CONTEMPORARY REVIEW

Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices

Subrat Das, MD,[*] Gregory P. Siroky, MD,[†] Shawn Lee, MD,[†] Davendra Mehta, MD, PhD, FHRS,[†] Ranjit Suri, MD, FHRS[†]

From [*]Department of Medicine, Mount Sinai Morningside-West, Icahn School of Medicine, New York, New York, and [†]Department of Cardiology, Mount Sinai Morningside, Icahn School of Medicine, New York, New York.

Remote monitoring of cardiac implantable electronic devices (CIEDs) has become routine practice as a result of the advances in biomedical engineering, the advent of interconnectivity between the devices through the Internet, and the demonstrated improvement in patient outcomes, survival, and hospitalizations. However, this increased dependency on the Internet of Things comes with risks in the form of cybersecurity lapses and possible attacks. Although no cyberattack leading to patient harm has been reported to date, the threat is real and has been demonstrated in research laboratory scenarios and echoed in patient concerns. The CIED universe comprises a complex interplay of devices, connectivity protocols, and sensitive information flow between the devices and the central cloud server. Various manufacturers use proprietary software and black-box connectivity protocols that are susceptible to hacking. Here we discuss the fundamentals of the CIED ecosystem, the potential security vulnerabilities, a historical overview of such vulnerabilities reported in the literature, and recommendations for improving the security of the CIED ecosystem and patient safety.

KEYWORDS Cardiac implantable electronic device; Cybersecurity; Data security; Hacking; Remote monitoring

(Heart Rhythm 2021;18:473–481) © 2020 Heart Rhythm Society. All rights reserved.

Introduction

Technological advances in microprocessors, high-density battery designs, and biomedical engineering in the last 2 decades have brought major changes to the way we monitor and treat patients. These effects have been felt mostly in the field of cardiology, specifically in the realm of cardiac implantable electronic devices (CIEDs), which include 2 broad categories: permanent pacemakers (PPMs) and implantable cardioverter-defibrillators (ICDs). PPMs and ICDs differ in programming and functionalities, but at the heart of the technology is a programmable platform, a lithium ion or other type of battery, a capacitor, and a pulse generator. With the advent of the Internet of Things (IoT), these devices can be used to remotely monitor patients through cloud-based servers that provide data to the physician or health care team (Figure 1).

Several studies have shown that remote monitoring (RM) of these devices improves patient outcomes, survival, and hospitalizations, and is being recommended as standard of care in multiple consensus statements and guidelines published by the Heart Rhythm Society (HRS).[1,2] In view of this and the demonstrated reduction of in-person visits, the burden on physicians and clinics, and the established reimbursement for remote services, there has been increasing adoption of RM into medical practice. However, with the increased dependence on IoT comes risks in the form of cybersecurity lapses and possible attacks. Multiple instances of such theoretical breaches have been reported by cybersecurity experts and the Food and Drug Administration (FDA) (see section on CIED security threats and action). Although no cyberattack leading to patient harm has been reported to date, the threat is real, as has been demonstrated in research laboratory scenarios. In a more fictional domain, the popular television show *Homeland* depicts the assassination of the Vice President of the United States by a terrorist remotely hacking into the victim's pacemaker. This may have been a concern in 2007 when doctors replaced then Vice President Dick Cheney's implantable defibrillator and asked the manufacturer to disable the remote monitoring feature, hoping to keep out any would-be hackers.[3]

Here we discuss the basics of the CIED ecosystem; potential targets for attack; reported events of such vulnerabilities in the literature, including the mitigation strategies involved; and recommendations for improving the overall security of the CIED ecosystem and thus patient safety.

The CIED universe

The CIED ecosystem comprises the implantable device; an external programmer (used in the physician's office to

Funding sources: The authors have no funding sources. Disclosures: The authors have no conflicts of interest to disclose. **Address reprint requests and correspondence:** Dr Ranjit Suri, Mount Sinai Morningside, 1111 Amsterdam Avenue, New York, NY 10025. E-mail address: ranjit.suri@mountsinai.org.

1547-5271/$-see front matter © 2020 Heart Rhythm Society. All rights reserved. https://doi.org/10.1016/j.hrthm.2020.10.009

