Indian Heart Journal 71 (2019) 427–430

Contents lists available at ScienceDirect

Indian Heart Journal

journal homepage: www.elsevier.com/locate/ihj

Editorial

Cardiac devices and cyber attacks: How far are they real? How to overcome?

Keywords:
CIED
Cybersecurity

ABSTRACT

Cardiac implantable electronic devices (CIEDs) include bradycardia pacemakers, defibrillators, and cardiac resynchronization therapy devices. These devices are proven to save lives and improve quality of life in indicated patients. Recent advances in CIED technology allow interrogating and transmitting data stored in these devices wirelessly through radiofrequency or Bluetooth technology and more recently through smartphones.[1] Remote monitoring of CIED uses telemetry and IP connectivity to transmit data from devices to the cloud and eventually to hospitals/clinics monitoring them. There has been overwhelming evidence in support of remote monitoring of CIEDs, improving patient outcomes, survival, and hospitalization.[2] Therefore, guidelines recommend remote monitoring for all CIEDs.[3] Remote monitoring allows frequent checks reducing clinic visits, improving efficiency of medical resources and timely intervention in patients with clinical events. Although internet of things (IOT) dependency is increasing, advantages of connectivity and data transfer come with a price of hacking, resulting in malfunction of computers, misuse of stolen data, or medical extortion. Therefore, cybersecurity has become a necessity in this digital world. Medical devices using net connectivity expose themselves to cyber attacks. Fortunately so far no hacking or cyber attack has been reported in patients with CIEDs, and most literature focuses on proof of concept and in-the-research laboratory scenarios. Although documented clinical events have not yet happened, the threat is real. It is essential to be well prepared for this potential but serious threat. It is imperative that device manufacturers, regulatory bodies, medical professionals, and patients all work together to prevent, identify, and mitigate cyber threat.

1. Why are CIED patients at risk of cyber attacks?

Remote monitoring of CIEDs involves transmission of data from patient device to health care professionals. The data transmitted include device function, cardiovascular events, and patient clinical status. This information is analyzed by the medical professionals to optimize medications, tailor therapy, and if necessary reprogram the device. Presently, CIEDs cannot be reprogrammed remotely, and for any reprogramming, an in-person visit to the hospital is necessary. Remote monitoring has proven to improve patient outcomes, reduce hospitalizations, and improve survival. It also regulates patient visits to the hospital, thereby overall reducing the cost burden and strain on health care providers.

1.1. What is the CIED ecosystem?

The CIED ecosystem consists of the device itself and the cloud-based systems and services employed for the diagnosis, therapy adjustment, and monitoring of patients. The other components of the ecosystem are the external programmer usually located at the hospital, the home monitor located at the patient's home, and other devices employed to use these applications (eg. smartphones, tablets, and laptops).

1.2. How does data transmission occur?

The transmission of data from the device earlier used inductive coil telemetry (which uses inductive RF field @ 0–300 kHz) to communicate over short ranges (0–10 cm), requiring proximity between the CIED and the programmer. Most devices now use RF-link telemetry, using traditional RF waves (@ 402–405 MHz, Medical Implant Communications Service—MICS core band) to communicate over longer ranges (0–200 m) and Wi-Fi and Bluetooth technology. The CIEDs are equipped with Wi-Fi transmitters that transmit and communicate with home and mobile monitoring systems, whenever both are in range.[1] These data are then forwarded via the internet to a server/cloud and relayed to the health care professionals, often through the hospital IT network. The information transmitted via the internet is sensitive, including all details of the patient profile, arrhythmia episodes, various alerts, device function status, and even the details of the medical team, hospital, and its computer network.[4]

https://doi.org/10.1016/j.ihj.2020.02.001

At all stages of data transmission, there is a potential threat of hacking.[5] The wireless feature exposes CIEDs to be potentially manipulated by hackers beyond the immediate vicinity of the patient. The transmission of data through the internet and hospital networks makes CIED vulnerable to cyber attacks from anywhere in the world. The transmitted medical data can be stolen, interrupted, or tampered. The worst-case scenario would be to manipulate the device function, cause battery drain, and disable the device. This potential cyber attack can occur anytime in the lifespan of the device!

