Protecting medical implants from attack

June 13 2011, By Larry Hardesty

Credit: M. Scott Brauer

Millions of Americans have implantable medical devices, from pacemakers and defibrillators to brain stimulators and drug pumps; worldwide, 300,000 more people receive them every year. Most such devices have wireless connections, so that doctors can monitor patients' vital signs or revise treatment programs. But recent research has shown that this leaves the devices vulnerable to attack: In the worst-case scenario, an attacker could kill a victim by instructing an implantable device to deliver lethal doses of medication or electricity.

At the Association for Computing Machinery's upcoming Sigcomm conference, researchers from MIT and the University of Massachusetts-Amherst (UMass) will present a new system for preventing such attacks. The system would use a second transmitter to jam unauthorized signals in an implant's operating frequency, permitting only authorized users to

communicate with it. Because the jamming transmitter, rather than the implant, would handle encryption and authentication, the system would work even with existing implants.

The researchers envision that the jamming transmitter — which they call a shield — would be small enough to wear as a necklace or a watch. A device authorized to access the implant would send encrypted instructions to the shield, which would decode and relay them.

Today's implantable medical devices weren't built with hostile attacks in mind, so they don't have built-in encryption. But even in the future, says Dina Katabi, an associate professor in MIT's Department of Electrical Engineering and Computer Science, handling encryption externally could still prove more practical than building it directly into implants. "It's hard to put [encryption] on these devices," Katabi says. "There are many of these devices that are really small, so for power reasons, for form-factor reasons, it might not make sense to put the [encryption] on them." Moreover, Katabi points out, building encryption directly into the devices could be dangerous. In an emergency, medical providers might need to communicate with the implant of an incapacitated patient, to retrieve data or send new instructions. Retrieving an encryption key from the patient's ordinary medical provider could introduce fatal delays, but with the MIT-UMass system, an emergency responder would simply remove the patient's shield.

Subtracted signals

Katabi and her graduate students Shyam Gollakota and Haitham Hassanieh, working together with Kevin Fu, an assistant professor of computer science at UMass, and his student Ben Ransford, conducted a series of experiments using implantable defibrillators obtained secondhand from Boston-area hospitals. (Defibrillators are generally replaced while they still have some battery life.) Programmable off-the-

shelf radio transmitters simulated the shield.

The key to the system, Katabi explains, is a new technique that allows the shield to simultaneously send and receive signals in the same frequency band. With ordinary wireless technology, that's not possible: The transmitted signal would interfere with the received signal, rendering it unintelligible. Researchers at Stanford University recently demonstrated a transmitter that could send and receive at the same time, but it required three antennas whose distance from each other depended on the wavelength at which they were operating. For medical-device frequencies, the antennas would have to be about a half a meter apart, making it impossible to miniaturize the shield.

The MIT-UMass system uses only two antennas and clever signal processing that obviates the need to separate them. "Think of the jamming signal that we are creating as a secret key," Katabi explains. "Everyone who doesn't know the secret key just sees a garbage signal." Because the shield knows the shape of its own jamming signal, however, it can, in effect, subtract it from the received signal.

Whether medical-device companies will invest in security systems like Katabi and Fu's — and whether patients will be willing to carry shields around with them — probably depends on how grave they consider the threat of attack to be. Katabi acknowledges that no such attacks have been documented to date. On the other hand, the Federal Communications Commission has recently moved implantable medical devices to a new frequency band that makes wireless communication with them possible across much greater distances.

"This is exactly the time when you want to do this kind of research," says Stefan Savage, a professor in the computer science and engineering department at the University of California at San Diego, and one of the leaders of the department's Security and Cryptography Group. "You

don't want to do it when there's an active threat." Savage sees no obvious technical obstacles to the deployment of the MIT-UMass system: "I think that's what people liked about it," he says, "that you could do it with existing devices, and that you did not have a lot of the overhead that it would take to come up with an entirely new thing." The question, he says, is whether manufacturers will have an incentive to absorb the cost of deploying it. "Value in the information-security market gets created by one of two people: bad guys, or regulatory bodies," he says. "You want to develop the technology in advance of the threat, but absent the threat, how do you sell the technology?"

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

More information: groups.csail.mit.edu/netmit/IMDShield/

Provided by Massachusetts Institute of Technology