JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY VOL. 71, NO. 11, 2018
© 2018 BY THE AMERICAN COLLEGE OF CARDIOLOGY FOUNDATION
PUBLISHED BY ELSEVIER

CARDIOVASCULAR MEDICINE AND SOCIETY

Cybersecurity for Cardiac Implantable Electronic Devices

What Should You Know?

Adrian Baranchuk, MD,[a] Marwan M. Refaat, MD,[b] Kristen K. Patton, MD,[c] Mina K. Chung, MD,[d] Kousik Krishnan, MD,[e] Valentina Kutyifa, MD, PhD,[f] Gaurav Upadhyay, MD,[g] John D. Fisher, MD,[h] Dhanunjaya R. Lakkireddy, MD,[i] from the American College of Cardiology's Electrophysiology Section Leadership

ABSTRACT

Medical devices have been targets of hacking for over a decade, and this cybersecurity issue has affected many types of medical devices. Lately, the potential for hacking of cardiac devices (pacemakers and defibrillators) claimed the attention of the media, patients, and health care providers. This is a burgeoning problem that our newly electronically connected world faces. In this paper from the Electrophysiology Section Council, we briefly discuss various aspects of this relatively new threat in light of recent incidents involving the potential for hacking of cardiac devices. We explore the possible risks for the patients and the effect of device reconfiguration in an attempt to thwart cybersecurity threats. We provide an outline of what can be done to improve cybersecurity from the standpoint of the manufacturer, government, professional societies, physician, and patient. (J Am Coll Cardiol 2018;71:1284–8) © 2018 by the American College of Cardiology Foundation.

The Internet of things (IOT) is the connected communication medium in which we all live. IOT brought our professional and personal lives onto a singular platform. The ability to control so many aspects of modern existence with the click of a button on your smart device is efficient and useful, but it comes with a price. IOT security concerns have been a persistent issue, particularly in technologically adept communities, but the explosion of connected devices used in everyday life has markedly increased the risks of inadequate cybersecurity. Hacking is defined as unauthorized access to a computer system to gain information or create problems within the system (1). At present, computer-savvy hackers have intruded into most areas of the IOT space. A Google search of "hacking + [devices such as refrigerators, baby monitors, TVs]" provides multiple interesting and/or concerning results (1,2). This brief perspective from the American College of Cardiology's Electrophysiology Council is intended

The views expressed in this paper by the American College of Cardiology's (ACC's) Electrophysiology Section Leadership Group do not necessarily reflect the views of the *Journal of the American College of Cardiology* or the ACC.

From the [a]Electrophysiology Section, Division of Cardiology, Queen's University, Kingston, Ontario, Canada; [b]Electrophysiology Section, Division of Cardiology, American University of Beirut, Beirut, Lebanon; [c]Electrophysiology Section, Division of Cardiology, University of Washington, Seattle, Washington; [d]Electrophysiology Section, Division of Cardiology, Department of Cardiovascular Medicine, Heart & Vascular Institute, Cleveland Clinic, Cleveland, Ohio; [e]Electrophysiology Section, Division of Cardiology, Rush University Medical Center, Chicago, Illinois; [f]Electrophysiology Section, Division of Cardiology, University of Rochester Medical Center, Rochester, New York; [g]Electrophysiology Section, Division of Cardiology, University of Chicago, Chicago, Illinois; [h]Electrophysiology Section, Division of Cardiology, Albert Einstein College of Medicine, New York, New York; and the [i]Electrophysiology Section, Division of Cardiology, University of Kansas, Kansas City, Kansas. Dr. Chung has received honoraria from UpToDate; has received research support from Zoll; and has served on the EPIC Alliance steering committee for Biotronik (uncompensated). Dr. Krishnan has served as a clinical trial principal investigator for St. Jude Medical. Dr. Kutyifa has received research grants from Boston Scientific and Zoll. Dr. Upadhyay has received research support from Medtronic and Biotronik. Dr. Fisher has served as a consultant to Medtronic; and has received fellowship support from Medtronic, Abbott, and Biotronik. Dr. Lakkireddy has served as a speaker for Janssen, Pfizer, and Biotronik; and has received unrestricted research grants from Bristol-Myers Squibb and Biosense Webster. All other authors have reported that they have no relationships relevant to the contents of this paper to disclose.