2. How can a 'hacker' compromise the functioning of CIEDs?

There are many ways in which a hacker can potentially breach the cybersecurity of the CIED ecosystem and these include the following:

1. CIED-Monitor/Programmer communication interception: Using software-defined radio (SDR) to intercept the RF signals.
2. Accessing the device USB port and reading or extraction of the monitor files.
3. Insertion of a backdoor (malware) into the monitor to modify/erase the contents of the monitor memory or induce programmer reading errors or cause spoof programming.
4. Initiate boundless telemetry sessions: maintain a telemetry session indefinitely active by regularly sending commands to prematurely reduce the CIED's battery lifetime.
5. Accessing the CIED ecosystem during firmware updates or levering into the device's local network access to interfere with the communication between the programmer and software update provider.

3. What are the potential cybersecurity risks for the CIED patients?

The intended goals for cyber-hacking a CIED include the following (summarized in Table 1):

1. To access patient-sensitive data
   - Either medical data or other personal information such as email, addresses, and phone and social security numbers could be stolen. Potential clients include insurance companies (medical or automobile) that may use this information either to assess insurance premiums or even refuse coverage in individual cases.
2. To gain knowledge of device operation and software
   - The intense competition between various device manufacturers can encourage industrial spies to target the CIED ecosystem and gain information about device design, software, engineering details, etc. This intellectual property theft can then be made available for sale to competitors or even counterfeit medical device manufacturers (akin to production of counterfeit or generic drugs)
3. Alter device behaviour to disrupt/interfere with patient follow-up or even endanger patient's life.
   - This is the most worrisome aspect of cyber-hacking. Changing device settings and issuing false alarms to make the patients visit the hospitals repeatedly or in extreme cases inducing battery depletion (by boundless telemetry) or even disabling therapy can endanger lives. Random or high-visibility individuals can be targeted raising issues of personal security. Individual CIED manufacturers can be targeted to seem as if their equipment is defective, thus damaging the company's sales revenue and reputation and money demanded to restore services (medical device–based extortion).

Table 1
The potential consequences of hacking a CIED are enumerated below.

A. Pacemaker
   a. Sensing concern: Oversensing and inhibition or loss of pacing
   b. Pacing concern: Sudden battery depletion and loss of pacing
B. ICD
   a. Sensing concern: Loss of pacing and inappropriate shocks
   b. Disabling therapy: Failure to terminate VT/VF
C. Sudden battery depletion
D. Failure to interrogate the device through telemetry
E. Stealing of patient and clinical data during wireless transmission by the remote monitoring systems
F. Gain unauthorized access to the hospital computer network, and causing its malfunction, when the CIED data are being transmitted to the health care providers via the internet.

Till date, there has not been any incidence of cyber attack and no harm has been done to a single patient with CIED. However, as a proof of concept of cyber threat, there has been experimental evidence jeopardizing the St Jude Merlin home monitoring system and more recently the Medtronic CareLink programmers.

The 2016 Muddy Waters Research reported that CIEDs manufactured by St Jude Medical (Abbott) are at risk of hacking.[6] The researchers provided a laboratory evidence of cybersecurity breach. With excess radio traffic, the Merlin product line would result in a 'crash' situation, wherein interrogation of the CIED with telemetry was no longer possible. This 'crash' condition was replicated by others but without affecting the essential clinical performance of the pacemaker and therefore no harm to the patient. The other cybersecurity breach was the 'battery drain' attack which could reduce the device longevity. This reporting resulted in a lawsuit, raised ethical concerns, and is also the first cybersecurity related recall by US FDA. Eventually, a software update helped resolve the issue.[7,8] There is a small, theoretic risk of CIED malfunction because of the update; however, this risk is negligible compared with the threat created by this cybersecurity breach.