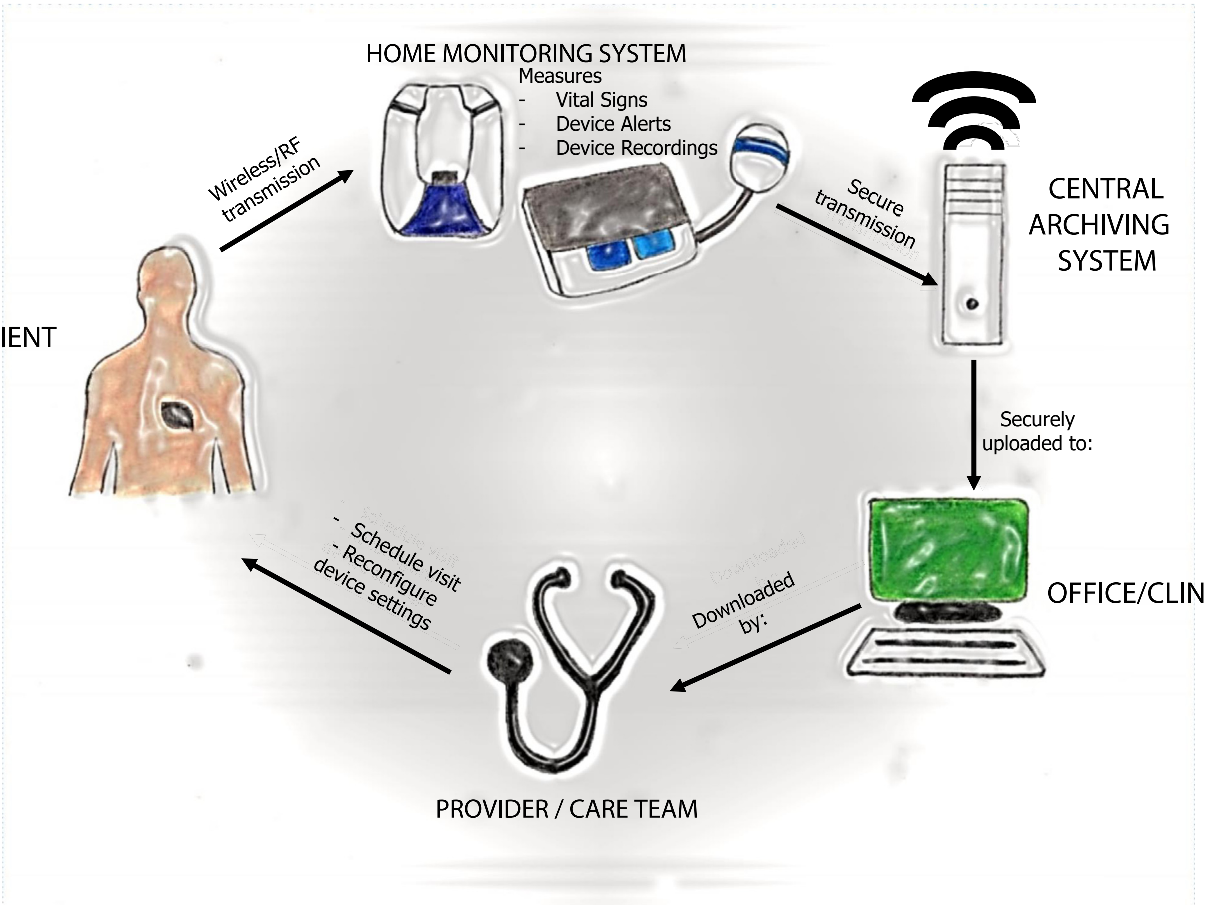


Figure 1 Schematic diagram showing how remote information is transmitted from a patient's cardiac implantable electronic device (CIED) to the health care provider. Starting from the patient, information uploaded from the patient's CIED to the home monitoring system is transmitted to a central archiving system, which then uploads the information to the physician's office. Once the physician/care team reviews the uploaded data, they can reach out to the patient to discuss necessary treatment options. RF = radiofrequency. (Illustrated by Dr Shawn Lee.)

interrogate and program the implanted device); a home monitor (receives transmission from the implantable device and sends it through the Internet to the cloud server); the cloud server; and proprietary software/hardware used by the physician's office to access patient data. The flow of data and information between these devices occurs via various open source and proprietary protocols that can be exploited.

Detailed information on the hardware and software architecture of CIEDs is difficult to obtain due to the proprietary nature of such devices, but a basic understanding of the devices can be formulated based on information gathered from patent documents and reverse-engineering efforts of cybersecurity experts. A CIED is composed of 4 essential components:

1. *Microprocessor:* Coordinates activities among the various components of the device and can be imagined as the "brain" of the device.
2. *Memory:* Comprises read-only memory (ROM) and random-access memory (RAM). The ROM contains low-level executable data, also known as firmware. The RAM contains device information, patient recordings, and treatment algorithms.
3. *Telemetry circuit:* Responsible for transmitting and receiving data to and from the home monitor or the external programmer.
4. *Timing circuit:* Synchronizes stimulation pulses to the heart chambers and memory access.

The CIED communicates with the home monitor and external programmer using either short-range (0–10 cm) inductive coil telemetry (ICT) with a frequency band of 0–300 kHz or long-range (0–200 m) radiofrequency (RF)-mediated telemetry with a frequency band of 402–405 MHz. The latter frequency band, also known as the medical implant communication service (MICS) band, initially was allocated by the Federal Communication Commission in 1999.[4] Because the MICS band is shared with devices utilized in metrological services, its use has been normalized to avoid interference. The devices use interference mitigation techniques such as listen before talk to determine the least

Table 1 Attack scenarios, vulnerability explored, and possible harm done

Attack scenario	Vulnerability explored/technique used	Possible harm
CIED–monitor communication interception	Intercepting RF signal with SDR	Stealing patient information Interrupting data transmission to home monitor Inserting wrong data into home monitor, jeopardizing data fidelity
Extraction of health data stored in monitor	Connecting to debugging ports MITM attacks during communication between monitor and central server	Stealing patient information Inserting wrong data into home monitor, jeopardizing data fidelity
Insertion of malware into monitor	MITM attack during firmware update Connecting to debugging ports	Causing dysfunction of the monitor Creating a backdoor to steal CIED data Disabling periodic data transmission between the monitor and central server, thus delaying timely recognition of life-threatening CIED recordings
Reading into monitor file system	Connecting to USB port and accessing unencrypted drives on the monitor	Stealing patient information Corrupting file systems and rendering the monitor nonfunctional Deleting stored data Changing stored data and affecting data fidelity Corrupting transmission protocols, rendering talk between the monitor and central server ineffective
Introduction of calibration error in the CIED	Injecting malware through RF commands, especially during home monitor–CIED interaction via the CIED or programmer	Inappropriate reading of patient rhythms Blocking delivery of lifesaving treatments to the patient
Keeping CIED telemetry session open indefinitely	Sending repeated RF signal using SDR	Decreasing device longevity by draining the battery
Insertion of malware into CIED	Sending unauthorized RF signals using SDR MITM attack during CIED–programmer communication	Inserting a faulty algorithm that can prevent appropriate shock or cause inappropriate shock to the patient, causing harm Stealing patient rhythm data Creating a backdoor into the CIED that can be exploited during future attacks
CIED–programmer communication interception	Intercepting RF signals with SDR	Stealing patient information Interrupting data transmission to home monitor Inserting wrong data into programmer, jeopardizing data fidelity Inserting malware into CIED during communication Inserting faulty algorithms and treatment protocols into CIED that can cause patient harm/death
Reading into programmer file system	Intercepting communication between programmer and central server, especially during firmware update process Using USB port or debugging port to read unencrypted files on the programmer memory	Stealing patient information Interrupting data transmission between the programmer and central server Exploiting root access and directory access, injecting malware into the programmer
Insertion of malware into programmer	MITM attack during update session Accessing USB or debugging port	Stealing patient information Keeping a backdoor open for future attacks Injecting faulty algorithms that can be later transmitted to the CIED and cause patient harm Causing programmer reading errors, making the device nonfunctional
Unauthorized access to cloud server	Exploring DDoS attack Sending malicious http server request	Massive data breach with potential to affect thousands of patients

