

Bloomberg the Company & its Products
Bloomberg Terminal Request a Demo

Bloomberg Anywhere Remote Login



Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome



to

Hac

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome

the

Hospita

**Firewalls and medical devices
are extremely vulnerable, and
everyone's pointing fingers**

**By Monte Reel and Jordan Robertson |
November 2015**

from **Bloomberg Businessweek**



Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome

In the fall of 2013, Billy Rios moved from his home in California to Rochester, New York, for an assignment at the Mayo Clinic, an integrated nonprofit medical group practice in the world. Rios is a “white hat” hacker, which means customers hire him to break into their own computers. His roster of clients has included the Pentagon, major defense contractors, Microsoft, Google, and some others he can’t talk about.

He’s tinkered with weapons systems, with aircraft components, and even with the electrical grid, hacking into the largest public utility district in Washington state to show officials how they might improve public safety. The Mayo Clinic job, in comparison, seemed pretty tame. He assumed he was going on a routine bug hunt, a week of solo work in clean and quiet rooms.

But when he showed up, he was surprised to find himself in a conference room full of familiar faces. The Mayo Clinic had assembled an all-star team of about a dozen computer jocks, investigators from some of the biggest cybersecurity firms in the country, as well as the kind of hackers who draw crowds at conferences such as Black Hat and Def Con. The researchers split into teams, and hospital officials presented them with about 40 different medical devices. Do your worst, the researchers were instructed. Hack whatever you can.

Like the printers, copiers, and office telephones used across all industries, many medical devices today are networked, running standard operating systems and living on the Internet just as laptops and smartphones do. Like the rest of the Internet of Things—devices that range from cars to garden sprinklers—they communicate with servers, and many can be controlled remotely. As quickly became apparent to Rios and the others, hospital administrators have a lot of reasons to fear hackers. For a full week, the group spent their days looking for backdoors into magnetic resonance imaging scanners, ultrasound equipment, ventilators, electroconvulsive therapy machines, and dozens of other contraptions. The teams gathered each evening inside the hospital to trade casualty reports.

“Every day, it was like every device on the menu got crushed,” Rios says. “It was all bad. Really, really bad.” The teams didn’t have time to dive deeply into the vulnerabilities they found, partly because they found so many—

defenseless operating systems, generic passwords that couldn't be changed, and so on

The Mayo Clinic emerged from a tangle of security requirements for information requiring that each device be vetted before purchasing contracts with the clinic, but he knew that only a few hospitals in the world had the resources and influence to pull that off, and he walked away from the job with an unshakable conviction: Sooner or later, hospitals would be hacked, and patients would be hurt. He'd gotten privileged glimpses into all sorts of sensitive industries, but hospitals seemed at least a decade behind the standard security curve.

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome

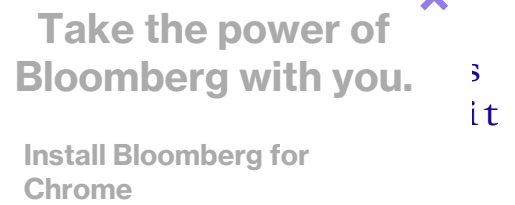
“EVERY DAY, IT WAS LIKE EVERY DEVICE ON THE MENU GOT CRUSHED,” RIOS SAYS. “IT WAS ALL BAD. REALLY, REALLY BAD.”

“Someone is going to take it to the next level. They always do,” says Rios. “The second someone tries to do this, they’ll be able to do it. The only barrier is the goodwill of a stranger.”

Rios lives on a quiet street in Half Moon Bay, a town about 25 miles south of San Francisco, pressed against a rugged curl of coastline where scary, 50-foot waves attract the state’s gutsiest surfers. He’s 37, a former U.S. Marine and veteran of the war in Iraq. In the Marines, Rios worked in a

signal intelligence unit and afterward took a position at the Defense Information Systems Agency. He practices jiu-jitsu, wanders the beach in board shorts, and shares his house with his wife, a 6-year-old daughter, and a 4-year-old son. His small home office is crowded with computers, a soldering station, and a slew of medical devices.

Shortly after flying home from the Mayo gig, Rios ordered his first device—a **Hospira Symbiq infusion pump**. He wasn't targeting or model to investigate; he simply happened to find one for about \$100. It was an odd feeling, putting it in his bag and buying one of these without some sort of license or permission. "OK to crack this open?"



