KIM ZETTER SECURITY 04.25.14 06:30 AM

IT'S INSANELY EASY TO HACK HOSPITAL EQUIPMENT

Instruments set out in preparation for operation in modern theatre PHOTO: CHARLES THATCHER/GETTY IMAGES

WHEN SCOTT ERVEN was given free rein to roam through all of the medical equipment used at a large chain of Midwest health care facilities, he knew he would find security problems–but he wasn't prepared for just how bad it would be.

In a study spanning two years, Erven and his team found drug infusion pumps–for delivering morphine drips, chemotherapy and antibiotics–that can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care.

restart or reboot them to wipe out the configuration settings, allowing an attacker to take critical equipment down during emergencies or crash all of the testing equipment in a lab and reset the configuration to factory settings.

"Many hospitals are unaware of the high risk associated with these devices," Erven says. "Even though research has been done to show the risks, health care organizations haven't taken notice. They aren't doing the testing they need to do and need to focus on assessing their risks."

Erven works as head of information security for Essentia Health, which operates about 100 facilities–including clinics, hospitals and pharmacies–in Minnesota, North Dakota, Wisconsin and Idaho. Essentia decided to open its facilities to a full-scale evaluation in 2012, and in a remarkable and laudable move, allowed Erven to publicly reveal some of his findings.

>"Many hospitals are unaware of the high risk associated with these devices."
Scott Erven

Erven won't identify specific product brands that are vulnerable because he's still trying to get some of the problems fixed. But he said a wide cross-section of devices shared a handful of common security holes, including lack of authentication to access or manipulate the equipment; weak passwords or default and hardcoded vendor passwords like "admin" or "1234"; and embedded web servers and administrative interfaces that make it easy to identify and manipulate devices once an attacker finds them on a network.

Although Erven and his team don't know whether any of these devices are connected directly to the internet–they plan a subsequent test to determine this–many of them are connected to internal networks accessible via the internet. Hackers could gain access to the devices by infecting an employee's computer via a phishing attack, then exploring the internal network to find vulnerable systems. A hacker who happens to be in the hospital could also simply plug his laptop into the network to discover and attack vulnerable systems.

"There are very few [devices] that are truly firewalled off from the rest of the organization," he says. "Once you get a foothold into the network … you can scan and find almost all of these devices, and it's fairly easy to get on these networks."

Erven, who plans to present some of his findings today at Thotcon in Chicago, began his research after a security consultancy performing a penetration test on an Essentia Health network discovered some devices connected to the network that had security issues. This, combined with previous research done by other security experts showing problems with insulin pumps, defibrillators and hardcoded passwords in medical devices, prompted Essentia to take an extensive look at all of its equipment.

"We had management backing to see what our risk exposure is across all health care systems," he says. "We tested every single device in our environment–various radiology stuff and MRIs, ultrasound and mammography systems, cardiology, oncology. We tested all of our lab systems, surgery robots, fetal monitoring, ventilators, anesthesia."

One of the main problems they found lay with embedded web services that allow devices to communicate with one another and feed digital data directly to patient medical records.

"A lot of the web services allow unauthenticated or unencrypted communication between the devices, so we're able to alter the info that gets fed into the medical record ... so you would get misdiagnosis or get prescriptions wrong," he says. "The physician is taught to rely on the information in the medical records ... [but] we could alter the data that was feeding from these systems, due to the vulnerabilities we found."

Erven says an attacker can collect data passing from medical devices to patient records, then replay it so that the same data gets passed into other records.

They also found problems with refrigeration systems for blood and pharmaceutical storage and cryogenics that aren't protected.

"They all have a web interface that allow you to set the temperature range," he says. Although he says the systems include email alerts and wireless pagers that notify lab and hospital staff if the temperature falls outside certain boundaries, the systems are only protected by hardcoded passwords, and once in the system, an attacker can turn off the email pager notification features or alter the settings to change when an alert is sent.

images are generally backed up in centralized storage units that require no authentication to access. While some of the front-end systems that physicians and other staff use to access the images do use hardcoded passwords and log who accesses the images, Erven says the backup is completely unprotected "and there is no logging if you go in the backdoor way and grab those images."

They also found surgery robots connected to internal networks. Although the robots generally have software firewalls to block connections to them, Erven and his team found that simply running an off-the-shelf vulnerability scanner against the firewall caused it to turn off and fail open.

"But we haven't figured out yet what we can do once those fail open," he says.

