Researchers Fight to Keep Implanted Medical Devices Safe from Hackers

Neal Leavitt

Implantable medical devices have become increasingly popular, and a growing number are equipped with wireless communications technology to increase their usefulness. However, this could make the devices susceptible to hackers.

Implantable medical devices—such as insulin pumps, cardiac pacemakers, and cardiac defibrillators—have become increasingly popular since being introduced about 50 years ago. In the US alone, 2.6 million people rely on IMDs.

An increasing number of today's devices are equipped with wireless technology enabling, for example, remote checks by healthcare workers.

"Patients often receive at-home, bedside monitors that wirelessly collect telemetry from implanted devices," said University of Massachusetts Amherst assistant professor Kevin Fu, codirector of the Medical Device Security Center.

The monitors relay stored information to a server, which then makes the distilled data available to clinicians, in some cases via Web browsers, added Wendy Dougherty, program director for public relations for IMD vendor Medtronic.

"Many of these devices now communicate with PCs to upload stored information and may soon communicate with devices such as smartphones," said Nathanael Paul, a research scientist at the US Department of Energy's Oak Ridge National Laboratory (ORNL).

All this convenience may come with unanticipated risks: the possibility that hackers could break into IMDs' communications and either send harmful commands to the devices or steal private patient information.

A team of researchers from Harvard University, the University of Massachusetts Amherst, and the University of Washington demonstrated in 2008 that hackers could extract patients' private medical information and reprogram their devices using off-the-shelf radio and computer equipment.

Currently, said Dougherty, the risk of malicious or otherwise unauthorized manipulation of an implantable device is very low.

"To our knowledge, there has never been a single reported incident outside of controlled lab experiments in more than 30 years of device telemetry use," she noted.

Currently, IMDs' benefits outweigh their risk, so patients should use them if prescribed, said Paul.

However, the risk is growing, as is the number of patients using IMDs in part because of the aging of the population.

"The time to prevent future attack scenarios is now," said Paul.

"Hacking a medical device—especially an implantable one—can have serious consequences and therefore must be taken seriously," said Ed Moyle, a senior manager with healthcare consultancy CTG.

INSIDE THE IMD

The first implantable cardiac pacemaker—developed by Medtronic founder Earl Bakken—was released in 1958.

IMDs have advanced over the years. For example, the devices are now capable of two-way wireless communications.

Many insulin pumps use low-power chips with small transceivers that send data—such as blood glucose levels—to other system components and then receive commands to, for instance, pump more insulin.

In October 2005, Zarlink Semiconductor introduced the first transceiver module designed explicitly for linking

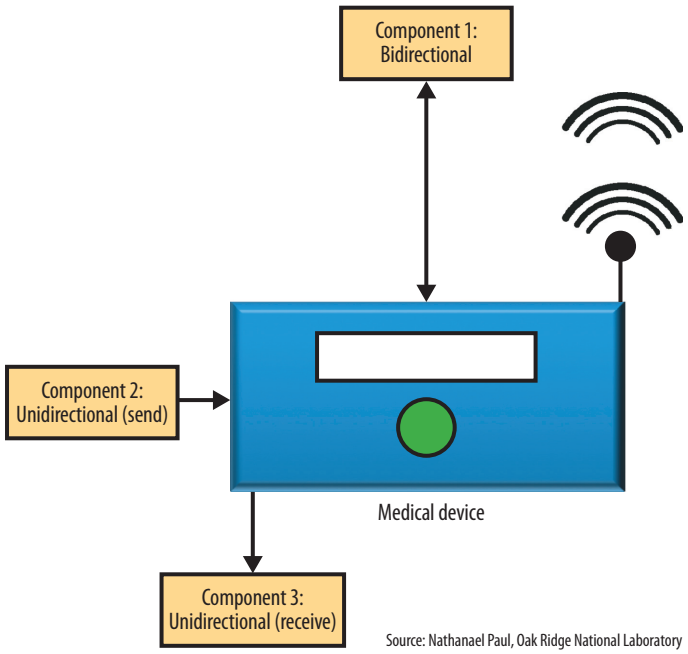

Figure 1. Many of today's implantable medical device systems, such as insulin pumps, are equipped with wireless technology. The IMD shown here could communicate with a bidirectional component, such as a remote controller; a send-only device, like a blood glucose monitor; or a receive-only device, such as a PC that acquires patient status information. These many lines of communications make IMDs vulnerable to hackers who could either send harmful commands to the devices or steal private patient data.

implanted medical devices and base stations.

