Implantable medical devices are vulnerable to hackers and cybercriminals. Insecure IT systems have left hospitals lousy with viruses and malware. How real is the danger? And what’s being done to fight it?

BY MIKE MILIARD, Managing Editor

The scene from the Showtime series Homeland is tough to watch: The Vice President of the United States, dying slowly as his heart beats faster. His pacemaker – a delicate implanted device, accessed and altered from some distant computer by a terrorist who’d learned its serial number – is going haywire.

It could happen, said Tim Zoph, CIO of Northwestern Memorial Hospital in Chicago, speaking at the Healthcare IT News/HIMSS Media Privacy & Security Forum this past December.

“Fact or fiction?” Zoph asked, clutching an innocuous-looking black box – a wireless transmitter used to give instructions to pacemakers – as he scanned the audience.

“The fact is,” he said, “they’re not secure.”

As healthcare becomes ever more interconnected, especially as myriad wireless medical devices start linking up with complex and Web-enabled IT systems, these technologies are increasingly vulnerable. Not just to nefarious hackers lurking in the shadows, but to more mundane but no less dangerous threats such as malware and the common computer virus.

“We’re starting to attach (medical devices) to electronic health records, and they’re not secure,” said Zoph. “We’re not doing it with security in mind.”

The vulnerabilities are enticing to curious techno-tinkerers, and the number and variety of threats is increasing. So far, neither device manufacturers nor federal regulators have been able to come up with fail-safe protections from a mutating menace.

Meanwhile patient safety for hundreds of thousands of people remains at risk.
“The security of medical devices is a complicated topic. It’s not for the faint of heart.”

Kevin Fu

Fixing a hole
There have been lots of hair-raising headlines lately: insulin pump hack delivers fatal dosage over the air, pacemaker hack can deliver deadly 50-volt jolt. Vulnerable medical devices create a clear and present danger.

“You’re going to hear a lot about worse-case-scenarios, but I think patients, by and large, should be concerned about the more average things,” said Kevin Fu, a professor of computer science and engineering at the University of Michigan, who specializes in medical device security.

By “more average,” Fu means the sorts of things that could happen to a plain old PC, any day of the week, thanks to something as mundane as an email that shouldn’t have been opened or a link that shouldn’t have been clicked.

Many medical devices run on Microsoft Windows or Windows variants, after all. In case it’s escaped your notice over the past 15 years or so, that’s an OS that’s especially susceptible to security issues. (So much so that Microsoft has a regularly scheduled day—“Patch Tuesday,” the second Tuesday of every month—dedicated to releasing updates to plug vulnerabilities.)

Infection with computer viruses is a common occurrence in households across the country. And in hospitals too.

Fu was quoted in a recent MIT Technology Review article in which he said the problem is “mind-boggling.” Malware, he said, is “rampan” in hospitals thanks to devices using unpatched operating systems.

The story noted, for instance, that Boston’s Beth Israel Deaconess Medical Center had nearly 700 pieces of equipment “running on older Windows operating systems that manufacturers will not modify or allow the hospital to change—even to add antivirus software—because of disagreements over whether modifications could run afoul of IT systems, which are often connected to the Internet, the opportunities for unwanted intrusion increase significantly.

“There’s a convergence of these new devices” implantable insulin pumps and defibrillators, smaller and more advanced than previously thought possible—“for treating diseases that previously we didn’t know we could treat.”

At the same time, these devices are becoming highly connected to networks, and sometimes to the Internet,” said Fu.

“These changes together have really changed the landscape.”

Hackers are scary. And the damage they can wreak is immense. During his January confirmation hearings, Secretary of State John Kerry called cyber-terrorism “the modern day, 21st century nuclear weapons equivalent.”

And they’re only getting smarter. “Twenty years ago, when you got spam or computer viruses, it might be the proverbial kid in the basement just sending it out,” said Fu. “Nowadays it comes from well-financed adversaries, taking over massive numbers of computer systems.”

The good news, he said, is that cyber criminals have not targeted medical devices yet. “But it does show that very rarely does the adversary get dumber over time. They tend to get much smarter.”

“Smart pumps run software,” Fu noted. “In his view, they are definitely devices that must be secure. “The only good news is there aren’t any.”

One’s own devices
Actually, in early 2012 a professional “white hat” hacker named Barnaby Jack, then working as a security professional at McAfee, did indeed discover that certain insulin pumps made by Medtronic are susceptible to hacking.

Someone with the motive and the means, he found, could access the devices from many yards way, shut off their security protections, and flood diabetics’ bloodstreams with insulin.

“There are computers that are just as exploitable as your PC or Mac, but they’re not looked at as often,” Jack told Bloomberg News. “When you actually look at these devices, the security vulnerabilities are quite shocking.”

Jack now works for Seattle-based security firm IOActive as director of embedded device security, researching protections for this new security front. His colleague, Gunter Ollmann, IOActive’s chief technology officer, puts the threat in perspective.