CIED = cardiac implantable electronic device; DDoS = distributed denial of service; MITM = man in the middle; RF = radiofrequency; SDR = software-defined radio; USB = universal serial bus.

interference channel and use adaptive frequency agility to transmit on the least used channel.[5] Although the signal transmission is governed by well-documented international protocols, the same does not hold for device authentication. Existing FDA regulations define good practices but are not binding on manufacturers.[6] Moreover, due to the limitations imposed by CIED size and design, use of resource-intensive cryptographic practices such as asymmetric cryptography is difficult.

The data collected by the home monitor and the external programmer are transmitted to the cloud server and further relayed to the physician's office over the Internet using a virtual private network (VPN). This transmission contains sensitive patient and device data, details of various triggering events, and physician/medical team information. Unfortunately, there is a threat of the transmission being hacked during all stages of the flow of information.[7] Per present guidelines, the CIED cannot directly interact with or download firmware from the cloud server. This is accomplished only through the external programmer at the physician's office using RF telemetry or ICT. However, the RF transmission can be intercepted using a software-defined radio (SDR), and then sensitive data could be viewed or malware implanted into the device during firmware update.

CIEDs reside in a diverse and complex world of open source and proprietary communication protocols, with major loopholes that can be exploited to gain unauthorized access to the devices. These intrusions can lead to data theft, device hijacking, or incorrect algorithm injections that result in inappropriate triggering or inhibition of therapies that would affect patient safety.

CIED vulnerabilities

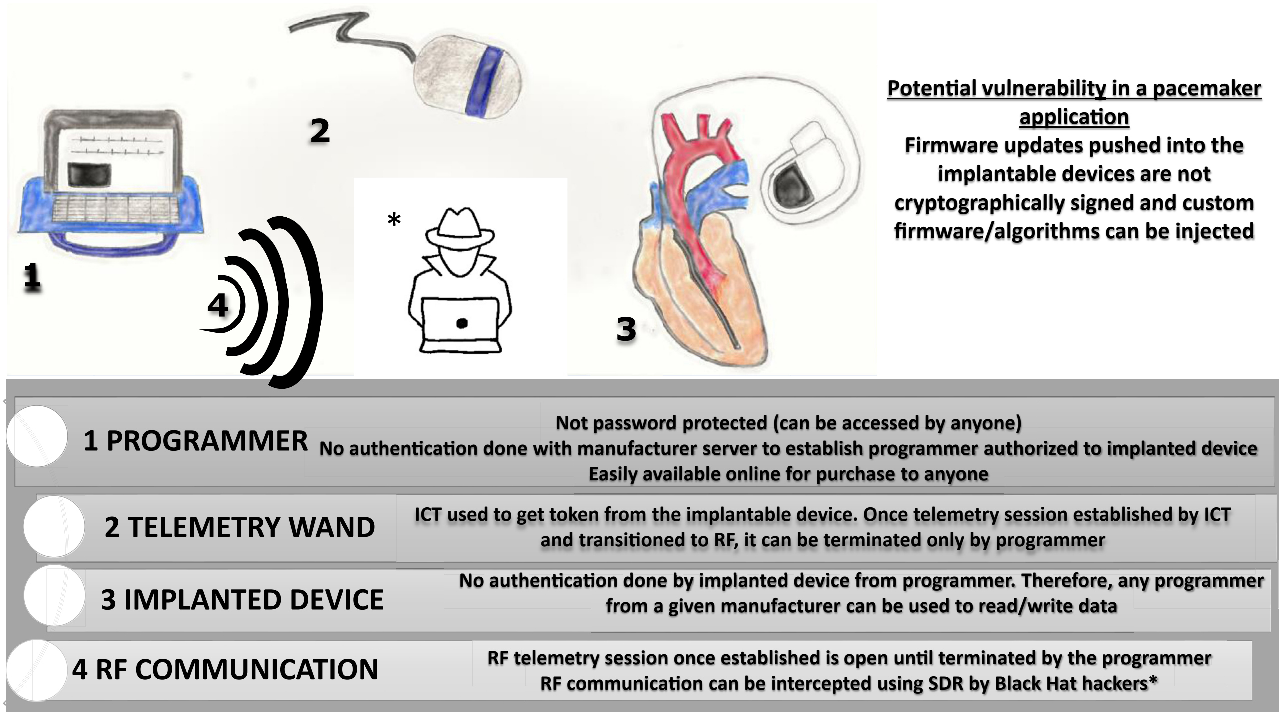
Hacking is defined as activities that are intended to compromise digital devices, including computers, IOT devices, or entire networks.[8] Although a cyberattack leading to patient harm has never been documented, multiple avenues exist through which cyberattacks can be carried out (Table 1).

