New Password in a Heartbeat

Rice University

Rice University researchers propose touch-to-access security for implanted devices

Pacemakers, insulin pumps, defibrillators and other implantable medical devices often have wireless capabilities that allow emergency workers to monitor patients. But these devices have a potential downside: They can be hacked.

Researchers at Rice University have come up with a secure way to dramatically cut the risk that an implanted medical device (IMD) could be altered remotely without authorization.

Their technology would use the patient's own heartbeat as a kind of password that could only be accessed through touch.

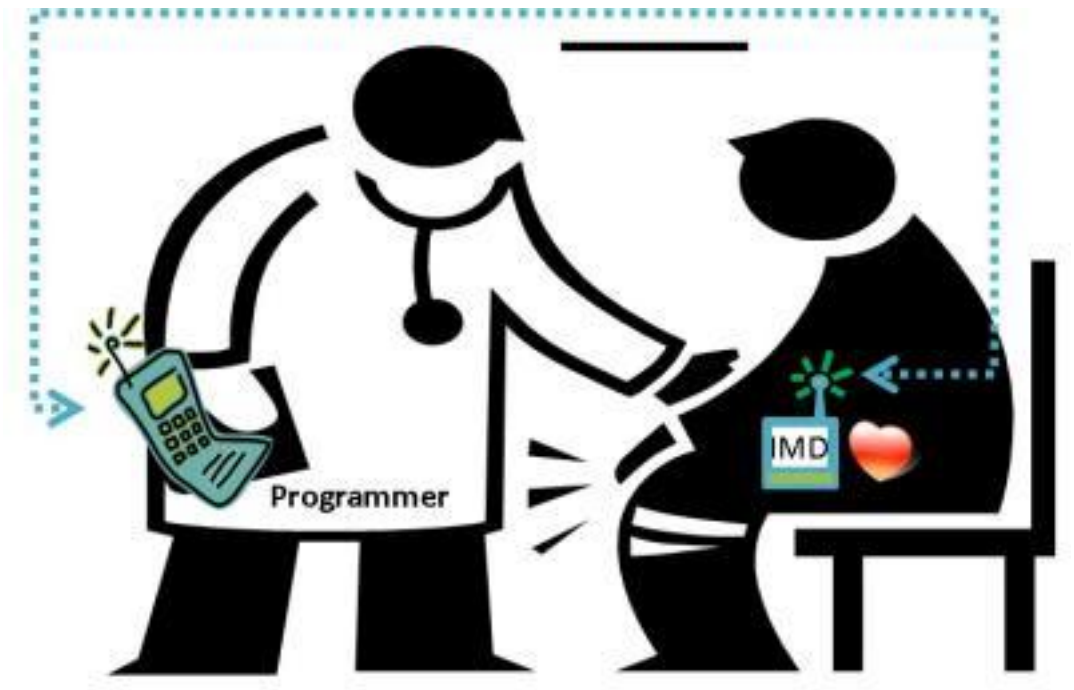
Rice electrical and computer engineer Farinaz Koushanfar and graduate student Masoud Rostami will present Heart-to-Heart, an authentication system for IMDs, at the Association for Computing Machinery's Conference on Computer and Communications Security in Berlin in November. They developed the technology with Ari Juels, former chief scientist at RSA Laboratories, a security company in Cambridge, Mass.

IMDs generally lack the kind of password security found on a home Wi-Fi router because emergency medical technicians often need quick access to the information the devices store to save a life, Rostami said. But that leaves the IMDs open to attack.

"If you have a device inside your body, a person could walk by, push a button and violate your privacy, even give you a shock," he said. "He could make (an insulin pump) inject insulin or update the software of your pacemaker. But our proposed solution forces anybody who wants to read the device to touch you."

The system would require software in the IMD to talk to the "touch" device, called the programmer. When a medical technician touches the patient, the programmer would pick up an electrocardiogram (EKG) signature from the beating heart. The internal and external devices would compare minute details of the EKG and execute a "handshake." If signals gathered by both at the same instant match, they become the password that grants the external device access.

"The signal from your heartbeat is different every second, so the password is different each time," Rostami said. "You can't use it even a minute later."



He compared the EKG to a chart of a financial stock. "We're looking at the minutia," Rostami said. "If you zoom in on a stock, it ticks up and it ticks down every microsecond. Those fine details are the byproduct of a very complex system and they can't be predicted."

A human heartbeat is the same, he said. It seems steady, but on closer view every beat has unique characteristics that can be read and matched. "We treat your heart as if it were a random number generator," he said.

The system could potentially be used with the millions of IMDs already in use, Koushanfar said. "To our knowledge, this is the first fully secure solution that has small overhead and can work with legacy systems," she said. "Like any device that has wireless access, we can simply update the software."

Koushanfar noted the software would require very little of an IMD's precious power, unlike other suggested secure solutions that require computationally intensive –

and battery draining – cryptography. "We're hopeful," she said. "We think everything here is a practical technology."

Implementation would require cooperation with device manufacturers who, Koushanfar said, hold their valuable, proprietary secrets very close to the chest, as well as approval by the Food and Drug Administration.

But the time to pursue IMD security is here, Rostami insisted. "People will have more implantable devices, not fewer," he said. "We already have devices for the heart and as insulin pumps, and now researchers are talking about putting neuron stimulators inside the brain. We should make sure all these things are secure."

For more information, visit Rice University [1].

Source URL (retrieved on *04/01/2015 - 11:11pm*):
http://www.mdtmag.com/news/2013/09/new-password-heartbeat

Links:
[1] http://media.rice.edu