“How real is that threat from malicious actors actually intentionally carrying these things out? I think it’s very low today,” said Ollmann. “I don’t foresee that becoming a common occurrence.”

That said, there is plenty of room for risk. Ollmann said he’s more worried about accidental corruption—about the “tinkering and (potential for) misadventure” that are part and parcel of even the most well-meaning, Web-based spelunking.

“When you look at these implantable medical devices, if someone wanted to attack them, there are enough proof cases on how to launch the attacks,” he said. It’s “the unintentional part” that keeps him up at night.

“These devices all have wireless communications, but there are controlling tools—PC-based, or otherwise—that doctors or others use for updates, or sending new commands or
We’re starting to attach (medical devices) to electronic health records, and they’re not secure.”

Tim Zoph

Device manufacturers “were very reluctant to hear what we had to say from the security front.”

Gunter Ollmann

new profiles to the devices. Those are much more vulnerable, because of their linkages to the Internet.

Fu agrees that a piece of malware or other computer bug, introduced into the hospital setting by some thoughtless employee’s laptop, is the bigger risk factor: “Certainly, the more connected the device is, the more security concerns would arise.”

Ollmann wonders if it’s all too much too fast – whether “the push to make these devices interconnected, with wireless communications, integrated into existing computer networks,” is happening before device manufacturers – to say nothing of care providers – have a proper handle on “what the security threats are and what the consequences of them are.”

The technology, he said, “is outstanding their ability to understand what the threats are to the platforms their integrating with.”

Speaking at the Clinical Engineering and IT Leadership Symposium at the 2013 HIMSS Annual Conference & Exhibition in March, David Classen, MD, chief medical informatics officer at Pascal Metrics and an associate professor of medicine at the University of Utah, made a sobering case that safety disasters involving poor device integration are “far more common than we realize.”

And a technology failure, “when you have a highly IT-rich environment, changes the safety net,” he said.

Even without viruses and malware in the equation, device integration, especially in areas such as ICU, is “really complicated,” he added. “We were naive to think it could be solved so quickly.”

Order of business

Everyone is grappling with these complex safety issues, whether they pertain to hospital integrations or outpatient implantables. Device manufacturers, especially, are trying to feel their way around this new threat landscape.

“If I had to give a school report card, I’d probably use more of a kindergarten report card: everybody’s above average,” said Fu, underscoring the manufacturers’ newness to these issues. “An ‘A’ for effort, at least.”

Most manufacturers “genuinely want to improve the security of their medical devices,” he said. “But they don't necessarily know how.”

Ollmann echoes that verdict: “So far, we have not seen the medical device manufacturers, particularly the implantable devices, have a strategy for securing these technologies.”

It’s not the technical hurdles, necessarily. “There are some brilliant technical people at many of these companies,” said Fu. “What they have trouble doing is translating it into return on investment.”

He explains that, presented with a new and different type of malfunction, “one that doesn’t subscribe to a notion of probability of error, probability of occurrence, a manufacturer does not know how to interpret that. So it’s a notion that’s really causing a rethinking in the manufacturing community: How do you quantify this?”

When I contacted Medtronic for a comment about the insulin pump vulnerabilities discovered by Barnaby Jack, company officials directed me to AdvaMed, the medical device trade organization of which it is a member.

“The highest priority is it’s got to be safe,” said Bernie Liebler, AdvaMed’s director of technology and regulatory affairs, offering some insight into device manufacturers’ challenges gauging probability.

“The FDA expects you to have a risk management system,” he said. “The point of a risk management system is to look at all the possible things that could go wrong the reasonable things, the unreasonable things, the far-fetched things. You place a probability about them, and then put in place mitigations to prevent them, or at least minimize the possibility of them happening.”

For a long time, said Liebler, manufacturers “have recognized that hacking is a possibility, and companies have been dealing with it.”

But how intense an effort is made depends on the device and the possible consequences, he said: “Headlines don’t necessarily make things more likely to happen.”

Sure, “you try to safeguard against everything. On the other hand, you have to safeguard most intensely against things that are most likely to go wrong. If you try to eliminate every single infinitesimal risk, you wind up with an unusable device and an extraordinarily expensive device.”

For his part, as a consultant, Ollmann said many manufacturers “were very reluctant to hear what we had to say from the security front.”

That’s something that’s not uncommon when new threats emerge. Often, when companies are confronted with security vulnerabilities they hadn’t considered, “their first reactions are often quite hostile,” he said. “And by hostile, I mean suppression of information, bringing in the lawyers first, before the engineers.”

Then, after several months of “fearful conversation and negotiation,” he said, “then the engineering team starts to be engaged and a more productive relationship starts to appear, and there are efforts to fix and remediate some of these technologies.”

Speaking for AdvaMed, Liebler said device manufacturers have a handle on the threat. “Do I think the companies are addressing it adequately? Probably,” he said. “Bubble gum and duct tape is not something that the industry believes in.”

Rules and regulations

In the past few years, politicians in Washington have started paying more attention to medical device security, and pushing for more robust security measures to be encouraged and enforced.