A. *Home monitor–CIED communication.* Present guidelines do not allow initiation of CIED to programmer/home monitor transmission until the transmission is initiated by the external device. The exception is Biotronik (Berlin, Germany) devices, for which only the implant can initiate communication. As such, Biotronik devices are best classified as "remotely monitored" devices as opposed to the devices of the other manufacturers, which are "remotely interrogated." In addition, most of the devices use cryptography to ensure that transmission occurs between trusted devices. One technique generally used is time-based, one-time password (TOP), which generates a password based on the time and a predefined secret key. For some devices, the secret key is the device's model or serial number. This can enable unauthorized users to generate valid passwords every time they want to establish a telemetry session.[9] Moreover, certain CIEDs have hardcoded unencrypted authentication credentials. In hardcoding, the credentials are written into the source code during the software development process, as opposed to obtaining the data from external sources or generating them at run time.[10] Hardcoded entities are difficult to modify, so once hacked they can be used endlessly to authenticate the device. Some CIEDs store and transmit information without encrypting it, which allows hackers to gain access to such implantable devices while they are communicating using the RF protocol.

B. *External programmer–CIED interaction.* An external programmer in the physician's office is used to interrogate and program the implanted device. To initiate a session, ICT is used to retrieve a token key from the CIED, which is then used to generate a session key. The token key can be the serial number of the implanted device (hardcoded into the device), TOP, or static advanced encryption standard key. Once the device identity has been verified, then the session is transitioned to RF telemetry. There are no interval authentication checks once the RF telemetry session is established, and the session can be terminated only from the programmer. Because the programmer does not authenticate the implantable device, the implication is that any programmer from the manufacturer can be used to read and write into any implantable device from that manufacturer. The programmer is not password protected and can be used by anyone who has access to the programmer. This makes the programmer a powerful and hence a "controlled" device (meaning returned to the manufacturer after use). Notwithstanding the grave consequences of unauthorized access to programmers, such programmers are easily available on bidding and online markets such as eBay.[11] Moreover, pacemaker firmware updates are not cryptographically signed, so pushing custom firmware into a CIED is a theoretical possibility (Figure 2).

C. *Initiate boundless telemetry session.* There are no limits to the number of telemetry sessions that can be initiated with the CIED. A hacker can keep initiating a new telemetry session before the previous one is terminated, thus keeping the telemetry session open indefinitely. In addition, once the telemetry session between the programmer and implantable device is established in the office, the session can be terminated only by the programmer. Hence, an individual with unauthorized access to the programmer (or in the more benign situation of forgetful office staff) can keep the telemetry session open indefinitely. Because these sessions are battery intensive, such a hack will drain the device's battery, decreasing the life of the implant.[12]

D. *Poor utilization of secure VPN during external programmer/home monitor communication with central cloud-based server.* It is general industry practice to download software and firmware updates from the server through a VPN. Although use of a VPN is considered good practice, some devices do not verify that they are still connected throughout the entire update process. In these



Potential vulnerability in a pacemaker application

Firmware updates pushed into the implantable devices are not cryptographically signed and custom firmware/algorithms can be injected

1 PROGRAMMER	**Not password protected (can be accessed by anyone)** **No authentication done with manufacturer server to establish programmer authorized to implanted device** **Easily available online for purchase to anyone**
2 TELEMETRY WAND	**ICT used to get token from the implantable device. Once telemetry session established by ICT and transitioned to RF, it can be terminated only by programmer**
3 IMPLANTED DEVICE	**No authentication done by implanted device from programmer. Therefore, any programmer from a given manufacturer can be used to read/write data**
4 RF COMMUNICATION	**RF telemetry session once established is open until terminated by the programmer** **RF communication can be intercepted using SDR by Black Hat hackers***

Figure 2 Office scenario in which an office programmer is used to read from/write to the cardiac implantable electronic device. Security vulnerabilities inherent to the process are highlighted. ICT = inductive coil telemetry; RF = radiofrequency; SDR = software-defined radio. (Illustrated by Dr Shawn Lee.)

situations, hackers can inject malicious software during the update process.[13] Hackers can also inject malware that creates backdoors, which can be used later to snoop into patient-sensitive data stored on the implanted device. These kinds of attacks are termed "man in the middle" (MITM) attacks.

E. *Unauthorized access to the universal serial bus (USB) port.* Some external programmers and home monitors have a USB port that can be used by the physician's clinical staff to export device information onto a USB stick. If these ports are not protected by strong passwords, they can be used to gain access to the external programmer or the home monitor, to read the stored data, or to inject malicious software that can alter the function of the implanted device.

Multiple attack scenarios can be executed based on the opportunity, intent, and expertise of the hacker. Given the ease of access to the programmer and the lack of authentication by the implanted device, it is an *intent* away from being exploited. The issue at hand is not that of technical difficulty but of social hacking.

CIED security threats and action

To the best of our knowledge no security breach/hacking effort resulting in direct patient harm has been reported to date, but multiple security vulnerabilities have been pointed out by security experts and verified by the FDA (Figure 3).

Muddy Water Research Report on Abbott (St. Jude Medical, St. Paul, MN)—2016

The research reported a cybersecurity vulnerability in Abbott CIEDs wherein increased radio traffic would cause devices in the Merlin product line to crash, and implantable device interrogation would no longer be possible.[14] Others have replicated the attack and found that it did not affect the basic functioning of the implantable device. The other breach mentioned in the report was a "battery drain" attack in which the longevity of the implantable device's battery was compromised. This had more serious implications that led to a lawsuit and later the first recall of a device by the FDA due to cybersecurity concerns.[15,16] The manufacturer eventually developed a firmware update that adjudicated the problem, and although there was a small theoretical risk of device malfunction associated with the update, a shared decision-making model was used to approach the discussion with patients.