Manuscript received October 18, 2017; revised manuscript received December 15, 2017, accepted January 10, 2018.

ISSN 0735-1097/$36.00 https://doi.org/10.1016/j.jacc.2018.01.023

to clarify issues that have recently arisen with respect to cybersecurity in cardiovascular implantable electronic devices (CIEDs).

CYBERSECURITY IN MEDICAL DEVICES

A global definition of cybersecurity includes "the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (3). In the medical field, cybersecurity refers specifically to the integration of medical devices, computer networks, and software (1). True cybersecurity begins at the point of designing protected software from the outset, and requires the integration of multiple stakeholders, including software experts, security experts, and medical advisors (1-3). Common reasons for hacking and modes of attack are summarized in the **Central Illustration**.

Many different medical devices have been targets of hacking for over a decade. Outside of the CIED world, some of the more notable are:

- Insulin pump hacking: a remote "hacking attack" was publicly demonstrated in both a Medtronic device (4) and a Johnson & Johnson device (5); and
- Drug infusion pumps.

The increasing number of medical devices using software has created a new cybersecurity concern in the medical industry—how can we protect devices from intentional harmful interference in their normal functioning (1)? Advanced wireless communications between health care providers and patients' devices have created the possibility of manipulating the normal interactions, including deactivating features; delaying, interfering, or interrupting communications; and altering programming. This poses a potential risk to clinical care, as patients could be harmed by the action of a malignant or inadvertent deleterious change in programming by the "hackers" (2).

CYBERSECURITY ISSUES IN CIEDs. In August of 2016, Muddy Waters Research LLC released a short-sell report maintaining that CIEDs manufactured by St. Jude Medical (now Abbott) were at high risk for medical device hacking (6). The report, written in collaboration with MedSec (Miami, Florida), a cybersecurity research firm focused on health care, details 2 types of cybersecurity breach, using screenshots as evidence: a "crash attack" leading to high rate pacing, and a battery drain attack (6). A major claim was that radiofrequency telemetry with the Merlin@home remote monitoring system (St. Jude Medical, now Abbott, St. Paul, Minnesota) was rendered incapable of communication after bombardment with radio traffic. An attempt to reproduce the "Muddy Waters" conditions by a group of researchers failed to produce any clinical harm; although telemetry could be inhibited, presumably to protect battery, there was no effect on essential device function (7). The motivation for the study and release of information does not appear to have been focused on patient safety, based on the public release of information without informing either the Food and Drug Administration (FDA) or the manufacturer prior to releasing the report (7). However, a warning letter was issued by the FDA (8) to Abbott urging the firm to increase cybersecurity based on the Muddy Waters report and the detection of areas of vulnerability in their remote monitoring system. Although the weaknesses in the integrity of cybersecurity for medical devices is obvious, its perceived effect on patients' safety by all "key players" (device industry, software designers, security researchers, agencies, and clinical health care providers) has not been the same.