The Worst Problems

Some of the most disturbing problems they found involved infusion pumps, ICDs (implantable cardiovascular defibrillators that deliver shocks to a patient who shows signs of going into cardiac arrest) and CT scans. They found a number of infusion pumps that have a web administration interface for nurses to change drug dosage levels from their workstations. Some of the systems are not password-protected, while others have hardcoded passwords that are weak and universal to all customers.

With the CT scan, they could alter configuration files and change radiation exposure limits that set the amount of radiation patients receive.

Though targeted attacks would be difficult to pull off in most cases they examined, since hackers would need to have additional knowledge about the systems and the patients hooked up to them, Erven says random attacks causing collateral damage would be fairly easy to pull off.

That's not the case with implantable defibrillators, however, which could be targeted.

"We found a couple of defibrillator vendors that use a Bluetooth stack for writing configurations and doing test shocks [against the patient] when they're implanted or after surgery," he says. "They have default and weak passwords to the Bluetooth stack so you can connect to the devices. It's a simple password like an iPhone PIN that you could guess very quickly."

Homeland in 2012 but the risks of such an attack are real. Physicians for former Vice President Dick Cheney had the wireless capability of his defibrillator disabled in 2007 to prevent terrorists from conducting such an attack to kill him.

Although the picture of hospital equipment that Erven and his team uncovered was gloomy, there was one bright spot among all the bad news – anesthesia equipment and ventilators are generally not networked and don't allow web administration, so someone would have to have physical access to the devices to alter them.

Hospitals Are Unaware of the Dangers

Erven says that the health care industry is just now waking up to the security problems with medical equipment, and that the problems exist because medical equipment has only ever been regulated for reliability, effectiveness and safety, not for security.

"The vendors don't have any types of security programs in place, nor is it required as part of pre-market submission to the [Federal Drug Administration]," Erven notes. "There's no security assessment before it goes to market."

Last spring, the FDA and DHS issued a notice to the health care industry about problems with hard-coded passwords in medical devices after two researchers found them in about 300 medical devices, including ventilators, pumps, defibrillators and surgical and anesthesia devices.

The alert advised health care facilities to examine their systems for problems and put controls in place to protect them from unauthorized users. But Erven says health care facilities can only do so much to wall-off devices; vendors must do more to secure the devices with encryption and authentication before they sell them to customers and fix the ones that are already in the field. FDA guidelines for medical devices now place the onus on vendors to ensure that their systems are secure and patched, and customers should demand they do so.

Although vendors often tell customers they can't remove hard coded passwords from their devices or take other steps to secure their systems because it would require them to take the systems back to the FDA for approval afterward, Erven points out that the FDA guidelines for medical equipment includes a cybersecurity clause that

FDA.

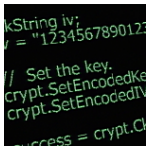
VIEW COMMENTS

SPONSORED STORIES

POWERED BY OUTBRAIN

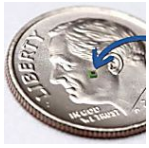
ZIMBIO

This Is What Famous Movie Bullies Look Like Now



VERIZON ENTERPRISE

You Could be the Next Victim of a Data Breach



BANYAN HILL PUBLISHING

Tiny Device to be in 50 Billion Products by 2020 (Read Article)

OUTBRAIN

Learn how to find new audience for your business

WEB LIFE ADVICE

Don't Turn Off Your Computer Until You've Done This...

NAV

How to Check Your Business Credit for Free

MORE SECURITY

DATABASES

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

LILY HAY NEWMAN

FACEBOOK

Facebook's Counterterrorism Playbook Comes Into Focus

EMILY DREYFUSS

SECURITY

Security News This Week: Microsoft's Patching *Old* Versions of Windows Because Things Are That Bad

LILY HAY NEWMAN

NATIONAL AFFAIRS

The Texting Suicide Case Is About Crime, Not Tech

ISSIE LAPOWSKY

WIKILEAKS

WikiLeaks Reveals How the CIA Could Hack Your Router

ANDY GREENBERG

NORTH KOREA

North Korea's Sloppy, Chaotic Cyberattacks Also Make Perfect Sense

ANDY GREENBERG

GET OUR NEWSLETTER

WIRED's biggest stories, delivered to your inbox.

Enter your email

SUBMIT

WE'RE ON PINTEREST

See what's inspiring us.

FOLLOW

ADVERTISE	SITE MAP
PRESS CENTER	FAQ
CUSTOMER CARE	CONTACT US
SECUREDROP	T-SHIRT COLLECTION
NEWSLETTER	WIRED STAFF
JOBS	RSS