New firewall to safeguard against medical-device hacking

April 12, 2012

Print Version

WEST LAFAYETTE, Ind. – Researchers at Purdue and Princeton universities have created a prototype firewall to block hackers from interfering with wireless medical devices such as pacemakers, insulin-delivery systems and brain implants.

The team had previously demonstrated how medical devices could be hacked, potentially leading to catastrophic consequences.

"You could imagine all sorts of scary possibilities," said Anand Raghunathan, a Purdue professor of electrical and computer engineering. "What motivated us to work on this problem was the ease with which we were able to break into wireless medical systems."

Raghunathan is working with Niraj K. Jha, a Princeton professor of electrical engineering, and Chunxiao Li and Meng Zhang, both Princeton graduate students in electrical engineering. He discussed the new concept and prototype during the Purdue Center for Implantable Devices Symposium earlier this year.

The potentially vulnerable devices include pacemakers and continuous glucose monitoring and insulin delivery systems for patients with diabetes, now in use by hundreds of thousands of people. Brain implants under development to control epilepsy and "smart prosthetics" operated using electronic chips also could be hacked, Jha said.

He stressed that the risk of devices being hacked is low but that security measures are merited before "attacks" in the lab are replicated on real systems.

"The benefits of pacemakers and insulin delivery systems far outweigh the remote risks posed by possible hackers," Jha said.

The team has created a prototype system called MedMon, for medical monitor, which acts as a firewall to prevent hackers from hijacking the devices. They demonstrated how MedMon could protect a diabetes system consisting of a glucose monitor and an insulin pump, which communicate with each other wirelessly

"It's an additional device that you could wear, so you wouldn't need to change any of the existing implantable devices," Raghunathan said. "This could be worn as a necklace, or it could be integrated into your cell phone, for example."

The researchers detailed earlier findings in a paper presented last year during the IEEE 13th International Conference on e-Health Networking, Applications and Services (Healthcom).

Many implantable devices have wireless transmitters and receivers, which enable health-care providers to perform diagnostics and to download data.

"For example, a diagnostic test is performed periodically to make sure they are running properly," Jha said. "And during health emergencies, medical personnel must be able to access the systems."

However, having wireless access also opens the door to potential hackers, who might alter the insulin dosage or direct pacemakers to malfunction, harming or killing a patient.

"Very little work exists on this important topic, and the security vulnerabilities of such systems are not well understood," Jha said.

The MedMon prototype, which has been tested and shown to protect an insulin pump from hacking, monitors communications going into and coming out of any implantable or wearable medical device. It uses "multi-layered anomaly detection" to identify potentially malicious transactions. Upon detecting potentially malicious activity, the firewall can raise an alarm to the user or block "malicious packets" from reaching the medical device by using electronic jamming similar to technology used in military systems.

The prototype is a proof of concept and would need to be miniaturized. A provisional patent application has been filed on the concept.

"This is still not going to solve privacy concerns," said Raghunathan, a member of Purdue's Center for Implantable Devices. "Someone could still learn that you have a medical device, but hopefully they are not going to be able to do anything bad to you. It is extremely difficult to make a system completely impregnable."

The researchers previously described two other potential solutions in a paper presented during last year's IEEE Healthcom conference. One of those concepts is based on a cryptographic technique now seen in automotive keyless entry systems and garage-door openers, and the other would use "body-coupled communication," which involves transmitting signals on a patient's skin.

The research has been funded by the National Science Foundation. Information about the Purdue Center for Implantable Devices, in the university's Weldon School of Biomedical Engineering, is available at https://engineering.purdue.edu/CID

Writer: Emil Venere, 765-494-4709, venere@purdue.edu

Sources: Anand Raghunathan, 765-494-3470, raghunathan@purdue.edu

Niraj K. Jha, 609-258-4754, jha@princeton.edu

Note to Journalists: An electronic copy of the research paper is available from Emil Venere, 765-494-4709, venere@purdue.edu

ABSTRACT

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System

Chunxiao Li, Niraj K. Jha, Department of EE, Princeton University, and Anand Raghunathan, School of ECE, Purdue University

Wearable and implantable medical devices are being increasingly deployed to improve diagnosis, monitoring and therapy for a range of medical conditions. Unlike other classes of electronics and computing systems, security attacks on these devices have extreme consequences and must, therefore, be analyzed and prevented with utmost effort. Yet, very little work exists on this important topic and the security vulnerabilities of such systems are not well understood. We demonstrate security attacks that we have implemented in the laboratory on a popular glucose monitoring and insulin delivery system available on the market, and also propose defenses against such attacks. Continuous glucose monitoring and insulin delivery systems are becoming increasingly popular among patients with diabetes. These systems utilize wireless communication links, which are frequently utilized as a portal to launch security attacks. Our study shows that both passive attacks (eavesdropping of the wireless communication) and active attacks (impersonation and control of the medical devices to alter the intended therapy) can be successfully launched using public domain information and widely available off-the-shelf hardware. The proposed attacks can compromise both the privacy and safety of patients. We propose two possible defenses against such attacks. One is based on rolling-code cryptographic protocols, and the other is based on body-coupled communication. Our security analysis shows that the proposed defenses have the potential to mitigate the security risks associated with personal healthcare systems.

Featured News

- Purdue dedicates renovated, newly named Roland G. Parrish library
- Purdue celebrates $10 million gift for center dedicated to student excellence, leadership
- Beef futures markets bounce back slightly after BSE reports
- Purdue Research Foundation assumes oversight of AMIPurdue
- Purdue campuses to host spring commencement ceremonies

- Cheetah Conservation Fund founder to speak at Purdue
- Tiny 'spherules' reveal details about Earth's asteroid impacts

More News »

Follow Us