Medtronic (Minneapolis, MN) CareLink Programmer—2018

Medtronic CareLink programmers (CareLink 2090 and CareLink Encore 29901) receive software updates either through the USB port or over the Internet using the Medtronic Software Distribution Network. Over-the-Internet updates are received through a Conexus wireless telemetry protocol, which is used as part of the communication method among Medtronic PPMs, ICDs, clinic programmers, and home

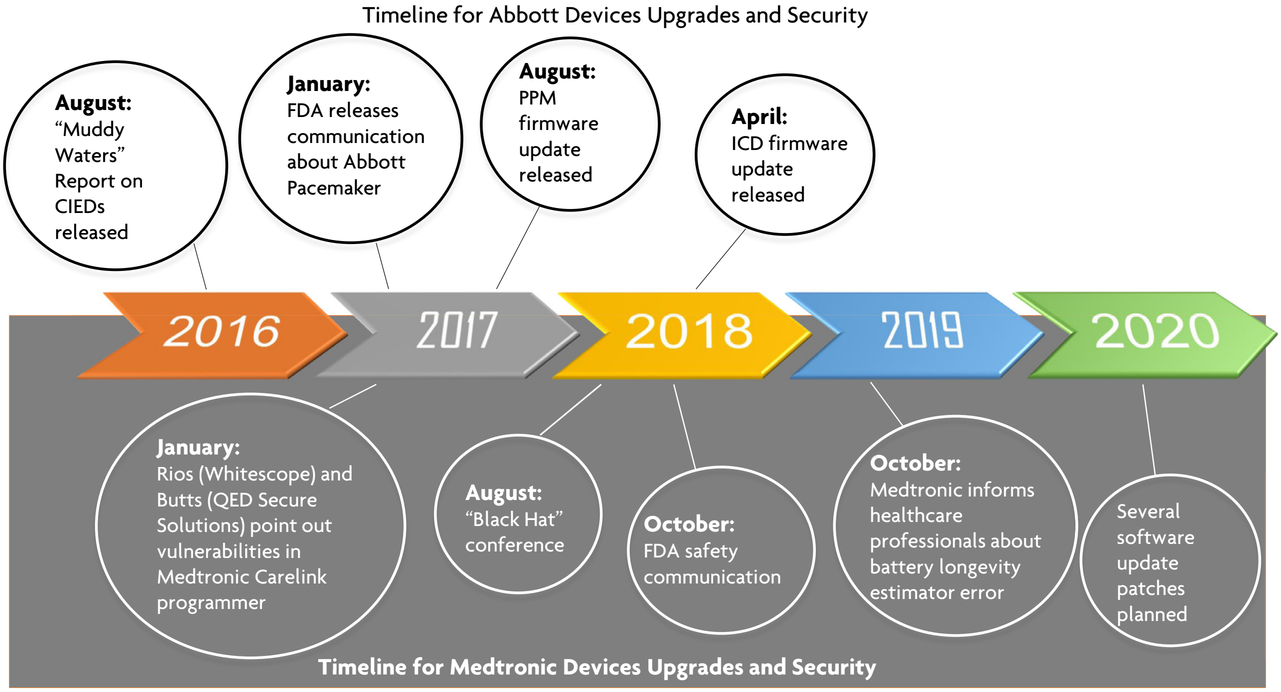

Timeline for Abbott Devices Upgrades and Security
August: "Muddy Waters" Report on CIEDs released
January: FDA releases communication about Abbott Pacemaker
August: PPM firmware update released
April: ICD firmware update released
2016
2017
2018
2019
2020
January: Rios (Whitescope) and Butts (QED Secure Solutions) point out vulnerabilities in Medtronic Carelink programmer
August: "Black Hat" conference
October: FDA safety communication
October: Medtronic informs healthcare professionals about battery longevity estimator error
Several software update patches planned
Timeline for Medtronic Devices Upgrades and Security

Figure 3 Timeline of cybersecurity events reported by security experts and the Food and Drug Administration (FDA), and the corrective measures taken by device manufacturers. CIED = cardiac implantable electronic device; ICD = implantable cardioverter-defibrillator; PPM = permanent pacemaker. (Illustrated by Dr Shawn Lee.)

monitors. This protocol has cybersecurity vulnerabilities as it does not use encryption, authentication, or authorization. Billy Rios of the security firm Whitescope and Jonathan Butts of QED Secure Solutions pointed out these vulnerabilities to the manufacturer in January 2017[17] and again at the Black Hat conference in August 2018.[18] The FDA became aware of this matter and published a security update on its website confirming the vulnerabilities. It confirmed that these vulnerabilities, if exploited, could allow an unauthorized individual (eg, someone other than the patient's physician) to access and potentially manipulate an implantable device, home monitor, or clinic programmer.[19] The vulnerabilities stem from use of an antiquated operating system (OS)—Windows XP—and the lack of digital code signing (DCS) during the updates. DCS is a cryptography practice that legitimizes the validity and integrity of the downloaded and installed software. DCS mitigates MITM attacks. The company responded to the threat by limiting the updates to take place only through the USB port and not over the Internet. The implantable devices were unaffected by this security vulnerability or the update process.[20]