IMDs work with various radio technologies that operate over distances of several centimeters and transmit within designated industrial, scientific, and medical frequency bands.

Most devices work with proprietary communications protocols. However, a few devices support the ZigBee wireless standard and vendors may release medical applications using Bluetooth, via the technology's Health Device Profile, soon, said University of Massachusetts Amherst doctoral candidate Benjamin Ransford.

IMDs often work with software-defined radios so that a single device could, for example, operate over multiple frequencies.

They also use various types of processors, including those that run the systems. They can also work with signal-processing chips, noted Medtronic's Dougherty. Some device companies even develop their own processors for complex calculations.

Today's IMDs don't connect directly to the Internet, although some wirelessly connect to a bedside monitor that then connects to the Internet.

DEVICES AT RISK

Connecting an IMD to computers and phones makes treatment and monitoring more convenient. However, this can also make the device susceptible to attacks already faced by computers and phones, as Figure 1 shows.

In 2003 and 2009, the Slammer and Conficker worms infected some networked hospital systems responsible for monitoring heart patients, said ORNL's Paul.

He noted that anyone can communicate with an IMD via wireless equipment that uses the same frequency and communications protocol as the device.

IMDs sometimes use off-the-shelf technologies for communications and other functionality. According to CTG's Moyle, these underlying technologies' vulnerabilities could affect the devices.

"A primary concern is [hackers] eavesdropping on the communication channel between the device and external control units," he noted. "Anytime you have a wireless data connection, you raise the possibility of this, as well as possible spoofing attacks." Such attacks would let hackers emulate a legitimate part of an IMD system and obtain or alter information.

Attackers could also intercept and record commands and then replay them.

Potential motivations for hacking IMDs include the desire to harm either a specific person or just someone in general.

Said Paul, "A public official or celebrity could be attacked. A student may even wish to skip a test and issue some commands to the teacher's medical device."

Other motivations, he noted, could include hurting an IMD maker's reputation or gaining personal satisfaction from hacking.

Hackers, added Moyle, could target people who they know wear IMDs or they could also launch attacks in crowded areas or near medical facilities, hoping someone with a device is nearby.

2008 IMD hacking demonstration

The Harvard University, University of Massachusetts Amherst, and University of Washington researchers in the 2008 IMD-hacking demonstration used inexpensive, off-the-shelf Linux PC and GNU radio software to intercept and capture the short-range signals that an implantable cardiac defibrillator sent to an authorized external controller.

"We studied the wireless communications to understand the specifics of how the IMD and [controller] com-

municate and utilized that knowledge to send commands of our own to the IMD," explained University of Washington assistant professor Tadayoshi Kohno.

"We were able to cause an implantable cardiac defibrillator to emit a shock designed to induce [a fatal heart rhythm]," said Fu. "The radio allowed us to listen to sample radio communications between a [controller] and the device, then replay the communication to control the device."

The researchers also obtained sample patient information placed on the device, including name, birth date, and diagnosis.

In addition, they shut off stored settings in the IMD, which would have left the device unable to respond to emergencies.

IMD advances bring problems

Most IMDs support only short-range communications, over distances from 2 to 5 centimeters.

However, the radio technology is improving. ORNL has communicated with IMDs at a range of 30 meters. "But this doesn't mean that they are intended to communicate at that distance," said the lab's Paul.

Longer ranges will enable greater patient mobility during in-home data collection. In addition, the computer equipment used to gather information can be moved farther from the patient, thereby protecting sterile zones in operating and patient rooms.

However, the longer range will also make IMD systems accessible to more people, including potential hackers.

Meanwhile, as is the case with most devices, IMDs have become more difficult to secure as they have become more functional and complex.

FIGHTING BACK

Researchers and manufacturers are trying to design security approaches that ensure that real-world attacks either don't happen or don't cause problems.

They must be careful that these approaches don't block IMD functionality or cause other problems because that could necessitate surgically removing and then replacing a device.

St. Jude Medical Center facilities use proprietary approaches to secure their IMDs, including the St. Jude Medical Accent RF pacemaker and the St. Jude Medical Anthem RF cardiac-resynchronization-therapy pacemaker. St. Jude officials wouldn't comment on the nature of their techniques.