ABBREVIATIONS AND ACRONYMS

CIED = cardiovascular implantable electronic device

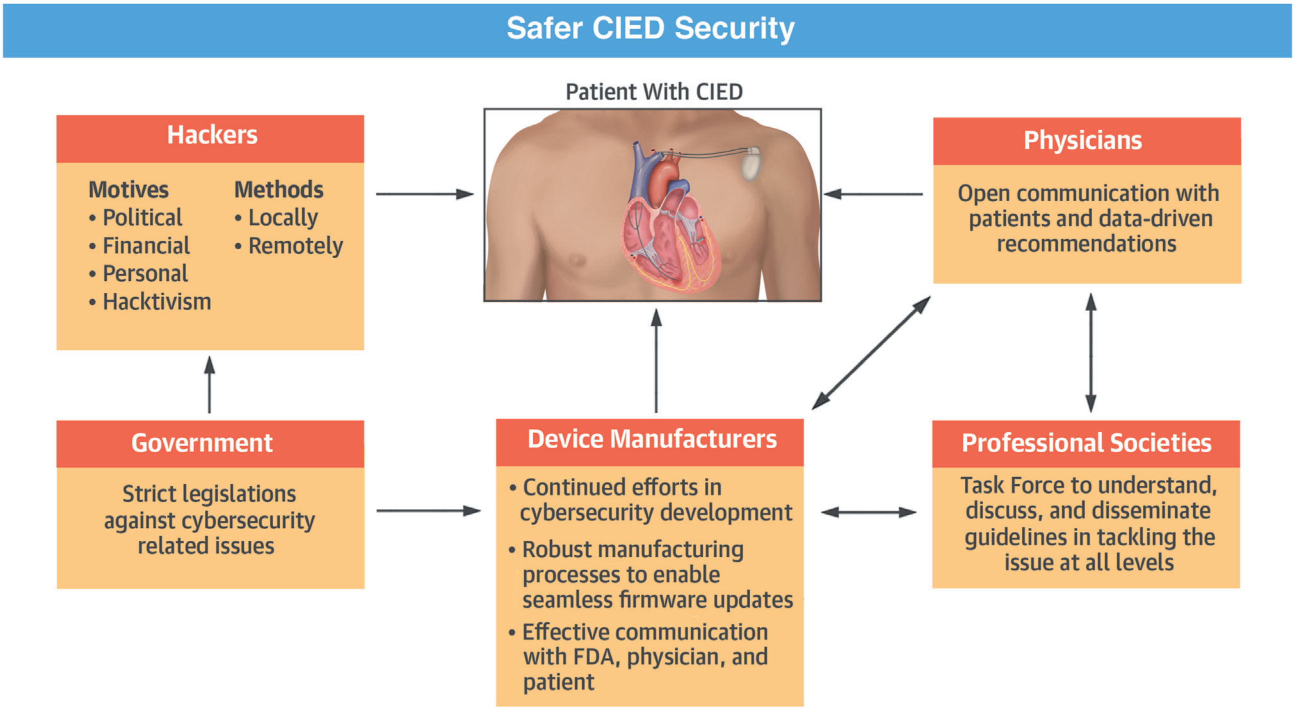
FDA = Food and Drug Administration

IOT = Internet of things

POTENTIAL CLINICAL CONSEQUENCES OF PACEMAKER HACKING. Patient safety issues with respect to pacemakers are largely confined to those resulting from oversensing or the potential of sudden battery depletion (**Table 1**). As happens with other causes of electromagnetic interference (radiation therapy, electrocautery, and welding) the detection of signals of noncardiac origin may inhibit pacing, inducing prolonged periods of asystole with the consequent risk of syncope or sudden death. Sudden battery depletion is also most clinically relevant in a pacing-dependent patient.

POTENTIAL CLINICAL CONSEQUENCES OF IMPLANTABLE CARDIOVERTER-DEFIBRILLATOR HACKING. Security vulnerabilities exist in all software. The same areas of vulnerability in pacemakers also apply to implantable cardioverter-defibrillators. Interrupting wireless communications (remote monitoring) would be possible for a hacker operating in the same radiofrequency as the medical device, and interruption of communication would inhibit the value of telemonitoring and allow any clinically relevant events to go undetected by the system. In a pacing-dependent patient with an implantable cardioverter-defibrillator, oversensing may inhibit pacing. In addition, oversensing may result in inappropriate and even life-threatening shocks. If reprogramming was performed, disabling therapies (antitachycardia pacing and shocks) would result in no response from the device upon clinical life-threatening ventricular tachycardias. Inducing

CENTRAL ILLUSTRATION Interaction Amongst Various Stake Holders in Addressing the Cybersecurity Issue



Safer CIED Security

Patient With CIED

Hackers

Motives
- Political
- Financial
- Personal
- Hacktivism

Methods
- Locally
- Remotely

Physicians

Open communication with patients and data-driven recommendations

Government

Strict legislations against cybersecurity related issues

Device Manufacturers

- Continued efforts in cybersecurity development
- Robust manufacturing processes to enable seamless firmware updates
- Effective communication with FDA, physician, and patient

Professional Societies

Task Force to understand, discuss, and disseminate guidelines in tackling the issue at all levels

Baranchuk, A. et al. J Am Coll Cardiol. 2018;71(11):1284–8.