In August 2011, for instance, Democratic Representatives Edward Markey and Anna Eshoo, of Massachusetts and California, respectively, wrote to the Government Accountability Office, requesting that it take a closer look at devices such as insulin pumps, implantable defibrillators and remote monitoring systems.

“It’s critical that these devices are able to operate together and with other hospital equipment, and not interfere with each other’s activities and data transmissions,” they wrote. “It’s also important that such devices operate in a safe, reliable and secure manner.”

In August 2012, GAO responded, issuing a study that confirmed “medical devices may operate in a safe, reliable and secure manner.”

GAO officials reported that “certain intentional information security threats were of greater concern” than others. Threats of “unauthorized access or denial-of-service...
DEVICES
CONTINUED FROM PAGE 6

A technology failure, “when you have a highly IT-rich environment, changes the safety net.”

David Classen, MD

attacks,” came in for close scrutiny.

“Additionally, experts made distinctions among intentional threats and the likelihood of their occurring,” according to the report. “For example, one expert cited malware as one of the greatest threats to active implantable medical devices. However, other experts considered malware as less of a concern because, according to these experts, certain devices are currently designed so that it would be difficult to install and propagate malware.”

At any rate, GAO concluded that the FDA should “develop and implement a plan expanding its focus on information security risks.”

FDA officials did not respond to numerous requests for comment. For his part, Fu said the question of more government regulation was still up in the air.

“Don’t think FDA will do it with regulations,” he said. “I think they’ll do it with guidance. It’s really burdensome for an agency to make regulations. This will, over time, probably be a fairly fast-moving target. I think they’re better off providing guidance to the industry on how they’d like to see this stuff addressed. If the world out there changes, they can change that guidance fairly quickly. You can’t change regulations quickly.”

Holding to account

In the meantime, there’s still “a lot of confusion among the various stakeholders, the manufacturers, the regulators, the hospitals, on whose responsibility it is to keep these devices up-to-date,” said Fu.

FDA guidance “specifically said manufacturers are expected to keep their operating their procurement processes to see more meaningful security in the products they buy,” said Fu. “It should be more clear what sort of maintenance will be provided: How often will patches be provided? Who will do it? Who pays for it?”

On the other side of the equation, manufacturers “need to think much more carefully about security during the concept phase, the very early stages of their device development,” he said. “It’s so hard to build in security after the fact, to bolt it on. It’s much smarter to design it in early.”

As device vendors and their provider clients work out ways to improve security and patient safety, several academic projects are exploring more creative ways to safeguard devices.

Researchers at MIT and the University of Massachusetts have done work developing technology to protect pacemakers and brain stimulators from intrusion, jamming unauthorized signals detected on a device’s frequency. The transmitter, according to MIT News, could be “small enough to wear as a necklace or a watch.”

MedMon, jointly developed by scientists at Purdue and Princeton, is a firewall that aims to shield implanted medical devices from cyber attacks with a similar strategy.

“What motivated us to work on this problem was the ease with which we were able to break into wireless medical systems,” Anand Raghunathan, a professor of electrical and computer engineering at Purdue, told the school’s news service.

In one of the more intriguing projects, Dartmouth researchers have developed a system that deploys biometric sensors to prevent hackers from gaining access to devices. The prototype uses the wearer’s unique physiological responses to prevent tampering via a unique encryption system.

“The bracelet can detect who is wearing it at any given time using bioimpedance,” said Cory Cornelius, a fourth-year graduate student in Dartmouth’s computer science department, tells Healthcare IT News. “Bioimpedance measures how your body (or in this case, your wrist) responds to a small electrical current. We hypothesized that the anatomy and geometry of your wrist will be sufficiently unique to identify you, so we use bioimpedance to measure this, and our work shows this is possible.”

This could be used to stymie “an insider threat where the wearer of the bracelet is actively trying to fool the system into thinking it is someone else,” he said.

Future shock?

If all this sounds like science fiction, just wait to see what things look like five or 10 years from now. The technology is evolving. And so are those who might like to probe its weaknesses and exploit them.

“You’re never finished,” said Liebler. Keeping devices secure “is a constant process. And when you see product failures of any type, you bring them back in, you look for the cause, you run it through the risk-management system, and figure out the best way to minimize that risk or make it go away, if possible.”

Things are different now. As amazing as these tiny devices once seemed, today they’re able to connect wirelessly to the Web, allowing physicians to monitor their patients’ vital signs or set new treatment parameters. It’s a whole new ballgame.

“Previous generations did not have wireless updates, and that internet connectivity,” said Ollmann. “What we’re doing, we hope, is raising awareness that the landscape has changed.”

Still, “Patients should trust their physicians and their devices. They’re much better off with these devices than without. And security is one of the unfortunate growing pains of the success of these devices,” said Fu.

“It’s much wiser to be aware of the risks than to put your head in the sand,” he added.

“Usually the bad guys are a couple steps ahead of the good guys.”