Infusion pumps can be found in almost every hospital room, usually attached to a metal stand next to the patient's bed, automatically delivering intravenous drips, injectable drugs, or other fluids into a patient's bloodstream. Hospira, a company that was bought by Pfizer this year, is a leading manufacturer of the devices, with several different models on the market. On the company's website, an article explains that "smart pumps" are designed to improve patient safety by automating intravenous drug delivery, which it says accounts for 56 percent of all medication errors.

Rios connected his pump to a computer network, just as a hospital would, and discovered it was possible to remotely take over the machine and "press" the buttons on the device's touchscreen, as if someone were standing right in front of it. He found that he could set the machine to dump an entire vial of medication into a patient. A doctor or nurse standing in front of the machine might be able to spot such a manipulation and stop the infusion before the entire vial empties, but a hospital staff member keeping an eye on the pump from a centralized monitoring station wouldn't notice a thing, he says.

In the spring of 2014, Rios typed up his findings and sent them to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In his report, he listed the vulnerabilities he had found and suggested that Hospira conduct further analysis to answer two questions: Could the same vulnerabilities exist in other Hospira devices? And what potential consequences could the flaws present for patients? DHS in turn contacted the Food and Drug Administration, which forwarded the report to Hospira. Months passed, and Rios got no response from the manufacturer and received no indication that government regulators planned to take action.

"The FDA seems to literally be waiting for someone to be killed before they can say, 'OK, yeah, this is something we need to worry about,'" Rios says.

Rios is one of a small group of independent researchers who have targeted the medical device sector in recent years, exploiting the **security flaws** they've uncovered to dramatic effect. Jay Radcliffe, a researcher and a diabetic, appeared at the 2011 Def Con hacking conference to demonstrate how he could hijack his Medtronic insulin pump, manipulating it to deliver a potentially lethal dose. The following year, Barnaby Jack, a hacker from New Zealand, showed attendees at a conference in Australia how he could remotely hack a

pacemaker to deliver a dangerous shock. In 2013, Jack died of a drug overdose one week before he was scheduled to attend Black Hat, where he promised to unveil a system that could pinpoint any wirelessly connected insulin pumps within a 300-foot radius, alter the insulin doses they administered.

Such attacks angered device makers and hospital administrators, who say the staged hacks threatened to scare the public away from technologies that do far more good than harm. At an industry forum last year, a hospital IT administrator lost his temper, lashing out at Rios and other researchers for stoking hysteria when, in fact, not a single incident of patient harm has ever been attributed to lax cybersecurity in a medical device. “I appreciate you wanting to jump in,” Rick Hampton, wireless communications manager for Partners HealthCare System, said, “but frankly, some of the *National Enquirer* headlines that you guys create cause nothing but problems.” Another time, Rios was shouted at by device vendors on a conference call while dozens of industry executives and federal officials listened in. “It wasn’t just someone saying, ‘Hey, you suck,’ or something,” Rios remembers, “but truly, literally, screaming.”

“All their devices are getting compromised, all their systems are getting compromised,” he continues. “All their clinical applications are getting compromised—and no one cares. It’s just ridiculous, right? And anyone who tries to justify that it’s OK is not living in this world. They’re in a fantasyland.”

