



Original URL: http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

By **Dan Goodin in San Francisco**

Posted in [Security](#), 27th October 2011 06:23 GMT

[Free whitepaper – IBM BNT RackSwitch and IBM System Networking Solutions](#)

In a hack fitting of a James Bond movie, a security researcher has devised an attack that hijacks nearby insulin pumps so he can surreptitiously deliver fatal doses to diabetic patients who rely on them.

The attack on wireless insulin pumps, made by medical devices giant Medtronic, was demonstrated Tuesday at the [Hacker Halted](#) [1] conference in Miami. It was delivered by McAfee's Barnaby Jack, the same researcher who last year showed how take control of two widely used models of automatic teller machines so he could to cause them to [spit out a steady stream of dollar bills](#) [2].

Jack's latest hack works on most recent Medtronic insulin pumps, because they contain tiny radio transmitters that allow patients and doctors to adjust their functions. It builds on [research presented earlier this year](#) [3] that allowed the wireless commandeering of the devices when an attacker was within a few feet of the patient, and knew the serial number of his pump. Software and a special antenna designed by Jack allows him to locate and seize control of any device within 300 feet, even when he doesn't know the serial number.

"With this device I created and the software I created, I could actually instruct the pump to perform all manner of commands," Jack told *The Register*. "I could make it dispense its entire reservoir of insulin, which is about 300 units. I just scan for any devices in the vicinity and they will respond with the serial number of the device."



An insulin pump made by Medtronic

It's not the first time a hacker has figured out how to wirelessly issue potentially lethal commands to a medical device implanted in a patient's body. In 2008, academic researchers demonstrated an attack that allowed them to intercept medical information from implantable cardiac devices and pacemakers and to cause them to turn off or [issue life-threatening electrical shocks](#) [4]. The devices are used to treat chronic heart conditions.

In a statement, Medtronic officials said they are working to improve the security of the medical devices the company sells by evaluating encryption and other protections that can be added to their design. Representatives are also informing doctors and patients of the risks so they can make more informed decisions. Medtronic officials have also promised to set up an industry working group to establish a set of standard security practices.

"Because insulin pumps are widely used by patients with diabetes for tight blood sugar control and lifestyle flexibility, we are also working to assure both patients and doctors that at this time we believe that the risk is low and the benefits of the therapy outweigh the risk of an individual criminal attack," the statement read.

The pumps are used to treat patients with diabetes by infusing their bodies with insulin, which is secreted by the pancreas. When insulin levels are too low, people suffer from excessive blood sugar levels, a condition known as hyperglycemia. When insulin levels are too high, they suffer from hypoglycemia, a condition that can result in death if left

unchecked.

The vulnerable Medtronic devices wirelessly send and receive data over the 900 MHz frequency, and Jack said it's impossible to disable this functionality. He wrote software that works with Medtronic-supplied USB devices that allow doctors and patients to wirelessly monitor the devices from a computer. Combined with custom-built antenna, his system scans a 300-foot radius for compatible devices.

Insecure by design

The pumps use no encryption to conceal the content of their transmissions, and a vulnerability allowed Jack to discover the device's serial number. His software also overrides restrictions that normally prevent the pump from receiving wireless commands to increase dosages. Under normal conditions, the pumps issue a vibration or loud tone when dispensing a dosage, but Barnaby's attack disables the warning mechanism.

"We're talking about code that was developed approximately 10 years ago, so there really wasn't security on the forefront of these embedded devices," Jack said. "To be honest, they weren't expecting people to rip them open and see what goes on under the hood."

Jack said one attack scenario would be to use the hack to target an individual known to use a vulnerable device. Without close monitoring, the victim would have little way of knowing the dosage had been altered, and the attack could be carried out by anyone within a few hundred feet.

A Medtronic spokeswoman declined to say how many pumps are susceptible to the attack. Jack said his hack works on pumps with model numbers of 712 and higher. The spokeswoman declined to say when those pumps were first marketed, but websites such as [this one](#) [5] list the manufacture date as 2006.

Jack said his research over the past few years has increasingly focused on the tiny computers included in the millions of devices used every day to treat medical conditions, dispense cash, and perform other vital functions.

"I've taken an interest in embedded devices because they're used for critical applications," he explained. "When you compromise these types of devices, there's a very real world effect." ®

Links

1. <http://www.hackerhalted.com/2011/>
2. http://www.theregister.co.uk/2010/07/28/atp_hacking_demo/
3. http://www.theregister.co.uk/2011/08/19/insulin_pump_hack/
4. http://www.theregister.co.uk/2008/03/12/heart_monitor_hacking/
5. <http://www.medwow.com/used-insulin-pump/medtronic/paradigm-712/961114655.item>

Related stories

[Insulin pump maker ignores diabetic's hack warnings](http://www.theregister.co.uk/2011/08/25/medtronic_insulin_pump_hacking/) (25 August 2011)
http://www.theregister.co.uk/2011/08/25/medtronic_insulin_pump_hacking/