Security Risks Found in Sensors for Heart Devices

University of Michigan

The type of sensors that pick up the rhythm of a beating heart in implanted cardiac defibrillators and pacemakers are vulnerable to tampering, according to a new study conducted in controlled laboratory conditions.

Implantable defibrillators monitor the heart for irregular beating and, when necessary, administer an electric shock to bring it back into normal rhythm. Pacemakers use electrical pulses to continuously keep the heart in pace.

In experiments in simulated human models, an international team of researchers demonstrated that they could forge an erratic heartbeat with radio frequency electromagnetic waves. Theoretically, a false signal like the one they created could inhibit needed pacing or induce unnecessary defibrillation shocks.

The team includes researchers from the University of Michigan, University of South Carolina, Korea Advanced Institute of Science and Technology, University of Minnesota, University of Massachusetts and Harvard Medical School.

The researchers emphasize that they know of no case where a hacker has corrupted an implanted cardiac device, and doing so in the real world would be extremely difficult.

"Security is often an arms race with adversaries," said Wenyuan Xu, assistant professor of computer science and engineering at the University of South Carolina. "As researchers, it's our responsibility to always challenge the common practice and find defenses for vulnerabilities that could be exploited before unfortunate incidents happen. We hope our research findings can help to enhance the security of sensing systems that will emerge for years to come."

This is not the first time vulnerabilities have been identified in implantable medical devices. But the findings reveal new security risks in relatively common "analog" sensors—sensors that rely on inputs from the human body or the environment to cue particular actions.

Beyond medical devices, analog sensors are also used in microphones in Bluetooth headsets and computers in web-based phone calls. In those places, too, the researchers discovered vulnerabilities.

"We found that these analog devices generally trust what they receive from their sensors, and that path is weak and could be exploited," said Denis Foo Kune, U-M postdoctoral researcher and visiting scholar in computer science and engineering, who will present the findings May 20 at the IEEE Symposium on Security and Privacy in San Francisco.

Although these medical systems and consumer electronics have security mechanisms, the information the analog sensors receive bypasses their safety layers. The devices convert the input from the sensors directly into digital information that they use to make quick decisions.

In the category of medical devices, the researchers tested cardiac defibrillators and pacemakers in open air to determine which radio waveforms could cause interference. Then they exposed the medical devices to those waveforms in a both a saline bath and a patient simulator. The experiments suggest that the human body likely acts as a shield, protecting the medical devices to a large degree, the researchers said.

They found that in the saline bath and the patient simulator, a perpetrator would need to be within five centimeters—about two inches—away to cause interference. Current guidelines instruct patients to keep potential sources of interference at least 27 centimeters, or 10.5 inches, away from their chest.

"People with pacemakers and defibrillators can remain confident in the safety and effectiveness of their implants," said Kevin Fu, U-M associate professor of electrical engineering and computer science. "Patients already protect themselves from interference by keeping transmitters like phones away from their implants. The problem is that emerging medical sensors worn on the body, rather than implanted, could be more susceptible to this type of interference."

The team proposes solutions to help the sensors ensure that the signals they're receiving are authentic. Software could, in a sense, ping the cardiac tissue to determine whether the previous pulse came from the heart or from interference. If the source was not the heart, the software could raise a red flag.

The researchers also found pathways to tamper with consumer electronics. They were able to use specific radio signals to convince the mic on a phone paired with a Bluetooth headset that a caller was dialing touch-tone selections at an automated banking line. They demonstrated this by changing the call language from English to Spanish.

Foo Kune said the technique could conceivably enable more harmful scenarios such as fraudulent money transfers. In another experiment, they canceled out speech on one side of a web-based phone call and replaced it with a song (Weezer's "Island in the Sun").

"The microphone was receiving the song even though the room was silent," Foo Kune said.

"This type of interference can be prevented with shields and filters like those seen today in military-grade equipment," said Yongdae Kim, professor of electrical engineering at the Korea Advanced Institute of Science and Technology. "Safety critical systems, such as smart grids and automated vehicles, rely more and more on sensing technology for their accurate operation. Malicious input signals with improved antenna and power may cause serious safety problems."

For more information, visit University of Michigan [1].

Links:
[1] http://www.umich.edu/