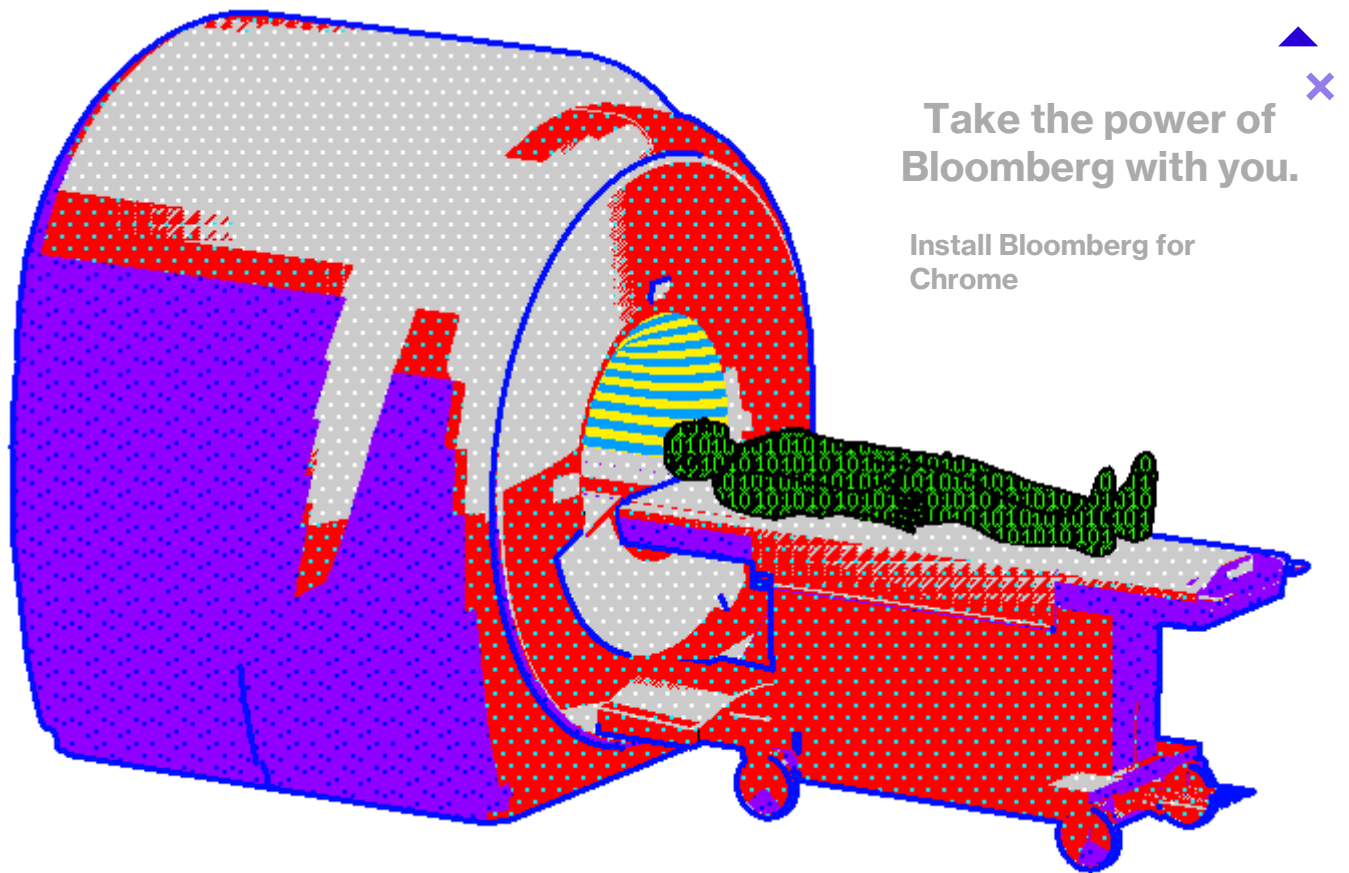
Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome



RIOS GREW INTERESTED IN S
DEVICES AFTER AN ASSIGNME
2013.

PHOTOGRAPHER: GRAEME MITCHELL



Last fall analysts with TrapX Security, a firm based in San Mateo, Calif., began installing software in more than 60 hospitals to trace medical device hacks. TrapX created virtual replicas of specific medical devices and installed them as though they were online and running. To a hacker, the operating system of a fake CT scan device planted by TrapX would appear no different than the real thing. But unlike the real machines, the fake devices allowed TrapX to monitor the movements of the hackers across the hospital network. After six months, TrapX concluded that all of the hospitals contained medical devices that had been infected by malware.

In several cases, the hackers “spear phished” hospital staffers, luring them into opening e-mails that appeared to come from senders they knew, which infected hospital computers when they fell for the bait. In one case, hackers penetrated the computer at a nurses’ station, and from there the malware spread throughout the network, eventually slipping into radiological machines, blood gas analyzers, and other devices. Many of the machines ran on cheap, antiquated operating systems, such as Windows XP and even Windows 2000. The hospital’s antivirus protections quickly scrubbed the computer at the nurses’ station, but the medical devices weren’t so well guarded.

