MedicalXpress

Holes found in report on St. Jude medical device security

August 31 2016

A recent report that alleges security flaws in St. Jude Medical's pacemakers and other life-saving medical devices has major flaws of its own, University of Michigan researchers say.

The U-M researchers have reproduced experiments that led to the allegations and come to strikingly different conclusions. The team is composed of several leading medical device security researchers and a cardiologist from the U-M Health System's Frankel Cardiovascular Center.

The unorthodox report that alleged the security flaws was released last week by short-selling investment research firm Muddy Waters Capital LLC and medical device security firm MedSec Ltd.

The U-M team reproduced error messages the report cites as evidence of a successful "crash attack" into a home-monitored implantable cardiac defibrillator. But the messages are the same set of errors that display if the device isn't properly plugged in.

"We're not saying the report is false. We're saying it's inconclusive because the evidence does not support their conclusions. We were able to generate the reported conditions without there being a security issue," said Kevin Fu, U-M associate professor of computer science and engineering and director of the Archimedes Center for Medical Device Security. Fu is also co-founder of medical device security startup Virta Labs.

When it's implanted, a defibrillator's electrodes are connected to heart tissue via wires that are woven through blood vessels. Through these wires, implantable defibrillators can perform sensing operations and also send shocks if necessary.

"When these wires are disconnected, the device generates a series of error messages: two indicate high impedance, and a third indicates that the pacemaker is interfering with itself," said Denis Foo Kune, former U-M postdoctoral researcher and co-founder of Virta Labs.

On page 17 of the Muddy Waters report, a screenshot cites these error messages as proof of a security breach.

"But really, we believe the pacemaker is acting correctly," Fu said. "To the armchair engineer it may look startling, but to a clinician it just means you didn't plug it in. In layman's terms, it's like claiming that hackers took over your computer, but then later discovering that you simply forgot to plug in your keyboard."

Ethicists and other researchers have criticized MedSec's technique of teaming with a short-seller to publicize its findings and benefit financially in the process. Short-selling is an investment practice that essentially involves betting that a particular stock will decline in value. If it does, then the investment firm profits. In this case, MedSec made a deal with Muddy Waters to share profits. St. Jude's stock fell sharply last week.

To conduct the medical device experiments, the U-M team used a new, properly functioning model of the defibrillator that the Muddy Waters study used—the Fortify Assura VR. In several additional instances, they say the device operated properly.

Even while the U-M researchers find fault with the Muddy Waters

report, they don't mean to suggest that these medical devices—or any medical devices for that matter—are necessarily secure. It's important to establish security workflows early on in the design process of medical devices, says Fu, who co-leads the $10 million National Science Foundation-funded Trustworthy Health and Wellness Project.

"While medical device manufacturers must improve the security of their products, claiming the sky is falling is counterproductive," Fu said. "Health care cybersecurity is about safety and risk management, and patients who are prescribed a medical device are far safer with the device than without it."

The team is continuing to investigate the claims in the Muddy Waters report and may have additional findings to report soon.

Dr. Thomas Crawford, U-M assistant professor of internal medicine, a cardiologist and a clinical electrophysiologist, agrees. Crawford implants and follows patients with pacemakers and implantable defibrillators.

"Given the significant benefits from home monitoring, patients should continue to use their prescribed cardiac devices while independent researchers investigate the claims made by MedSec and their financial partner Muddy Waters Capital LLC," he said.

Crawford adds that home monitoring has been shown to reduce a variety of adverse events, with some studies even showing reduction in overall mortality over periodic checks of devices in the doctor's office. The devices can send alerts to a central monitoring service, which then is forwarded to the physician, so that it can be dealt with immediately, if necessary.

Provided by University of Michigan