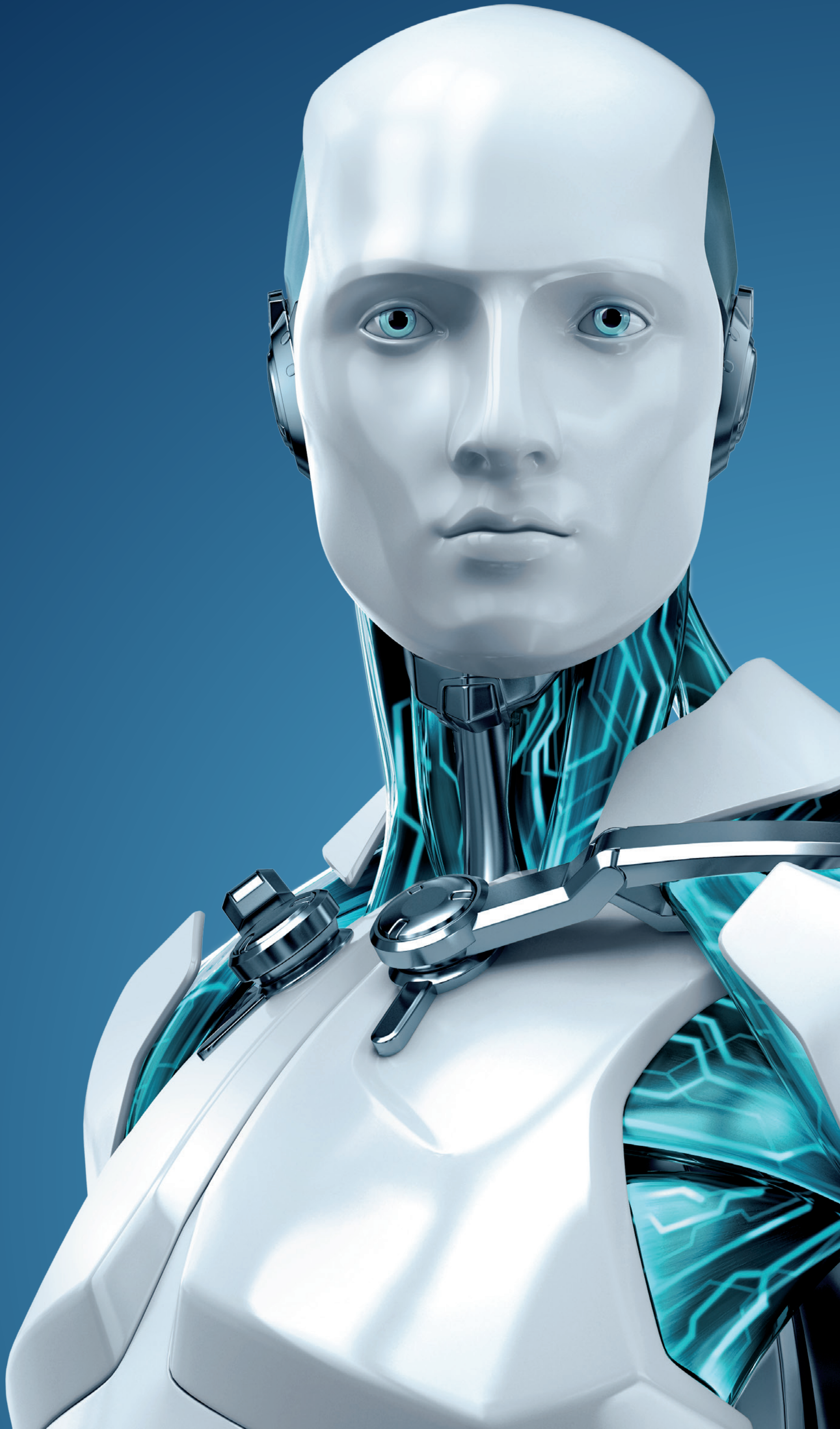
TECH BRIEF

A turning point in medical device security



ESET®

ENJOY SAFER TECHNOLOGY™

A TURNING POINT IN MEDICAL DEVICE SECURITY

By Stephen Cobb, ESET Security Researcher

How hackable are medical devices? Are surgical robots safe? How real was that death-by-pacemaker scene in Showtime's spy drama Homeland? These questions are no longer the stuff of fiction. They quickly become very relevant and real if you or a loved one is facing surgery or has to depend on a medical device such as an insulin pump or a pacemaker.

Factor in the predicted growth of telemedicine, which relies heavily on networked communications between doctors, devices, and patients, and it all adds up to a serious cause for concern. On the bright side, we have a window of opportunity right now to create secure technology that can deliver better healthcare to more people at a lower cost without compromising security.

