Insulin pumps, monitors vulnerable to hacking

August 4 2011, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Even the human bloodstream isn't safe from computer hackers.

A security researcher who is diabetic has identified flaws that could allow an attacker to remotely control insulin pumps and alter the readouts of blood-sugar monitors. As a result, diabetics could get too much or too little insulin, a hormone they need for proper metabolism.

Jay Radcliffe, a diabetic who experimented on his own equipment, shared his findings with The Associated Press before releasing them Thursday at the Black Hat computer security conference in Las Vegas.

"My initial reaction was that this was really cool from a technical perspective," Radcliffe said. "The second reaction was one of maybe sheer terror, to know that there's no security around the devices which are a very active part of keeping me alive."

Increasingly, medical devices such as pacemakers, operating room monitors and surgical instruments including deep-brain stimulators are being made with the ability to transmit vital health information from a patient's body to doctors and other professionals. Some devices can be remotely controlled by medical professionals.

Although there's no evidence that anyone has used Radcliffe's techniques, his findings raise fears about the safety of medical devices as they're brought into the Internet age. Serious attacks have already been demonstrated against pacemakers and defibrillators.

Medical device makers downplay the threat from such attacks. They argue that the demonstrated attacks have been performed by skilled security researchers and are unlikely to occur in the real world.

But hacking is like athletics. Showing that a far-fetched attack is possible is like cracking the 4-minute mile. Once someone does it, others often follow. Free or inexpensive programs eventually pop up online to help malicious hackers automate obscure attacks.

Though there has been a push to automate medical devices and include wireless chips, the devices are typically too small to house processors powerful enough to perform advanced encryption to scramble their communications. As a result, most devices are vulnerable.

Radcliffe wears an insulin pump that can be used with a special remote control to administer insulin. He found that the pump can be reprogrammed to respond to a stranger's remote. All he needed was a USB device that can be easily obtained from eBay or medical supply companies. Radcliffe also applied his skill for eavesdropping on computer traffic. By looking at the data being transmitted from the computer with the USB device to the insulin pump, he could instruct the USB device to tell the pump what to do.

Radcliffe, who is 33 and lives in Meridian, Idaho, tested only one brand of insulin pump - his own - but said others could be vulnerable as well.

Although an attacker would need to be within a couple hundred feet of the patient to pull this off, a stranger wandering a hospital or sitting behind a target on an airplane would be close enough.

Radcliffe also found that it was possible to tamper with a second device he wears. He found that he could intercept signals sent wirelessly from a sensor to a machine that displays blood-sugar levels. By broadcasting a

signal that is stronger than the real-time, authentic readings, the monitor would be tricked into displaying old information over and over. As a result, a patient who didn't notice wouldn't adjust insulin dosage properly.

With a powerful enough antenna, Radcliffe said, an attacker could be up to half a mile away. This attack worked on two different blood-sugar monitors, Radcliffe said.

"Everybody's pushing the technology to do more and more and more, and like any technology that's pushed like that, security is an afterthought," Radcliffe said.

Radcliffe refused to identify any of the three device makers, in part out of concern for his own safety. He is concerned that the devices don't appear to have an easy way to be updated with new software to fix the problems. He said he intends to notify the manufacturers after Thursday's presentation outlining the weaknesses.

The hacking fears come on top of human errors and technical glitches tied to medical devices. The U.S. Food and Drug Administration has identified software and design errors as critical concerns in investigating hundreds of deaths potentially linked to drug pumps.

FDA officials declined to comment specifically on Radcliffe's findings, saying they hadn't seen the research. But the FDA said that any medical device with wireless communication components can fall victim to eavesdropping. It warns device makers that they are responsible for making sure they can update equipment after it's sold.

Industry officials downplay the potential threat.

"The risk to a patient with diabetes of having their monitors hacked is

extraordinarily small, and there's a great health risk of not monitoring than the risk of being hacked," said Wanda Moebius, a vice president at the Advanced Medical Technology Association, an industry group.

Few public studies have been done on the susceptibility of medical devices to hacking.

One such study, which appeared in 2008 from a consortium of academics, found that a popular type of device that acted as both a pacemaker and defibrillator could be remotely reprogrammed to deliver potentially deadly shocks or run out its battery.

The problem was the way the device transmitted data unencrypted and accepted commands wirelessly from unauthorized devices. One limitation of the study was that researchers only examined an attack from a few centimeters away from the targeted device.

Yoshi Kohno, a University of Washington professor of computer science who was a co-author of that study, said that Radcliffe's new research reinforces the urgency of addressing security issues in medical devices before attacks move out of research labs.

"The threat hasn't manifested yet, so what they and we are trying to do is see what the risk could be in the future," said Kohno, who wasn't part of Radcliffe's research.

Radcliffe said the point of his research is not to alarm people. He said the issues he's discovered are important to address publicly as the medical industry moves aggressively toward more networked devices.

"It would only take one person to do this to kill someone and then you have a catastrophe," he said.