacemaker manufacturers. It is imperative for healthcare providers to remain vigilant and promptly identify any suspicious activities or attacks. Manufacturers bear the responsibility of communicating to the patients about potential risks associated with their devices. The collective awareness and communication among these stakeholders will play a pivotal role in ensuring heightened security levels.[13]

Furthermore, fostering a culture of shared threat intelligence within the healthcare industry is a key factor at play for this to work. Healthcare providers must collaborate to exchange information on threats, which will enable the acquisition and application of contemporary security methodologies across the board. This cooperative approach empowers the healthcare industry to adapt and counteract evolving security threats effectively.

4 Results

Our investigation into the vulnerabilities associated with patient's Bluetooth pacemakers unveiled critical results, which emphasized the urgent need for a comprehensive and robust cybersecurity measures that will ensure patient safety and healthcare trust.

4.1 *Identification of Vulnerabilities:*

Through our extensive research and analysis, various vulnerabilities within Bluetooth pacemaker systems were identified. These vulnerabilities encompassed very significant issues such as unauthorized access, improper authentication protocols, and the unencrypted storage of sensitive patient medical data. Most notably, research by cybersecurity experts, including the likes of Billy Rios, Jonathon Butts, and Marie Moe, has played a pivotal role in uncovering some of these vulnerabilities. Their conducted studies have highlighted weaknesses within pacemaker infrastructure, showcasing the potential risks associated with these vulnerabilities.

4.2 *Severity and Impact of Vulnerabilities:*

The vulnerabilities that we identified posed severe threats to patient safety and healthcare infrastructure. These vulnerabilities, if potentially exploited, could result in life-threatening scenarios. These could include remote control manipulation of pacemaker functions, which could lead to the death of the patient and unauthorized access to sensitive patient medical information or records. The severity of these potential consequences has underscored that there is a critical need for immediate action to address these vulnerabilities and any prevent potential harm to patients that rely on Bluetooth pacemakers.

4.3 *Real-world Examples and Demonstrations:*

Researchers have conducted real-world demonstrations that have vividly showcased the potential risks that are posed by these vulnerabilities. Several experiments illustrated how attackers could remotely access and manipulate Bluetooth pacemaker functions, demonstrating the alarming consequences of potential cyber-attacks. Marie Moe's Pacemaker Hacking Project highlighted five major security vulnerabilities in her implanted device, emphasizing the stark reality of these vulnerabilities and their potential for exploitation.

4.4 *FDA's Response and Mitigation Efforts:*

The Food and Drug Administration responded swiftly to the identified vulnerabilities by issuing recalls for susceptible Bluetooth pacemakers. The Food and Drug Administration also devised comprehensive plans to help mitigate these potential risks. Several of their initiatives included the establishment of the CyberMed Analysis board, which fosters a collaboration between stakeholders to enhance cybersecurity measures for these medical devices. This proactive approach demonstrated regulatory efforts to address vulnerabilities and ensure patients are safe.

4.5 *Technological Advancements and Solutions:*

Through technological advancements, such as MIT's development of several external encryption devices. We showcased promising solutions to mitigate risks associated with vulnerable Bluetooth pacemakers. These different innovations have aimed to safeguard Bluetooth pacemakers from potential attacks by using methods of advanced encryption and authentication features. This emphasized the crucial role that of how other technology can enhance the Bluetooth pacemaker's security

4.6 *Importance of Collaborative Efforts:*

Collaborative efforts amongst manufacturers, healthcare providers, regulatory bodies, and cybersecurity experts have emerged. With this collaboration effort critical factors in addressing vulnerabilities have started to take place, yielding promising results. These collective efforts between the different groups are aimed at implementing robust cybersecurity measures, sharing threat intelligence, and started to foster a culture of proactive risk mitigation, for the health of the patient. The significance of this type of collaboration was evident in the multifaceted approach to tackling vulnerabilities and ensuring patient safety and trust of medical providers, as well as manufacturers of these Bluetooth medical devices.

4.7 *Implications for Patient Safety and Healthcare Trust:*

The overall implications of vulnerabilities in Bluetooth pacemaker systems extended beyond each individual device security, it was also encompassing broader implications for patient safety and healthcare trust. The importance of which is invaluable, due to the lifesaving nature of the Bluetooth pacemaker devices. By addressing these vulnerabilities, it was shown that it was crucial not only for ensuring patient well-being but also for fostering trust in healthcare technology. Ongoing research initiatives and collaborative efforts and endeavors remain an essential part in maintaining patient safety and bolstering trust in the world's healthcare systems.

5 Conclusion

The vulnerabilities within Bluetooth-enabled patient pacemakers have emerged as a major concern, highlighting the urgency for strong cybersecurity measures to ensure patient safety and uphold trust in healthcare technology. With the inclusion and evolution of Bluetooth connectivity in these life-saving devices, while offering an important convenience in real-time monitoring and data transmission, there are vulnerabilities that pose a substantial security risk. Through a deep dive and examination of existing research, real-life incidents, and expert findings, this paper highlights the gravity of vulnerabilities existing in pacemaker systems.[14]

5.1 Impact of Vulnerabilities:

The identified vulnerabilities, that include improper authentication, unencrypted storage of medical data, and the potential for remote control manipulation, are threats to patient safety. Studies and experiments by cybersecurity experts on top of the discoveries of Marie Moe highlight the concerning consequences and unfortunate reality of potential cyber-attacks on Bluetooth pacemakers. The vulnerabilities, if exploited, could lead to dangerous situations, that could potentially compromise patient health and confidentiality.