Medtronic Longevity Estimate Software Error—2019

In October 2019, Medtronic informed health care professionals that a subset of PPMs and ICDs (including cardiac resynchronization therapy and Micra transcatheter pacing system devices) manufactured between October 2018 and April 2019 may display an inaccurately short estimate of battery longevity. The battery itself was working appropriately and did not require replacement. Approximately 53,100 of 1.23 million CIEDs distributed worldwide from the identified device families are susceptible to displaying this inaccurate longevity. Through September 2019, Medtronic reported that there had been only 3 complaints and no serious adverse events or deaths. Because battery longevity estimation is calculated by the external programmer and not the implantable device, individual CIEDs did not need to be updated. A software patch to fix this issue was released in October 2020.[21]

A way forward

Cybersecurity of CIEDs is a collaborative effort among device manufacturers, regulatory bodies (FDA, Department of Homeland Security), professional organizations (Heart Rhythm Society), physicians, information technology (IT) security experts, and, last but not the least, patients (including advocacy groups). The cybersecurity aspects must be incorporated during the design phase of the device, as resource constraints on computing and cryptographic algorithms need to be tackled. This should be followed up with a strong and independent assessment of postimplant threat analysis and truthful reporting of cyberattack events. Patient data should always be encrypted with asymmetrical encryption methods, whenever possible. Stringent data transmission protocols should be followed based on the principles of confidentiality, integrity, authenticity, accountability, and reliability.[22] Each of the stakeholders should work on their part to make the CIED ecosystem reliable and secure (Figure 4).

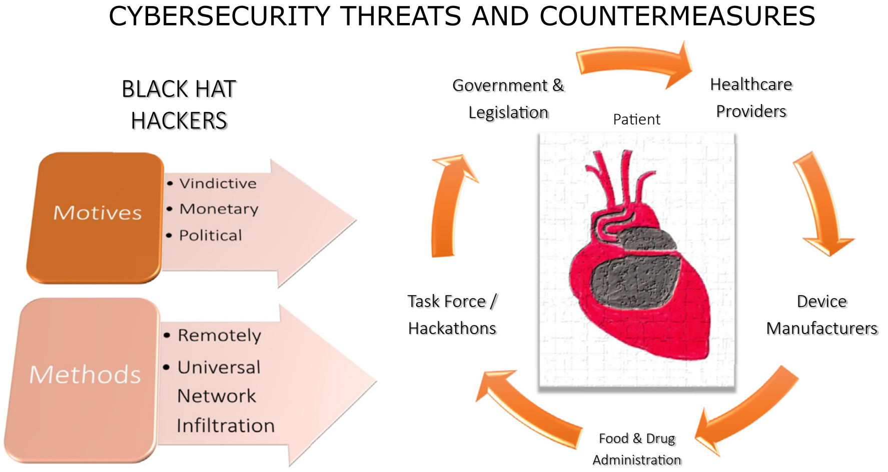


Figure 4 Cardiac implantable electronic device ecosystem, hacker motives and methods, and various players involved in keeping the ecosystem secure. (Illustrated by Dr Shawn Lee.)

CIED manufacturers

Device manufacturers should be cognizant of cybersecurity threats during the device development phase. Use of the latest OS, healthy coding practices, and integration of firmware that can be updated at later dates are some of threat mitigation steps that can be followed by manufacturers. There has been increasing criticism by IT security experts and patient advocacy groups regarding the use of proprietary and black-box algorithms and codes by device manufacturers. Manufacturers should use open source OS and make their source code public. These steps help in effective debugging of codes and timely reporting of security threats that can be acted upon. Encryption of patient data and secure transmission protocols should always be used and should be part of the device development process. Continued surveillance through the life of the CIED should be practiced, with prompt identification of security flaws and swift rectification of the identified flaws. Device manufacturers should be more forthcoming in their responses to security concerns raised by independent security experts and work with them to solve any issues. A more robust collaboration effort across CIED vendors is required to jointly develop standards that improve and promote "widespread immunity."

Another area of concern is the minimal accountability regarding the supply and use of programmers. Programmers are not password protected, do not require verification from the central server, and are not verified by implanted devices (Figure 2). As such, physical custody of programmers and strict access restrictions are important components of security. Despite this issue, external programmers or home monitors can be easily purchased from online sites. Although such websites should be more responsible with their listings, it should be the manufacturer's primary responsibility to regulate access to such devices. We propose that all programmers should be accounted for. A technique such as that used by the Apple iPhone can be implemented wherein a programmer that is reported as missing is deactivated by the manufacturer from its central server. Also, it should be mandatory for the programmers to have booting password and verification from the manufacturer's server before they can initiate any telemetry session. These steps will ensure that the programmers are being operated by authorized users.

Telemetry sessions initiated during office visits should be timed and auto-terminate after the specified time. This will ensure that no indefinite telemetry sessions are running between the implantable device and the programmer, which is an easy target for snooping using SDR. The current philosophy of "security through obscurity" practiced by device manufacturers needs to be replaced by open source coding practices. Device manufacturers should declare, at least broadly, the steps they take to ensure data and patient safety. The "black-box" approach toward data handling and cybersecurity can only decrease patient and physician trust in devices and technology in general. Device manufacturers should collaborate to formulate and implement security standards that will foster trust and help the industry in the long run. We propose that manufacturers in conjunction with cybersecurity experts work toward establishing industry standards on data collection, transmission, and storage. An interoperable, open source platform will accelerate device adoption and patient trust. Collaborative efforts in the past steered by the HRS and the Cardiology Domain of the Integrating the Healthcare Enterprise in the form of Connectathon events have led to uniform CIED nomenclature, development of new data elements, and interoperability across multiple platforms.[23] Such collaborative efforts with CIED manufacturers can lead to robust and interoperable cybersecurity protocols.

