YOU CAN'T MAKE THIS UP

DEATH BY HACKING A DEFIBRILATOR

Implanted pacemaker/defibrillators from several manufacturers can be commanded to deliver a deadly shock from someone on a laptop up to 50 feet away – the result of poor software programming by medical device companies.

That is the assertion reported by a news service based on research from at analyst at IOActive, a security vendor. The flaw lies with the programming of the wireless transmitters used to give instructions to pacemakers and implantable cardioverter-defibrillators (ICDs), which detect irregular heart contractions and deliver an electric shock to avert a heart attack.

In the past, pacemakers and ICDs were reprogrammed by medical staff using a wand that had to pass within a couple of meters of a patient who has one of the devices installed. The wand flips a software switch that would allow it to accept new instructions. But the trend is now to go wireless. Several medical manufacturers are now selling bedside transmitters that replace the wand and have a wireless range of up to 30 to 50 feet.

The US Food and Drug Administration (FDA) just looks at the medical effectiveness of devices and does not do an audit of a device's code. In 2006, the FDA approved full radio-frequency based implantable devices operating in the 400 MHz range. As many as 4.6 million pacemakers and ICDs were sold between 2006 and 2011 in the US alone.

With that wide transmitting range, remote attacks against the software become more feasible. In addition it was found that devices would give up their serial number and model number after being wirelessly contacted with a special command. With the serial and model numbers, a person could then reprogram the firmware of a transmitter, which would allow reprogramming of a pacemaker or ICD in a person's body. Ironically, both the implants and the wireless transmitters are capable of using AES (Advance Encryption Standard) encryption, but it is not being enabled, The devices also have "backdoors," or ways that programmers can get access to them without the standard authentication using a serial and model number.

At an October presentation in Australia the analyst illustrated in a comic-book like fashion a slide showing a man who looked quite similar to former U.S. vice president Dick Cheney, who has long suffered from heart problems. He pointed out the flaws in an implanted pacemaker/defibrillator device could mean an attacker could perform a fairly anonymous assassination from 50 feet away. A laptop doesn't look like a device that is capable of killing someone or as an audience member said "There's no muzzle flash with a laptop."