Many of the hospitals that participated in the study rely on the device manufacturers to maintain security on the machines, says Carl Wright, general manager for TrapX. That service is often sporadic, he says, and tends to be reactive rather than preventive. “These medical devices aren’t presenting any

indication or warning to the provider that someone is attacking it, and they can't defend themselves at all," says Wright, who is a security officer for the U.S. military.

After hackers had compromised a medical device in a hospital there, using the machine as a permanent base from which to attack the network. Their goal, according to Wright, was to steal as much information as possible.

A credit card is good only until its expiration date and becomes almost useless as soon as the owner notices that it has been stolen. Medical profiles often contain that same credit card information, as well as Social Security numbers, addresses, dates of birth, familial relationships, and medical histories—tools that can be used to establish false identities and lines of credit, to conduct insurance fraud, or even for blackmail. Simple credit card numbers often sell for less than \$10 on the Web's black market; medical profiles can fetch 10 times as much. For a hacker, it's all about resale value.

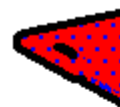
The decoy devices that TrapX analysts set up in hospitals allowed them to observe hackers attempting to take medical records out of the hospitals through the infected devices. The trail, Wright says, led them to a server in Eastern Europe believed to be controlled by a known Russian criminal syndicate. Basically, they would log on from their control server in Eastern Europe to a blood gas analyzer; they'd then go from the BGA to a data source, pull the records back to the BGA, and then out. Wright says they were able to determine that hackers were taking data out through medical devices because, to take one example, they found patient data in a blood gas analyzer, where it wasn't supposed to be.

In addition to the command-and-control malware that allowed the records to be swiped, TrapX also found a bug called Citadel, a type of ransomware that's designed to restrict a user's access to his or her own files, which allows hackers to demand payment to restore that access. The researchers found no evidence suggesting the hackers had actually ransomed the machines, but its mere presence was unsettling. "That stuff is only used for one purpose," Wright says.

Hospitals generally keep network breaches to themselves. Even so, scattered reports of disruptions caused by malware have surfaced. In 2011, the Gwinnett Medical Center in Lawrenceville, Ga., shut its doors to all non-emergency patients for three days after a virus crippled its computer system. Doctor's offices in the U.S. and Australia have reported cases of cybercriminals encrypting patient databases and demanding ransom payments. Auditing firm KPMG released a survey in August that indicated 81 percent of health information

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome



technology executives said the computer systems at their workplaces had been compromised by a cyber attack within the past two

Watching all this, Rios grew anxious for federal investigators to address the vulnerabilities he'd found in the Hospira pumps. He sent reminders to the Department of Homeland Security, and they responded to his suggestions. According to an e-mail from Rios, "not interested in verifying that other pumps are vulnerable."

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome

A few weeks after he received that message, an increasingly frustrated Rios found himself in a vulnerable position: immobilized in a hospital bed, utterly dependent upon, of all things, an infusion pump.

“WE HAVE TO CREATE VIDEOS AND WRITE REAL EXPLOIT CODE THAT COULD REALLY ILL SOMEBODY IN ORDER FOR ANYTHING TO BE TAKEN SERIOUSLY.”

Late last July, Rios began snoring loudly, which interrupted his sleep enough that he went to a doctor, who discovered a polyp inside his nose, near the cerebral membrane. The polyp was removed—a simple outpatient procedure—but days later Rios developed a fever and noticed clear liquid leaking from his nose. Years before, he'd broken it, and the doctors thought the polyp had grown around scar tissue. When the polyp was removed, some of the scar tissue that had protected his brain casing must have been clipped, too. The clear liquid coming out of his nose was cerebral fluid.

He spent two weeks at Stanford Hospital, in a room filled with the kind of gadgetry he'd been breaking into. After a few dazed days in bed, he got his bearings and assessed his situation. His bed was plugged into a network jack. The pressure bands strapped around his legs, which periodically squeezed his calves to aid circulation, were also connected to a computer. He counted 16 networked devices in his room, and eight wireless access points. The most obvious of these was the CareFusion infusion pump, a brand he hadn't looked into yet, that controlled the fluids that were pumped into his arm. "It wasn't like I was going to turn to the doctor and say, 'Don't hook me up to that infusion pump!'" Rios recalls. "I needed that thing."

He noticed that the other patient in his room, separated from him by a curtain, was connected to a Hospira pump. “I kept thinking,” he says. He opted for silence.