5.2 Regulatory and Collaborative Initiatives:

Regulatory bodies like the FDA have responded swiftly to vulnerability discovered, by issuing recalls and creating comprehensive plans to mitigate risks associated with vulnerable pacemakers. Collaboration between manufacturers, healthcare providers, regulatory bodies, and cybersecurity experts have emerged as critical strategies to address vulnerabilities. Other initiatives such as the establishment of platforms for collaboration and technological advancements in encryption devices have shown promise in strengthening pacemakers against any potential cyber threats.

5.3 Implications and Future Directions:

The implications of these vulnerabilities in Bluetooth pacemaker systems extend beyond individual device security, there is also an emphasis on patient safety and healthcare trust. This will ensure patient well-being and will foster trust in healthcare technology, by requiring ongoing collaboration, shared threat intelligence, and a proactive approach toward risk mitigation. Future endeavors must focus on implementing practices such as end-to-end encryption, intrusion detection systems, and frequent firmware updates, that will necessitate collective action from stakeholders for strong security measures.

5.4 Conclusion:

To conclude, the vulnerabilities found in Bluetooth-enabled patient pacemakers pose significant risks to patient safety and healthcare fields. Addressing these vulnerabilities is a priority for patient well-being and the of fostering trust in healthcare technology. Through ongoing research, regulatory initiatives, and collaboration, it is imperative to strengthen security measures. Ultimately protecting patients who are reliant on Bluetooth pacemakers.[15]

References

1. A. Kapoor, A. Vora, and R. Yadav, "Cardiac devices and cyber attacks: How far are they real? how to overcome?," 2019.
2. H. A. M. Puat and N. A. Abd Rahman, "Iomt: a review of pacemaker vulnerabilities and security strategy," in *Journal of Physics: Conference Series*, vol. 1712, p. 012009, IOP Publishing, 2020.
3. T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga, and H. Marquering, "Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: a scoping review," *IEEE Access*, vol. 8, pp. 84352–84361, 2020.
4. C. Ward, S. Henderson, and N. H. Metcalfe, "A short history on pacemakers," *International journal of cardiology*, vol. 169, no. 4, pp. 244–248, 2013.
5. M. Baruscotti, A. Barbuti, and A. Bucchi, "The cardiac pacemaker current," *Journal of molecular and cellular cardiology*, vol. 48, no. 1, pp. 55–64, 2010.
6. B. Alexander, S. Haseeb, and A. Baranchuk, "Are implanted electronic devices hackable?," *Trends in cardiovascular medicine*, vol. 29, no. 8, pp. 476–480, 2019.
7. B. Ransford, D. B. Kramer, D. Foo Kune, J. Auto de Medeiros, C. Yan, W. Xu, T. Crawford, and K. Fu, "Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists," *Pacing and Clinical Electrophysiology*, vol. 40, no. 8, pp. 913–917, 2017.
8. U.S. Food and Drug Administration, "Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication." https://wayback.archive-it.org/7993/20201222110125/https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals, Month Year. Accessed on: December 2, 2023.
9. Keysight, "Uncovering Hidden Threats in Bluetooth Low Energy Medical Devices."
10. National Vulnerability Database, "CVE-2019-19194." https://nvd.nist.gov/vuln/detail/CVE-2019-19194, 2019. Accessed on: December 2, 2023.
11. B. Alexander, V. Neira, D. Campbell, E. Crystal, C. Simpson, A. Enriquez, S. Chacko, H. Abdollah, D. Redfearn, and A. Baranchuk, "Implantable cardioverter-defibrillator–cybersecurity," *Circulation: Arrhythmia and Electrophysiology*, vol. 13, no. 3, p. e008261, 2020.
12. U.S. Food and Drug Administration, "FDA Brief: FDA Warns Patients, Providers About Cybersecurity Concerns with Certain Medtronic Implantable Devices." https://www.fda.gov/news-events/fda-brief/fda-brief-fda-warns-patients-providers-about-cybersecurity-concerns-certain-medtronic-implantable, Month Year. Accessed on: December 2, 2023.

13. Healthcare IT Analytics, "Today's Top Medical Device Security Challenges Mitigation Strategies." https://healthcareexecintelligence.healthitanalytics.com/news/todays-top-medical-device-security-challenges-mitigation-strategies, Month Year. Accessed on: December 2, 2023.
14. V. Tsira, G. Nandi, *et al.*, "Bluetooth technology: Security issues and its prevention," *A Survey. In International Journal of Computer Technology and Applications (IJCTA) Vol*, vol. 5, 2014.
15. K. G. Tarakji, A. M. Zaidi, S. L. Zweibel, N. Varma, S. F. Sears, J. Allred, P. R. Roberts, N. A. Shaik, J. R. Silverstein, A. Maher, *et al.*, "Performance of first pacemaker to use smart device app for remote monitoring," *Heart Rhythm O2*, vol. 2, no. 5, pp. 463–471, 2021.