More recently (2018), 'CareLink,' the Medtronic programmer, was found to have a cybersecurity breach.[9,10] The Medtronic CareLink 2090 and CareLink Encore 29901 programmers receive software updates through a USB port or via the internet using the 'Software Distribution Network' (SDN). The process of updating the software through SDN was perceived to be vulnerable to cyber attack. There was a potential risk of intercepting and modifying the updates on the programmers such that using them to update the CIED could lead to its malfunction. This threat was fixed by recommending and ensuring that the software update was performed manually by the Medtronic engineer using the USB.

In broad terms, cyber attack on CIEDs may be passive or active. A passive attack accesses sensitive information exchanged between the device and health care network occurring in an insecure transmission. The modern day CIEDs store all contact details of the patient-physician-hospital. This information can be stolen and misused or leveraged by the hacker for a ransom or identity theft. The data generated, stored, and transmitted by the CIEDs should be protected against loss or manipulation. An active cyber attack would mean that the diagnostic or therapeutic capability of the CIEDs operating function are altered, resulting in direct harm to the patient or a battery drain resulting from a bombardment of information request.

Cyber attacks are likely to increase over the years and through the life cycle of the CIED. It remains to be seen whether these attacks will directly impact patients or health care facilities or the device manufacturer.

4. How to prevent the cyber attacks on CIEDs?

Cybersecurity for CIEDs need a close and timely collaboration with the device manufacturer, governmental regulatory body, physicians, IT specialists, and patients. The process for cybersecurity starts with the conception and design of the CIEDs and continues through the manufacturing, implanting, and follow-up of these devices. The postimplant surveillance must be robust, identifying vulnerabilities and addressing these issues quickly and continue to do so throughout the lifespan of the CIEDs. Patient data should always be encrypted and transferred via a secured network. High level of security in data transmission must be employed using principles of confidentiality, integrity, authenticity, accountability, and reliability.[11] CIED access to hackers should be prevented and rarely the remote monitoring option may have to be temporarily disabled.

A. CIED manufacturer's role: Cybersecurity protocol should be followed in manufacture of these devices. IT security and solutions are an integral part for mitigating the risks of cyber threats for CIEDs. 'Firmware' should be installed in these devices which can be updated anytime later, when new vulnerabilities are identified.[12] There should be access logs, which can identify unauthorized accesses. Appropriate cryptographic measures should be utilized during wireless transmissions from the device. Authentication processes will help reduce the security breaches. Surveillance through the life of CIED is essential and includes identifying security flaws and rectifying them promptly. The manufacturer should immediately alert the federal agency and physicians on any vulnerability, quickly resolve the issue, and update the CIEDs, with the help of IT experts. The manufacturer should provide all details of the potential security breach, measures to be taken (software update, etc.), CIED models, and programmers involved in their website, press release, and helplines. The solution provided for the cybersecurity breach should be virtually risk free so that every patient requiring the necessary update for their CIED receives so.
B. Physician's role: Physician's role is to be updated with all the potential and documented cyber threats. This information could be accessed through the manufacturer, published literature, professional organization/councils advisory, or consensus documents. It is important that the physician clearly understands the security risk and necessary steps to be implemented. The patient should be engaged by the physician, allay their anxiety, and perform the necessary software updates along with the industry engineers. There is a small but distinct risk, especially in pacing dependant patients of a potential malfunction of the device during firmware updates.
C. Hospitals' role: The hospital computer network is an easier target for hackers, and therefore, it should be adequately protected from any unauthorized access.[13] More secure networks with identity-access management systems need to be installed. Active consideration should be given to recruit cybersecurity professionals to ensure that there are no cybersecurity threats in systems. Secure system authentication with robust passwords, countermeasures (proxy between the programmer and device), not using unpatched hospital networks and most importantly conducting awareness campaigns among the staff who use those devices, so that they are aware of the problem and avoid using software beyond the supported period.
D. Patient's role: Patient's role is to understand the potential cybersecurity risk with all CIEDs. The technological advance allowing home monitoring and transmission of data has overall improved patient outcomes, but it has come with a price of exposing them to hacking. Patients should realize that no harm has been done to any patient so far; however, the potential risk is real and everyone should play their part to nullify the danger. In case of any media report, it is best for them to contact their implanting physician and clarify. Looking up the website of the manufacturer and federal agencies will provide them with details on the security issue and the proposed solution.