CIED = cardiovascular implantable electronic device; FDA = Food and Drug Administration.

arrhythmias via noninvasive programmed stimulation could be also be a potential risk. Sudden battery depletion remains a clinical concern in pacing-dependent patients due to the inability to deliver therapies during clinical life-threatening arrhythmias (Table 1).

TABLE 1 Areas of Vulnerability in Pacemakers and ICDs

Type of Vulnerability	Pacemakers	ICDs
Sensing	Oversensing can be critical in pacing-dependent patients	Oversensing can be critical in pacing-dependent patients
Overdrive pacing	++	+++
Sudden battery depletion	Critical in pacing-dependent patients	Critical in pacing-dependent patients. Inability to deliver therapies (ATP/shock) if needed
Interruption of wireless communications	+++	+++

ATP = antitachycardia pacing; ICD = implantable cardioverter-defibrillator.

WHAT ARE THE EXISTING FEDERAL OR INTERNATIONAL GUIDELINES ON CYBERSECURITY FOR MEDICAL DEVICES?

This is a very complicated question, and the answer is evolving rapidly. The FDA has issued both pre- and post-market guidance for the security of medical devices. The guidance references other standards from the National Institute of Standards and Technology and International Organization for Standards. China is an example of another country that has communicated standards regarding the security of medical devices. A number of recent legislative proposals related to medical device security have been advanced in the U.S. Congress.

HOW TO REDUCE THE RISK OF HACKING?

A secure system lifecycle approach begins at the conception of device development and continues through manufacture and post-implant monitoring. Cybersecurity needs should also be addressed during both pre- and post-market product testing. As cyber vulnerabilities can emerge quickly, strong postmarket processes must be in place to monitor the environment for new vulnerabilities and to respond in a timely manner. In current-generation devices that have theoretical or known vulnerabilities, firmware is useful (defined as a kind of software that is embedded in the hardware of a technological device requiring updates from time to time). Remote monitoring or interrogation of all telemonitored devices is possible, because all CIEDs being followed remotely already communicate with the manufacturer's web site.

At this time, there is no evidence that one can reprogram a CIED or change device settings in any form. The likelihood of an individual hacker successfully affecting a CIED or being able to target a specific patient is low. A more likely scenario is that of a malware or ransomware attack affecting a hospital network and inhibiting communication (**Central Illustration**). In this case, loss of remote communication may prevent timely transmission of a clinical event. If this scenario occurs, an in-person appointment may be required to restore communication with the device and patient; this may not be convenient for patients living in remote locations.

WHAT SHOULD PATIENTS DO IN LIGHT OF THE RECENT ABBOTT FIRMWARE UPDATE NOTICE?

Abbott has placed patient resources on their web site (9). Affected patients can reach out to their cardiologists/electrophysiologists to discuss. The recent Abbott firmware update takes approximately 3 min to complete, and places the patient at VVI 67 beats/min. The risk of CIED malfunction due to the update is estimated as: complete loss of function (0.003%), loss of device settings (0.023%), and failure of update (0.161%) (9). Thus far, there have been no actual clinical reports of malicious or inadvertent hacking or malware attacks affecting CIEDs. Most believe the risk of the software update is far outweighed by the theoretic risk of a cybersecurity breach.

IS THIS JUST A PROBLEM WITH ABBOTT CIEDs, OR ARE THERE SIMILAR VULNERABILITIES IN OTHER MANUFACTURERS' PLATFORMS?