Questions about the security of medical devices are receiving broader attention today thanks to alerts this year from two federal agencies, the Department of Homeland Security and the U.S. Food and Drug Administration.[1]

Speaking as someone who has spent a lot of time dealing with attacks on digital systems, and who also happens to be facing robotic surgery this year, I was somewhat taken aback by the stated purpose of this alert:

> The FDA is recommending that medical device manufacturers and health care facilities take steps to ensure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Is it just me, or does "take steps" sound like we are currently a long way from where we need to be? Here's what the FDA did not say: "take steps to assure *patients* that appropriate safeguards are in place to reduce the risk of failure." Frankly, such assurances would be hard to justify right now. Just ask Jay Radcliffe, a computer security professional who is also diabetic. In 2011 he demonstrated an attack in which insulin pumps could be remotely controlled to deliver too much or too little insulin to the patient. As reported in *Wired*, this led to calls for a federal inquiry into the security of medical devices,[2] the results of which appeared in an August 2012 report, titled: "FDA Should Expand Its Consideration of Information Security for Certain Types of Devices."[3]

Then, there is the research that led to the DHS alert in June of this year, issued by ICS-CERT (the Industrial Control Systems Cyber Emergency Response Team). Here's how that alert begins:

> Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could

[1] FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

[2] Security of medical devices. http://www.wired.com/2011/08/medical-device-security/

[3] FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. http://www.gao.gov/products/GAO-12-816

> be exploited to potentially change critical settings and/or modify device firmware. ICS-ALERT-13-164-01[4]

Many of the passwords documented to DHS by Rios and McCorkle allowed firmware attacks, permitting malicious reprogramming of the device, a low-level attack against which even basic consumer devices are already protected, through firmware signing (e.g., Xbox, PlayStation 3, and Nintendo Wii).

For an academic perspective on medical device security, look at the work of Kevin Fu, a professor at the University of Michigan College of Engineering and one of the authors of the 2008 IEEE paper "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses."

Fu is one of the prime movers at the Ann Arbor Research Center for Medical Device Security (known as Archimedes), and you can find that 2008 paper, and many others in the same vein, on the publication page of the Archimedes project website.[5] Researchers from Archimedes were the first to demonstrate wireless pacemaker hacks (as reported in *Wired*, March, 2008[6]):

> One extreme medical device hack has been demonstrated more recently by Barnaby Jack, the director of embedded device security for IOActive, who tragically died shortly before appearing at this year's Black Hat conference. Jack had been showing people how it was possible to commandeer an ICD (implantable cardioverter-defibrillator) and, from a distance of up to 50 feet, trigger a potentially fatal 830-volt shock to a patient's heart (Jack's research on this had led him to rate the infamous Homeland episode plausible).

Does this mean we are now seeing malicious code written to infect and abuse pacemakers and insulin pumps? I'm not aware of anything like that appearing "in the wild" just yet. And frankly, that type of code may not be as big a threat to medical devices as the cyberhygiene of the environments in which they operate. While both Jack and Fu have called for less sensationalism when talking about medical device security, they have also voiced an urgent need to improve the security of medical devices, and the digital hygiene of the environments in which they exist. For example, speaking at a meeting of the medical-device panel at the NIST Information Security and Privacy Advisory Board, of which he is a member, Fu last year noted that conventional malware is "rampant" in hospitals because many medical devices are using outdated and unpatched operating systems.

So the first cases of physical harm caused by malware may not come from sophisticated code that targets medical devices, but from common viruses and worms slowing down systems such as fetal monitors used to handle high-risk pregnancies, a real-world example cited last year by the chief information security officer at Beth Israel Deaconess Medical Center in Boston. The irony here is that controls to prevent such incidents are well known and well tested. We're not talking about APTs (advanced persistent threats). We're talking about healthcare entities failing to run antivirus scans, something that the Ponemon Institute documented last year in its Third Annual Patient Privacy and Data Security Study.[7]

[4] ICS-ALERT-13-164-01. http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

[5] Archimedes. http://www.secure-medicine.org/publications

[6] Wired. http://www.wired.com/2008/03/scientists-demo/

[7] Third Annual Patient Privacy and Data Security Study. http://www.ponemon.org/blog/third-annual-patient-privacy-data-security-study-released

Despite HIPAA's security and privacy rules and regulations, the healthcare industry has not yet fully internalized the need for security by design, either in its IT systems or in the medical devices used to deliver care to patients. Which is a pity, because we are entering a new phase of healthcare delivery, according to Venkat Rajan, industry manager, advanced medical technologies for global growth, at consulting firm Frost and Sullivan:

> The concepts of accountable care and pay-for-performance, coming from the general need to reduce healthcare costs and the specific requirements of the Affordable Care Act, demand better access to more patient data, all of which implies greater connectivity, particularly in areas such as remote care or telemedicine.

The technology to deliver secure connectivity and safe systems exists. If we exert the will to implement that technology in this next wave of healthcare delivery, we stand to reap great benefits. If not, the cost to society could be enormous. Personally speaking, I've told my surgeon to bench the robot pending a more complete risk assessment.