Regulatory authorities

The FDA believes that regular updates of devices, home monitors, and external programmers can lead to better security of the device ecosystem and should be incorporated during the product development stage. Recent software update experiences highlight the importance of balancing patient safety and device security.[24] The HRS is cognizant of this challenge and during its leadership summit proceedings has advised physicians to include software update discussions during routine preimplantation visits as well as to reiterate to patients that such updates might be required during the lifetime of the device.[16] The Manufacturer and User Facility Device experience (MAUDE) database maintained by FDA, although a great resource for reporting medical device errors, is moderated by the FDA and is not entirely democratic. Reporting should be democratized with equal contributions from academic societies, physicians, and patients. This will avoid serial underreporting and provide a better understanding of cybersecurity threats. Moreover, the COVID-19 pandemic has generated increased interest from the electrophysiology community in remote programming and management of CIEDs. At present, CIEDs can only be remotely monitored and not programmed. For programming we rely on the office programmer to initiate a telemetry session using ICT, followed by RF telemetry for further interaction with the CIED (Figure 2). This added layer of security in the form of ICT and the requirement of an office programmer ensures that the CIED is programmed by authorized health care workers. The convenience of remotely programming CIEDs should be weighed against the possible hacking opportunities it provides to agents seeking to do harm. Do no harm should the guiding philosophy. A point in case is that of implantable loop recorders. These devices can be programmed remotely, and a potential hack that turns off arrhythmia detection can be deleterious. Regulatory authorities should enforce manufacturers' declarations that the mechanisms in place to ensure the remote management of device settings are safe. In most cases, device size limits the use of asymmetric cryptography and verification of downloaded data by the implanted device. Manufacturers and physicians rely on the office programmer to verify the fidelity of downloaded software and algorithms before they are pushed into the CIED during an office visit. Pushing such updates or algorithms directly to CIEDs at home over a wireless network (Wi-Fi) may not be safe as Wi-Fi networks often are not password protected.

Physician's role

Physicians should be aware of the latest security guidelines issued by device manufacturers, regulatory authorities, and society guidelines. A survey conducted in 2014 by the European Heart Rhythm Association (EHRA) on remote monitoring of CIEDs in Europe found that around 9% of the surveyed centers recognized the legal issues related to RM and data security.[25] A more recent survey by the same organization in 2019 found that 49% of respondent physicians were aware of the General Data Protection Regulation (GDPR), 61% acknowledged cybersecurity issues, and 38% undertook specific steps to address these concerns at their institution.[26] Moreover, in the same survey, 92% of respondents mentioned that their patients never or rarely voiced concerns regarding the safety of their data when their CIED was being remotely monitored. These surveys highlight the importance of physicians' knowledge of, and their role in educating patients about, CIED cybersecurity. The surveys also explored who CIED manufacturers and third-party providers perceived to be the data controller. The 5 manufacturers that were surveyed recognized health care institutions as the data controller. Only one of them recognized physicians as jointly controlling the data. In view of this finding, health care institutions should work in conjunction with manufacturers to promote data security. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) is the overarching act that protects patient data, and physicians should highlight it during office visits. Physicians should discuss HIPAA with their patients and keep them updated. Patients should be informed during the preimplantation visit as well as postimplantation follow-up visits that CIEDs require firmware updates to keep the devices safe. This continued conversation can allay patients' fear regarding firmware updates and help with better adherence to good cybersecurity practices. In addition, physicians should reiterate that although there is a theoretical risk of the device getting hacked, no such efforts have led to patient harm in the past. The CIED universe and the legalities involved vary significantly based on national and local regulations. Physicians should keep the best interest of their patient as the guiding light in their discussions and actions.

Patient's role

Data security starts with data and its ownership. As pointed out in the recent European Society of Cardiology/EHRA guidelines, based on the GDPR enforced in the European Union, patients have a right to their data and to the portability and removal of that information from the database. [26] In the United States, health data are protected by HIPAA. Although HIPAA has no discrete provisions for CIED data, the general principles of de-identifying patient data, making the data accessible to patients, and the business obligation to protect sensitive health data are in place. Moreover, multiple federal privacy bills have been introduced in Congress to widen the scope of HIPAA to include device data.[27,28] Patients should be actively involved in this process individually and through advocacy groups to promote these bills. Patients should understand the potential cybersecurity risk associated with implanted CIEDs and make an informed decision regarding implantation and care of their device. Every procedure/device comes with inherent risks and benefits, which patients should discuss with their doctor during every visit. Patients should be aware of good cybersecurity practices, including use of strong Wi-Fi passwords at home, restricting access of strangers to their home monitor, and informing the physician's office regarding any malfunction of their home monitor. Informed consent for medical devices typically does not address issues of medical device data ownership and privacy. This needs to be addressed by a consortium of medical societies, manufacturers, and patient advocacy groups. Special importance should be given to the CIED data storage and use laws in place. Such interactions will empower patients and improve their trust in CIED technology.

White hat hackers' role

As evident from the timeline of events in the Medtronic CareLink Programmers (Figure 3), there is a significant delay (in this case 1.5 years) between the time vulnerabilities are detected and corrective measures are taken. This delay can have severe health consequences for thousands of people who rely on manufacturers to fix the vulnerability. CIED manufacturers, regulatory authorities, and academic societies should work toward creating a platform for nonpunitive reporting and transparent redressal of such threats. Cybersecurity experts should be encouraged to find vulnerabilities, and white hat hacking should be an integral part of the collaborative effort. We propose conducting CIED hackathons at regular intervals. Such hackathons can be a great opportunity to troubleshoot potential lapses hidden among the maze of proprietary algorithms and antiquated OS used by these devices. Manufacturers should provide the participants with devices and source codes. White hat hackers should be incentivized to find vulnerabilities (a standard practice in Silicon Valley where companies such as Google and Facebook give monetary compensation for flaws found in their code), and manufacturers should work with them to fix any issues. The FDA and HRS should oversee such events for transparency of reporting and redressal. Patients and advocacy groups should be encouraged to participate in such events, as doing so can help them appreciate the technical complexity of the devices and the security limitations.

