# New frontier for cybersecurity: your body

June 23 2013, by Rob Lever

So far, the idea of hacking into medical devices has been limited to fiction and hacker demonstrations.

But US regulators and security experts say the threat is real: malicious actors can gain access to devices ranging from pacemakers to insulin pumps, with potentially fatal results.

The US Food and Drug Administration this month warned manufacturers to step up their vigilance, saying it has learned of "cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations."

Officials say they know of no deliberate hacking of medical devices. But on the television drama "Homeland," the vice president of the United States is assassinated by hackers who gain access to his pacemaker and deliver a fatal electric shock.

"The good news is that we are not aware of any incidents in the real world. But the bad news there is no science behind looking for it," said Kevin Fu, a University of Michigan professor of computer science specializing in health security.

"It takes just a blink of the eye for malware to get in."

Fu co-authored a 2008 research paper highlighting the risks of implantable devices like cardiac defibrillators, which could be reprogrammed by hackers who get into system's wireless network.

"My opinion is that the greater risk is from malware that accidentally gets into a device rather than the attacks in fictionalized programs," Fu said.

"Malware will often slow down a computer, and when you slow down a medical device it no longer gives the integrity needed to perform as it should."

Barnaby Jack at the security firm IOActive, said the "Homeland" scenario was "fairly realistic," and that he would demonstrate a similar attack at an upcoming hacker gathering.

"In 'Homeland,' they required a serial number, my demonstration doesn't," he said.

Jack has been researching implantable medical devices such as pacemakers and defibrillators from a major manufacturer, and said he has found the devices "to be particularly vulnerable."

He said that from a range of 10 to 15 meters (30 to 50 feet) "I can retrieve the credentials needed to interrogate the individual implants remotely."

In another publicized incident, security specialist Jay Radcliffe, who is diabetic, demonstrated in 2011 the potential to hack into an insulin pump to change dosage levels.

Security specialists say that in addition to implanted devices, hospital equipment such as monitoring systems, scanners and radiation equipment are connected to networks which could have lax security, creating similar security holes. Some heart and drug monitoring systems use open Wi-Fi connections that can be hacked.

"The vast majority of medical devices in hospitals I've been to use Windows XP or Windows 95. These are extremely vulnerable to computer malware," Fu said.

Attacks or insertion of malware could affect things like radiation therapy, or devices which mix nutrients for intravenous delivery, he said.

Medical devices and equipment may have passwords, but these can be hacked as well, as shown in a recent report by the security firm Cylance, which obtained passwords to 300 different devices.

"We could have reported 1,000 different backdoor passwords, we could have even gone all the way to 10,000," said a blog post from Cylance's Billy Rios and Terry McCorkle. "We stopped at 300 because we felt 300 was sufficient to get our point across."

This finding prompted a warning from the Department of Homeland Security's Cyber Emergency Response Team for industrial systems, which said security should be stepped up for surgical devices, ventilators, drug infusion pumps and other equipment.

A number of computer security firms are working to help the industry, but Fu said these solutions are often the equivalent of a Band-Aid.

"Most cybersecurity problems can be traced back to the design," he said

"I have doubts that a strategy just based on antivirus or firewalls can be effective."

Experts say that despite all the risks, people still are better off with than without these devices.

"The chance of a targeted malicious attack against someone's medical

device is extremely low, and the last thing we want is for people to lose faith in these life saving devices," Jack said.

"We think that any risk, no matter how low, still needs to be eliminated. We hope by raising awareness of these issues and bringing the threats to the attention of the manufacturers, that they can take steps to improve the security of these devices."