Medical Xpress

Can your cardiac device be hacked?

February 20 2018

Credit: CC0 Public Domain

Medical devices, including cardiovascular implantable electronic devices could be at risk for hacking. In a paper publishing online today in the *Journal of the American College of Cardiology*, the American College of Cardiology's Electrophysiology Council examines the potential risk to patients and outlines how to improve cybersecurity in these devices.

Cybersecurity in the medical field refers to the integration of medical devices, computer networks and software. While there have been no actual clinical reports of malicious or inadvertent hacking or malware attacks affecting cardiac devices, recent reports have discovered this possibility. Reasons for hacking include political, financial, social and personal motives. Devices can be hacked locally or remotely. The Food and Drug Administration has issued both pre-market and post-market guidance for the security of medical devices and legislative proposals related to medical device security have been advanced in the U.S. Congress.

"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," said Dhanunjaya R. Lakkireddy MD, professor of medicine at the University of Kansas Hospital, a member of the Electrophysiology Council and the corresponding author of the paper.

Medical devices have been targets of hacking for over a decade. The increasing number of medical devices using software has created the need to protect devices from intentional harmful interference on their normal functioning. Advanced wireless communications between health care providers and patients' devices have created the theoretical possibility for the deactivation of features, the alteration of programming, and the delaying, interfering or interrupting of communications.

There are a number of possible clinical consequences that may result from the hacking of a cardiac device. In patients with pacemakers, concerns mostly consist of oversensing or battery depletion. For patients with implantable cardioverter-defibrillators (ICDs), it is possible for hackers to interrupt wireless communications, inhibiting the value of telemonitoring and allowing any clinically relevant events to go undetected by the system. Oversensing may inhibit pacing or result in inappropriate or life-threatening shocks. Battery depletion can lead to a device being unable to deliver therapies during life-threatening arrhythmias.

"At this time, there is no evidence that one can reprogram a cardiovascular implantable electronic device or change device settings in any form," Lakkireddy said. "The likelihood of an individual hacker successfully affecting a cardiovascular implantable electronic device or being able to target a specific patient is very low. A more likely scenario is that of a malware or ransomware attack affecting a hospital network and inhibiting communication."

The council said that cybersecurity needs should also be addressed during product testing both pre- and post-market. Because cyber vulnerabilities can emerge quickly, strong post-market processes must be in place to monitor the environment for new vulnerabilities and to respond in a timely manner. The council suggests that firmware may be useful in devices with possible vulnerabilities. Physicians who manage cardiac devices 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 manage patients with devices.

The council members said they do not feel that enhanced monitoring or elective device replacement is necessary at this time.

"Given the lack of evidence that hacking of cardiac devices 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," Lakkireddy said.

More information: *Journal of the American College of Cardiology*

(2018). DOI: 10.1016/j.jacc.2018.01.023

Provided by American College of Cardiology

Citation: Can your cardiac device be hacked? (2018, February 20) retrieved 25 April 2024 from https://medicalxpress.com/news/2018-02-cardiac-device-hacked.html