Is a pacemaker capable of mass murder?

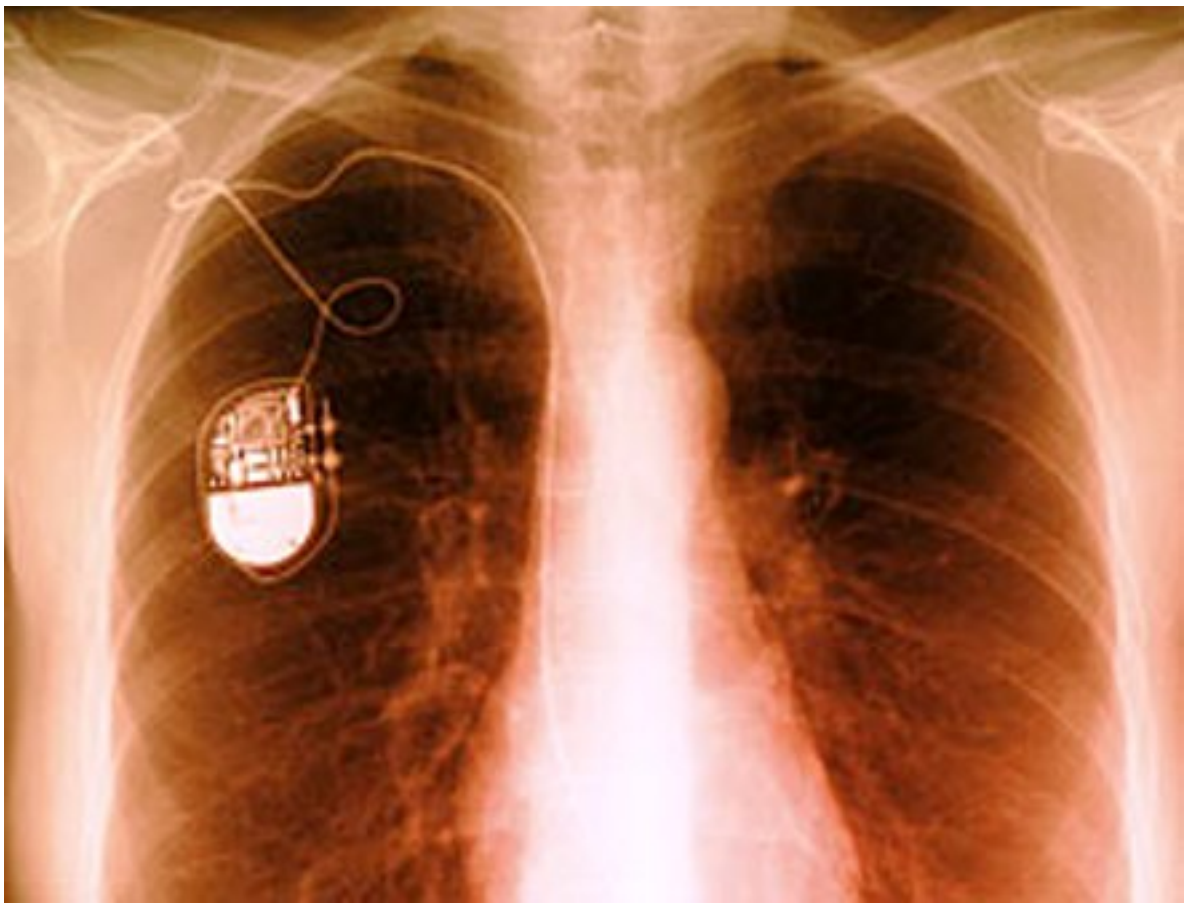
Kasey Panetta, Associate Editor

 When you are a patient in a hospital, you tend to expect that the electronics are either top of the line or at least functioning correctly. You expect that the devices doctors implant in your body are reliable and safe. These seem like safe assumptions.

Unfortunately, you could be mistaken.