Based on research into failure modes, this is not a problem restricted to Abbott. The risks exist for any device that is connected to the Internet. Outside of the realm of CIED management, these issues obviously also apply to other medical devices (pain pumps, insulin pumps, continuous positive airway pressure, and rhythm and hemodynamic monitoring) that are connected to the Internet for remote monitoring and programming purposes.

WHAT SHOULD PHYSICIANS ADVISE? IS THE RISK OF DEVICE FAILURE FROM FIRMWARE UPDATE MUCH MORE SIGNIFICANT THAN THE HYPOTHETICAL "HACKING" RISK?

Physicians who manage CIEDs should be aware of both documented and possible cybersecurity risks. Systems should be established to communicate updates in these areas quickly and in an understandable way to the rest of the clinical team that manages patients with devices. Policies and procedures for these communications may be informed by the clinic's prior response to FDA device recalls. There are a variety of resources available through Abbott specifically addressing the cybersecurity issue in their press release and their web site (9). Clinics and hospitals should review security updates and be aware of the issues at hand. Patients should be engaged in the conversation, and a shared decision is critical. At this point in time, the Electrophysiology Council feels that no enhanced monitoring or elective device replacement is necessary. The overall effect of firmware is yet to be understood.

WHAT IS THE FUTURE EFFECT ON MANUFACTURING, POLICY, AND PENALTIES?

Not all CIEDs are the same, and the potential outcome of hacking depends on both the kind of device and the patient's dependence. The fewer remote interactions with a device, the less chances exist for hackers to disrupt the communications. However, given the lack of evidence that hacking is a relevant clinical problem, coupled with evidence of the benefits of remote monitoring, one should exercise caution in depriving a patient of the clear benefit of remote monitoring (10).

The possible future effect of this issue is immense. The FDA, manufacturers, and professional societies like the American College of Cardiology and Heart Rhythm Society are actively participating in larger conversations regarding overall risks and how to best protect patients and provide the most effective care. This is an evolving area of medical care and legal regulation, which will continue to progress rapidly. We should all stay tuned.

ADDRESS FOR CORRESPONDENCE: Dr. Dhanunjaya R. Lakkireddy, Cardiovascular Research Institute, University of Kansas Hospital and Medical Center, MS 4023, 3901 Rainbow Boulevard, Kansas City, Kansas 66160. E-mail: dlakkireddy@kumc.edu.

REFERENCES

1. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckl) 2015;8:305–16.

2. Clery D. The privacy arms race. Could your pacemaker be hackable? Science 2015; 347:499.

3. Lewis JA. Cybersecurity and critical infrastructure protection. 2006. Available at: http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf. Accessed September 3, 2017.

4. Takahashi D. Insulin pump hacker says vendor Medtronic is ignoring security risk. Available at: https://venturebeat.com/2011/08/25/insulin-pump-hacker-says-vendor-medtronic-is-ignoring-security-risk. Accessed September 3, 2017.

5. Rockoff JD. J&J warns insulin pump vulnerable to cyber hacking. The Wall Street Journal. Available at: https://www.wsj.com/articles/j-j-warns-insulin-pump-vulnerable-to-cyber-hacking-1475610989. Accessed September 3, 2017.

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/. Accessed August 30, 2016.

7. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. Pacing Clin Electrophysiol 2017;40:913–7.

8. U.S. Food and Drug Administration. Cybersecurity vulnerabilities identified in St. Jude Medical's implantable cardiac devices and Merlin@home transmitter: FDA safety communication. Available at: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. Accessed September 3, 2017.

9. Abbott. Cybersecurity update: cybersecurity: your safety is our top priority. Available at: https://www.sjm.com/cyberupdate. Accessed September 3, 2017.

10. Ladapo JA, Turakhia MP, Ryan MP, Mollenkopf SA, Reynolds MR. Health care utilization and expenditures associated with remote monitoring in patients with implantable cardiac devices. Am J Cardiol 2016;117:1455–62.

KEY WORDS cardiac implantable electronic devices, cybersecurity, hacking, remote monitoring