When he was able to drag himself out of bed, Rios went into the bathroom, where he gave it a good once-over. He found a wireless card, pushing the buttons on it, seeing what he could do, he recalls. It only inflamed his concerns. “Whatever what password they’re using to let the pump join the network, I could get that off the pump pretty easily.”

In the hallway just outside his room, Rios found a computerized dispensary that stored medications in locked drawers. Doctors and nurses normally used coded identification badges to operate the machine. But Rios had examined the security system before, and he knew it had a built-in vulnerability: a hard-coded password that would allow him to “jackpot” every drawer in the cabinet. Such generic passwords are common in many medical devices, installed to allow service technicians to access their systems, and many of them cannot be changed. Rios and a partner had already alerted Homeland Security about those password vulnerabilities, and the agency had issued notices to vendors informing them of his findings. But nothing, at least at this hospital, had been done. In the hallway, he quickly discovered that all the medications in the device’s drawers could have been his for the taking. “They hadn’t patched it at this point, so I was testing some passwords on it, and I was like, ‘This s--- works!’”

He didn’t touch any drugs, he says, but when he was released, he tried to turn up the heat on Hospira. He’d already told the federal government that he knew how to sabotage the pumps, but after he returned home he decided to make a video to show them how easily it could be done. He aimed the camera directly at the infusion pump’s touchscreen and demonstrated how he could remotely press the buttons, speeding through password protections, unlocking the infuser, and manipulating the machine at will. Then he wrote out sample computer code and sent it to the DHS and the FDA so they could test his work for themselves.

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome



▲
✕
Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome



“We have to create videos and write real exploit code that could really kill somebody in order for anything to be taken seriously,” Rios says. “It’s not the right way.”

But it got the FDA’s attention. Finally, after more than a year of hectoring from Rios, the FDA in July issued an **advisory urging hospitals to stop using the Hospira Symbiq infusion pump** because it “could allow an unauthorized user to control the device and change the dosage the pump delivers.”

“It’s viewed as precedent-setting,” says Suzanne Schwartz, who coordinates cybersecurity initiatives for the FDA’s Center for Devices and Radiological Health. “It’s the first time we’ve called out a product specifically on a cybersecurity issue.”

“There have been no known breaches of a Hospira product in a clinical setting, and the company has worked with industry stakeholders to make sure that doesn’t happen,” says MacKay Jameson, a spokesman for Pfizer.

The medical research community didn’t break out in celebration over the advisory. Hospira said that it would work with vendors to remedy any problems and that the Symbiq model was off the market. But the advisory was merely that: It didn’t force the company to fix the machines that were already in hospitals and clinics, and it didn’t require the company to prove that similar cybersecurity flaws didn’t also affect its other pump models. For some researchers, the advisory felt like a hollow victory.

“It was the moment we realized that the FDA really was a toothless dragon in this situation,” says Mike Ahmadi, a researcher at Rios Security, a cybersecurity sector.

Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome

The FDA’s challenge is a tricky one: to draft regulations specific enough to matter yet general enough to outlast the technology much faster than the products the agency must certify. In a new set of guidelines last October that recommended—but didn’t require—that medical device manufacturers consider cybersecurity risks in their design and development phases and that they submit documentation to the agency identifying any potential risks they’ve discovered. But the onus doesn’t rest solely on manufacturers; Schwartz emphasizes that providers and regulators also need to address the challenge, which she calls one “of shared responsibility and shared ownership.”

Divvying up that responsibility is where things get messy. After the guidelines were published, the American Hospital Association sent a letter to the FDA saying health-care providers were happy to do their part, but it urged the agency to do more to “hold device manufacturers accountable for cybersecurity.” It said device vendors need to respond faster to vulnerabilities and patch problems when they occur. Device vendors, meanwhile, have pointed out that to be hacked, criminals first need to breach the firewalls at hospitals and clinics; so why was everyone talking about regulating the devices when the providers clearly needed to improve their network protections? Hospira, in a statement issued after the FDA advisory, labeled hospital firewalls and network security “the primary defense against tampering with medical devices” and said its own internal protections “add an additional layer of security.” Others have suggested that security researchers such as Rios are pressuring the industry to adopt security measures that might get in the way of patient care.