Different types of IMDs could use the same kinds of security approaches. However, those techniques might function differently with the various types of IMDs. For example, an implanted insulin pump interacts with external components of the system continually throughout the day. In pacemakers, there is less interaction and all components are internal.

Researchers are trying to meet the security challenges that IMDs face.

Oak Ridge research

Paul's group at ORNL has conducted experiments implementing attacks on commercially deployed insulin-pump systems.

In the process, they have developed a detailed model of potential threats. For example, said Paul, if a smart phone is used in insulin pump systems in the future to store blood glucose levels, as has been proposed, hackers changing those values could hurt patients.

The researchers are addressing these threats by creating new protocols to protect IMDs' control channels and the patient data they store and transmit.

For instance, noted Paul, systems could use very-short-range communications. This would make attacks more difficult by disallowing long-range attacks.

ORNL researchers are also creating new insulin-pump-system architectures, such as those that implement encryption and those that better support important security properties like authentication.

Encryption

Few IMDs encrypt signals, but this will soon change, said CTG's Moyle.

Encryption could limit data interception and hide the commands used with the devices so that only permitted controllers could work with them.

However, noted Paul, there are limits to this approach because encryption capabilities could add complexity and require more system resources to function properly. Some IMDs might not have sufficient battery and computing power to implement certain encryption algorithms.

Zero-power defense

Adding complexity such as security features could be undesirable because they could consume IMDs' limited battery life. In response, researchers are considering a security mechanism called the zero-power defense.

The goal is to enhance the security of an IMD without using energy from the device's battery, according to the University of Massachusetts Amherst's Ransford.

An energy-harvesting computer could serve as a gateway device. People trying to communicate with an IMD power the gateway device with their own radio transmissions. The gateway then runs a challenge-response protocol that makes people prove they're allowed to contact the IMD.

Unauthorized parties are thus deterred without using any of the IMD's battery power, noted Ransford.

Patient-centered approaches

University of Washington professor Batya Friedman said the school's Value-Sensitive Design Research Lab, which she codirects, surveyed cardiac patients with IMDs about suggested security solutions.

Friedman said patients preferred security solutions that warned of potential problems, didn't require them to do anything inconvenient, and didn't call attention to their condition.

Some experts have suggested implementing passwords that must be entered before someone can access an IMD.

However, doctors who might not know the password would have to be able to control the devices in case of emergency, particularly if the patient is unconscious. To deal with this, patients could wear bracelets that show their passwords. However, they could lose the bracelets.

One proposed solution popular with the security community—IMD-access passwords tattooed on patients as barcodes visible only under ultraviolet light—met with mixed results because some respondents didn't like the idea of tattoos, explained Tamara Denning, a doctoral student at the Value-Sensitive Design Research Lab.

"Our observations suggest that no single security approach may be attractive to all patients but rather that different types of security approaches may appeal to different patients," Denning said.

Issues

IMD security faces several key challenges. First, adding security could hurt system performance and increase cost, at least initially.

Some approaches may require completely new devices or components. For example, healthcare providers implementing two-way communications in IMD systems would have to replace unidirectional equipment.

At a minimum, ORNL's Paul said, adding technologies such as encryption would require updates of the software on some IMDs and the controller.

However, he added, the biggest challenge will be finding solutions that are acceptable to patients.

Today's IMDs increasingly use wireless communications that provide monitoring and other benefits for patients, so the technology is here to stay, said Paul.

But as IMDs become smaller, more resource-constrained, increasingly complex, and more functional, the challenges in making them secure while taking into account considerations such as usability, patient values, and battery life will increase.

"We really need a concerted effort on the part of all relevant stakeholders, including computer security researchers, medical practitioners, device manufacturers, [regulators], social scientists, and patient advocacy groups," said the University of Washington's Friedman.

This effort, added Paul, should also include the benefits of standardizing various IMD security properties.

Stated the University of Massachusetts' Fu, "Legislators should give regulators the authority to require adequate privacy controls before an IMD can reach the market."

Legislation should avoid mandating specific technical approaches but instead just provide incentives and penalties, he added.

However, he said, manufacturers are ultimately responsible for IMD safety.

"Medical devices save lives, but they are no more immune to security and privacy risks than any other computing device," he said. "We'd better get the security and privacy right during the early design stages because surgically replacing an insecure medical device is much less convenient than an automated Windows update. And the consequences can be fatal." C

Neal Leavitt is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, France, Germany, Hong Kong, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.

Editor: Lee Garber, *Computer*;
l.garber@computer.org