There is a very low level of security on medical devices and medical equipment, leaving them vulnerable to malware and hacking, and the person taking the unknown risk is the patient.
Luckily, the risk has been relatively low, particularly when compared to the medical advantages the technology provides. Unfortunately, as researchers and professional hackers begin to discover to what extent the devices can be hacked, it’s possible those with more sinister plans will see the security gap as an opportunity.

In a presentation that seems to belong in a horror film and not at a conference, Barnaby Jack, an IOActive researcher at the BreakPoint Security Conference in Melbourne, Australia, demonstrated that he could reverse-engineer a pacemaker to change from a life-saver to a weapon.



The problem is that updates used to be provided to the device by a medical professional who had to be within a few inches of the patient, according to CIO [1]. However, because of the increase in wireless technology, the inches have expanded to a larger radius, leaving the devices vulnerable to more attacks.

Jack found that by utilizing a “secret function” hidden in the medical devices, he was able to gather model and serial numbers from all pacemakers and implantable cardioverter-defillibrators within 30 feet, according to MIT’s Technology Review. [2]

Because those stolen numbers act as authorization keys, Jack was able to reverse engineer the terminals which communicate with the devices. This allowed him access to usernames and passwords from the manufacturer’s development server. With that unprotected information in hand, Jack could load infected firmware masquerading as an update onto the devices. That might not seem like a huge deal—considering he could initially only access pacemakers in a 30-foot plus range—but due to the nature of the technology, once the bad firmware is loaded, the infected pace maker will then infect any clean pacemaker or implantable cardioverter-defillibrator it encounters.

Consider, for a moment, the damage this could cause in a hospital or retirement facility.

Jack, who did not release the presentation to the public for fear of identifying the company who manufactured the devices, then developed “Electrical field,” a program which can scan for the devices in range. By manipulating the actual

function of the pacemakers, Jack would be able to deliver up to 850 volts—enough to induce cardiac arrest. If the first shock doesn't kill you, the device can also be instructed to deliver continuous shocks.

A recent Report to Congressional Requesters by the US Government Accountability Office pointed out the need for better regulation by the Food and Drug Administration (FDA). Currently, the government watchdog only considers unintentional threats to the devices, not malicious threats. Because the threat extends past pacemakers to any active medical device which uses electronics and wireless communications, like an insulin pump, it's an important topic of discussion.

The experts are conflicted. One camp firmly believes this is an attack waiting to happen, while the other insists that the devices are designed so that it would be difficult to "install and propagate malware," according to the 2012 report. Jack's ideas of "mass murder" remain firmly in the worst case scenario column; let's just hope they stay there.
In the hospital

Just when you thought it was safe to go back in the hospital, a medical-device panel at the National Institute of Standards and Technology Information Security & Privacy Advisory Board found increasing amounts of hospital equipment is infected with or vulnerable to malware.

Hackers are able to target the hospitals more easily because of the recent improvements in communication and connectivity, according to MIT's technology review [2]. Not only are the Window's systems themselves vulnerable to attack—software companies often refuse any security changes to their product—but most systems are connected to the easily hacked internet.

Mark Olsen, chief information security office at Beth Israel, gave an example of how the malware slowed the fetal monitors used for high-risk pregnancies in the ICUs so the monitors couldn't track or monitor the data. Because the women are in an IC ward, the machines are a back-up to an ever-present medical professional. Unfortunately, the malware didn't stop at the IC wards. According to Olsen, it threatens devices that prepare intravenous drugs and nutrition, diagnostic equipment, even radiology equipment, slowing the devices to the point where they're useless or even dangerous to use.

The upside is no one has been harmed, yet it's a problem that the community is taking seriously. The downside is security specialists are only starting to discover where and to what extent the machines are vulnerable to attack.

Links:

[1] http://www.cio.com.au/article/439322/pacemaker_hack_can_deliver_deadly_830-volt_jolt/
[2] http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices/