Paper evaluates hacking vulnerabilities in pacemaker systems

May 30 2017, by Nancy Owano

Credit: CC0 Public Domain

(Tech Xplore)—What's wrong with pacemakers? Actually, the issue of security gets to the heart of the matter.

The recent paper everyone is talking about is from WhiteScope. They send up signals that pacemaker systems need to address challenges in security. WhiteScope's report did not show high marks for security in these devices.

The May 17 paper is "Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies" by Billy Rios and Jonathan Butts, PhD. What did they hope to accomplish? They went in for a security evaluation on the implantable cardiac device "ecosystem."

They obtained physician programmers, home monitoring devices and implantable cardiac devices for four implantable cardiac device vendors. Conceptually, they wrote, the vendors use a similar architecture framework.

Results: They found potential security risks stemming from underlying protocols and system-to-system communications involving embedded devices.

In a WhiteScope IO blog entry, Rios noted, "Pacemaker systems are 'system-of-systems'. Looking at all four manufacturers, there are essentially four components to modern pacemaker system deployments: the pacemaker devices, pacemaker programmers, home monitoring systems, and the supporting/update infrastructure. All components are vital to the safe functioning of the pacemaker system."

According to the BBC, Rios said "all the problems he and his co-workers uncovered had been reported to the US Department of Homeland Security, which oversees companies that make medical devices."

Threatpost said the paper described a list of cybersecurity issues regarding devices built by manufacturers.

For example, in their look at programmers built by different vendors, they discovered vulnerabilities associated with outdated libraries and software in the pacemaker programmers.

Posted in December last year, Suzanne Schwartz, M.D., M.B.A., wrote in *FDA Voice* that "Digital connections power great innovation—and medical device cybersecurity must keep pace with that innovation. The same innovations and features that improve health care can increase cybersecurity risks. This is why we need all stakeholders in the medical device ecosystem to collaborate to simultaneously address innovation and cybersecurity."

In implementing a program to manage cybersecurity risks, she wrote, manufacturers should, among other things, have a way to monitor and detect cybersecurity vulnerabilities in their devices; establish a process for working with researchers and other stakeholders to get information about potential vulnerabilities ("coordinated vulnerability disclosure policy"); and deploy mitigations (e.g., software patches) to address issues early, before they can be exploited and cause harm.

Dan Goodin in *Arts Technica* commented. Such attacks would not provide "the kind of easy profits that motivate more traditional hacking crimes. Still, there's something unsettling about life-critical medical devices lacking the kinds of security precautions that come standard in many smartphones."

More information: Full report: drive.google.com/file/d/0B_Gsp … YkJfaVlBeGVCSW8/view

Citation: Paper evaluates hacking vulnerabilities in pacemaker systems (2017, May 30) retrieved