Uploaded to the VFC Website

2018

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of "Frequently Asked Questions, please go to:

Veterans-For-Change

If Veterans don't help Veterans, who will?

Note: VFC is not liable for source information in this document, it is merely provided as a courtesy to our members & subscribers.

UA researcher developing new technology to detect malware in implantable medical devices

March 10, 2017

Nearly a million new forms of malware are unleashed on the world every day. Manufacturers of software for smartphones, laptops and security cameras, as well as banks, retailers and government agencies, release upgrades frequently to try to protect customers and assets.

Yet the millions of people with implanted medical devices typically never receive software upgrades to address security vulnerabilities for the gadgets in their bodies.

"It used to be we only had to worry about breaches of our computers and smartphones," said Roman Lysecky, an associate professor in the University of Arizona Department of Electrical and Computer Engineering. "Industry analysts predict that by 2020 most of the 20 billion electronic devices on the market will be interconnected -- and millions of these will be implantable medical devices."

Like other modern electronics, implantable medical devices are connected through the internet or wireless technologies. They include cardiac pacemakers and defibrillators for people with arrhythmia, insulin pumps for people with diabetes and brain neurostimulators for people with Parkinson's disease.

Many IMDs have sensors to monitor vital signs such as heart rate and transmit data to healthcare providers' computers in real time. Doctors can evaluate patients remotely and, with a few simple adjustments, improve their conditions or even save their lives.

But along with their benefits, IMDs pose risks.

Hackers who gain access to confidential patient information could use malware as "ransomware." Worse, they could put a patient with an implanted cardiac pacemaker -- there are more than 225,000 such people in the United States alone - into cardiac arrest.

"This hasn't happened yet to our knowledge," said Lysecky, an expert in connected, or embedded, electronic systems who is leading two federally

funded projects to reduce cybersecurity risks in pacemakers and other biomedical devices. "But security researchers have proved it is possible."

Good Timing

Lysecky is pioneering technologies to enable IMDs to detect malware and help ensure they will continue functioning properly in a patient when their security is breached. He has built a prototype of a network-connected pacemaker and is running experiments based on case studies of malware infecting other types of embedded systems.

In one project funded by the National Science Foundation, he and co-principal investigator Jerzy Rozenblit, UA Distinguished Professor and Oglethorpe Endowed Chair in the Department of Electrical and Computer Engineering and professor of surgery in the College of Medicine, are developing runtime anomaly detection.

This technology exposes minuscule changes in the timing of how computations and data are transmitted from the pacemaker to a cardiac data log, revealing the potential presence of malware.

A pacemaker might be engineered to send data to the patient's digital cardiac log every three milliseconds or to send specific types of data, such as ventricular or atrial readings, in less than 10 milliseconds. Any aberrations in these precisely timed processes could signal the presence of malware. The changes would immediately alert a doctor, who could then take action remotely, possibly with the patient never knowing of the harm averted.

Lysecky, recipient of a prestigious NSF Early Career Award, is also looking for malware mimicry, whereby hackers tweak functioning of IMDs in subtle ways to avoid detection.

His team, including doctoral students Sixing Lu and Minjun Seo, achieved a 100-percent detection rate for mimicry malware using runtime anomaly detection in the prototype pacemaker system. The researchers reported their findings for the 2015 Workshop on Embedded Systems Security and in the Institute of Electrical and Electronics Engineers' Embedded Systems Letters in 2016.

Pressure Building for Regulations

Pacemakers are not yet required to have built-in detection and mitigation capabilities, but pressure is building.

"As a cardiologist, I have seen an increase in patient awareness of security issues about their implanted devices in the digital realm," said Dr. Peter Ott, an associate professor in the UA College of Medicine Sarver Heart Center who has collaborated with Lysecky and Rozenblit and routinely implants cardiac pacemakers and defibrillators in patients. "I expect such concerns will grow."

The U.S. Food and Drug Administration has identified hundreds of medical devices infected by malware and first published recommendations in October 2014 for manufacturers to consider software protections throughout a product's lifecycle. In December 2016 the agency issued security guidelines encouraging pacemaker manufacturers to regularly monitor, maintain and update software.

"We believe manufacturers should build implantable medical devices like pacemakers with malware detection strategies from the get-go, and provide patches as future problems develop," said Lysecky, who is looking toward clinical trials of his runtime anomaly detection system at Banner-University Medical Center Tucson in the coming years.

Thwarting Hackers from Every Angle

Lysecky is working on another project, with a grant from the Army Research Office, to make medical implants more resistant to side-channel attacks. He and co-principal investigator Janet Meiling Roveda, UA professor of electrical and computer engineering, are developing mathematical models to analyze changes not only in timing, but also in power consumption and electromagnetic radiation.

"Side-channel attacks like these are a critical threat to the security of embedded systems," Lysecky said. "By analyzing data transmission timing, power consumption and electromagnetic radiation from a life-critical device such as a pacemaker, a hacker can extract data like cryptographic keys that are essential for shielding communications from unauthorized users."

Source:

University of Arizona College of Engineering