Conclusion

It is essential that all stakeholders, including medical device manufacturers, federal regulatory authorities, physicians, and patient advocacy groups, come together on a common platform to address cybersecurity concerns associated with CIEDs. Security should be considered at the design phase and carried forward to the implementation and postmarketing survey phases. An area of concern in postmarketing surveillance is the lack of transparency and the constant denial on the part of medical manufacturers about the security concerns raised by independent auditors and cybersecurity firms. Federal agencies, especially the FDA, should play a critical role as the gatekeeper of such discussions and should monitor companies for prompt redressal of security concerns. Involving physicians in the discussion will help foster a better understanding on their part in such security issues, which will translate into better patient communication and increase adherence to firmware and other security updates put forth by manufacturers.

References

1. Maisel WH, Paulsen JE, Hazelett MB, Selzman KA. Striking the right balance when addressing cybersecurity vulnerabilities. Heart Rhythm 2018;15:e69–e70.
2. Slotwiner D, Varma N, Akar JG, et al. HRS Expert consensus statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. Heart Rhythm 2015;12:e69–e100.
3. Arndt RZ. Hacked medical devices could wreak havoc on health systems. January 20, 2018. Modern Healthcare, https://www.modernhealthcare.com/article/20180120/NEWS/180129999/hacked-medical-devices-could-wreak-havoc-on-health-systems.
4. Federal Communications Commission. Establishment of a medical implant communications service in the 402-405 MHz Band. Federal Register 1999; 64:69926–69934.
5. Cox TJ. Frequency agile telemetry system for implantable medical device, 2004. US Patent 6,763,269.
6. Kramer DB, Baker M, Ransford B, et al. Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance. PloS One 2012;7:e40200.
7. Ricci L, Paulsen J, Browning S, et al. An overview of the security of cardiac implantable electronic devices. Pacing Clin Electrophysiol 2017;40:911–912.
8. What is hacking—Everything you need to know hackers. Malwarebytes, https://www.malwarebytes.com/hacker/.
9. Cybersecurity and Infrastructure Security Agency. ICS Advisory (ICSMA-17-241-01). Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities, https://us-cert.cisa.gov/ics/advisories/ICSMA-17-241-01.
10. Chandavarkar BR, Hardcoded credentials and insecure data transfer in IoT: National and international status. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225520.
11. Rios B. Understanding pacemaker systems cybersecurity. Available at http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html. Accessed November 13, 2020.
12. Hei X, Du X, Wu J, Hu F. Defending resource depletion attacks on implantable medical devices. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL; 2010, pp. 1–5, doi: 10.1109/GLOCOM.2010.5685228.
13. National Institute of Standards and Technology. National Vulnerability Database NVD-CVE-2018-10596 Detail. July 2, 2018, https://nvd.nist.gov/vuln/detail/CVE-2018-10596.
14. MW is short St. Jude Medical (STJ: US). August 25, 2016. Muddy Waters LLC, https://www.muddywatersresearch.com/research/stj/mw-is-short-stj/.
15. Kapoor A, Vora A, Yadav R. Cardiac devices and cyber attacks: how far are they real? How to overcome? Indian Heart J 2019;71:427–430.
16. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit. Heart Rhythm 2018;15:e61–e67.
17. Newman LH. A new pacemaker hack puts malware directly on the device, https://www.wired.com/story/pacemaker-hack-malware-black-hat/. Accessed January 21, 2021.
18. Goodin D. Hack causes pacemakers to deliver life-threatening shocks, https://arstechnica.com/information-technology/2018/08/lack-of-encryption-makes-hacks-on-life-saving-pacemakers-shockingly-easy/.
19. US Food and Drug Administration. Cybersecurity vulnerabilities affecting Medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication, https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.
20. Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Expert Rev Med Devices 2018;15:403–406.
21. Longevity estimator software error for subset of Medtronic CIEDs. Heart Rhythm Society, https://www.hrsonline.org/guidance/safety-alerts/longevity-estimator-software-error-subset-medtronic-cieds.
22. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. Pacing Clin Electrophysiol 2017; 40:913–917.
23. Slotwiner DJ, Abraham RL, Al-Khatib SM, et al. HRS White Paper on interoperability of data from cardiac implantable electronic devices (CIEDs). Heart Rhythm 2019;16:e107–e127.
24. Baranchuk A, Alexander B, Campbell D, et al. Pacemaker cybersecurity: local experience with a firmware upgrade. Circulation 2018;138:1272–1273.
25. Hernández-Madrid A, Lewalter T, Proclemer A, Pison L, Lip GY, Blomstrom-Lundqvist C. Remote monitoring of cardiac implantable electronic devices in Europe: results of the European Heart Rhythm Association survey. Europace 2014; 16:129–132.
26. Nielsen JC, Kautzner J, Casado-Arroyo R, et al. Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles—ESC Regulatory Affairs Committee/EHRA Joint Task Force Report. Europace 2020 Jul 29;:euaa168.
27. Bailin P. Executive summary: evolution of health data regulation. April 1, 2019, https://medium.com/datavant/executive-summary-evolution-of-health-data-regulation-faa5fbb4dc3c.
28. Ger M. Meeting medical device data privacy, governance, and security challenges, https://blog.cloudera.com/meeting-medical-device-data-privacy-governance-and-security-challenges/.