Researchers Hack Defibrillators

March 12 2008

Tadayoshi Kohno (left) and doctoral student Dan Halperin co-authored the first known study on security concerns related to implantable medical devices.

Some medical devices such as implantable cardiac defibrillators and pacemakers are now equipped with wireless technology, allowing for remote device checks and freeing patients from repeated doctor visits. But this convenience may come with unanticipated risks. A team of researchers from three leading universities has demonstrated that patients' private medical information could be extracted and their devices reprogrammed without the patients' authorization or knowledge.

There has never been a reported case of a patient with an implantable cardiac defibrillator or pacemaker being targeted by hackers, and the researchers emphasized that the study was designed to identify and prevent future problems. Undertaking the study required a high level of technical expertise, and the published paper omits certain details in methodology that prevents the findings from being used for anything

other than improving patient security and privacy.

The study was led by two computer scientists, Tadayoshi Kohno of the University of Washington and Kevin E. Fu of the University of Massachusetts Amherst, and cardiologist Dr. William H. Maisel of the Beth Israel Deaconess Medical Center and Harvard Medical School. Their scholarly peer-reviewed report will be presented and published at the Institute of Electrical and Electronic Engineers Symposium on Security and Privacy in Oakland, Calif., May 19, 2008.

Dr. Maisel, director of the Medical Device Safety Institute at Beth Israel Deaconess Medical Center in Boston, notes, “One of the purposes of this research is to encourage the medical device industry to think more carefully about the security and privacy of patient information, particularly as wireless communication becomes more common. Fortunately, there are some safeguards already in place, but device manufacturers can do better.”

The team expects this issue to take on greater importance as implantable cardiac defibrillators operate wirelessly at greater distances. These devices typically receive short-range wireless signals over several feet, but new technologies are expanding that reach even farther, creating the potential for information to be intercepted en route.

“We hope our research is a wake-up call for the industry,” said Kohno, an assistant professor of computer science and engineering at the University of Washington. “In the 1970s, the Bionic Woman was a dream, but modern technology is making it a reality. People will have sophisticated computers with wireless capabilities in their bodies. Our goal is to make sure those devices are secure, private, safe and effective.”

Fu, an assistant professor of computer science at UMass Amherst, noted

that the study developed several prototype defenses. “One of our primary contributions is the invention of three defense mechanisms that require no battery power, making them potentially easy to incorporate in the devices without extensive redesigning. While there has been much research that explores the biological safety of implantable medical devices, there is limited understanding about the related issues of wireless security and privacy. Understanding the security and privacy of implantable devices is essential for protecting the nation’s health and cyber infrastructure.”

The researchers’ experiments used an implantable cardiac defibrillator, a sophisticated device that automatically regulates the heart beat by sending small electrical signals to the heart to stimulate the heart rate or by delivering a large shock to restore a potentially fatal heart rhythm back to normal. Implantable defibrillators have improved survival in selected patients at risk for sudden cardiac death, and millions of the devices have been implanted worldwide. The model used in the researchers’ experiment contained computers and radios that allow health-care practitioners to diagnose patients, read and write private medical information, and adjust the device’s therapy settings wirelessly.

In computer laboratory bench tests, the research team used an inexpensive software radio to intercept and capture signals sent from the implantable device. They were able to obtain detailed information about a hypothetical patient, including name, diagnosis, date of birth and medical ID number. Researchers could determine the make and model of the device and access real-time electrocardiogram results as well as data on the hypothetical patient’s heart rate and cardiac activity.

The team then mounted several attacks. Researchers were able to turn off the therapy settings stored in the implantable device, rendering it incapable of responding to dangerous cardiac events. Additional commands were delivered, resulting in the delivery of a shock that could

induce ventricular fibrillation, a potentially lethal arrhythmia.

Three deterrence and prevention mechanisms were developed as part of the study, including a notification device that audibly alerts patients of security sensitive events, a device that authenticates requests for access from outside devices and a vibrating device that patients can sense. All three mechanisms require no power from the battery, and one of them was evaluated for effectiveness in a substance similar to human tissue.

Because the team studied one common model of implantable cardiac defibrillator, the susceptibility of similar devices to privacy and security risks is uncertain. The researchers believe future studies are needed to assess potential risks associated with other implantable devices equipped with wireless technology. The researchers feel strongly that nothing in their report should deter patients from receiving these devices if recommended by their physician. The implantable cardiac defibrillator is a proven, life-saving technology.

Source: University of Washington