5. Conclusions

CIEDs continue to advance in technology and are increasingly utilizing wireless transmission, internet, and hospital computer network to transmit sensitive demographic and clinical data of patients and device performance. This has resulted in overall improving patient outcomes and recent guidelines recommend remote monitoring for all CIED patients. However, with this connectivity, hacking of patient data and jeopardizing device function and hospital networks have become a potential and real threat. Although the goal is to design CIEDs that are perfectly secure, it is important to realize that computer systems relying on internet and intranet networks are potentially exposed to cyber threats. For cybersecurity of CIEDs, regular updates will be required, and the procedures for updates must be familiar to health care professionals and patients.

All stake holders including the manufacturers, security experts, clinicians, regulators, and patients need to collaborate, develop, and maintain good secure processes to overcome this challenge. It is equally important to communicate and improve public perception about CIED cybersecurity. So far, no patient harm has been reported because of a cyber attack on CIEDs, and the challenge in the future is to maintain this security alongside increasing advances in device complexities.

References

1. Martignani Cristian. Cybersecurity in cardiac implantable electronic devices. *Expet Rev Med Dev*. 2019;16(6):437–444.
2. Maisel William H, Paulsen Jessica E, Hazelett Matthew B, Selzman Kimberly A. Striking the right balance when addressing cybersecurity vulnerabilities. *Heart Rhythm*. 2018;15(7):e69–e70.
3. Slotwiner David, Varma Niraj, Akar Joseph G, et al. Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. *Heart Rhythm*. 2015;12(7):e69–e100.
4. Baranchuk Adrian, Refaat Marwan M, Patton Kristen K, et al. Cybersecurity for cardiac implantable electronic devices. What should you know? *J Am Coll Cardiol*. 2018;71(11):1284–1288.
5. Ricci Linda, Paulsen Jessica, Browning Stephen, et al. An overview of the security of cardiac implantable electronic devices. *Pacing Clin Electrophysiol*. 2017;40:911–912.
6. Muddy Waters LLC. *MW Is Short St. Jude Medical (STJ: US)*; August 25, 2016. Available at: http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/.
7. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome.
8. Slotwiner David J, Deering Thomas F, Fu Kevin, Russo Andrea M, Walsh Mary N, Van Hare George F. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians—proceedings of the Heart Rhythm Society's Leadership Summit. *Heart Rhythm*. 2018;15(7):e61–e670.
9. Pycroft Laurie, Aziz Tipu Z. Security of implantable medical devices with wireless connection: the dangers of cyber-attacks. *Expet Rev Med Dev*. 2018;15(6):403–406.
10. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.
11. Ransford Benjamin, Kramer Daniel, Foo Kune Denis, Auto de Medeiros Julio, Yan Chen, Xu Wenyuan. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. *Pacing Clin Electrophysiol*. 2017;40:913–917.
12. Alexander B, Haseeb S, Baranchuk A. Are implanted electronic devices hackable? *Trends Cardiovasc Med*. 2019;29(8):476–480.

13. Paulsen Jessica E, Hazelett Matthew B, Schwartz Suzanne B. CIED Cybersecurity risks in an increasingly connected world. *Circulation*. 2018;138:1181–1183.

Aditya Kapoor
Department of Cardiology, Sanjay Gandhi PGIMS, Lucknow, India

Amit Vora[*]
Arrhythmia Associates, Mumbai, India

Rakesh Yadav
Department of Cardiology, All India Institute of Medical Sciences, Delhi, India

[*] Corresponding author.
E-mail address: amvora@hotmail.com (A. Vora).