IT WAS THE MOMENT WE REALIZED THAT THE FDA REALLY WAS A TOOTHLESS DRAGON IN THIS SITUATION.”

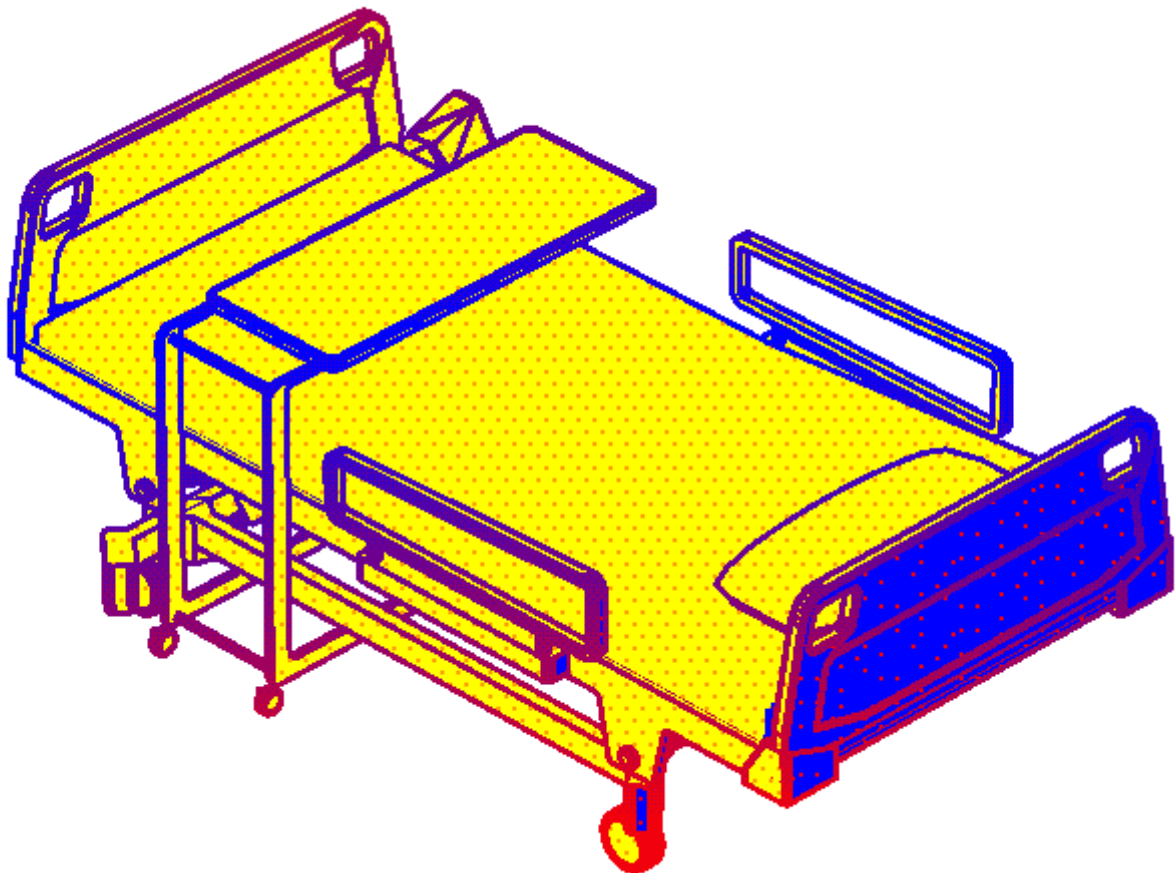
At a forum sponsored by the FDA to discuss the guidelines, an anesthesiologist from Massachusetts General Hospital in Boston used the example of automated medicine cabinets, like the one that Rios had cracked, to make this point. After Rios told the government about the password vulnerability, some hospitals began instituting fingerprint scans as a backup security measure. “Now, one

usually wears gloves in the operating room,” Dr. Julian Goldman told those at the forum. Fumbling with those gloves, fiddling with contaminated blood got near the exposed hands, and it turned out to be a maddening hassle, he suggested, a waste of time. “I can tell you that it certainly doesn’t suddenly need something,” Goldman said, “and as you reach for the drawers, you hear click-click-click-click, you are reaching for the drawers to get access to a critical drug.”

Take the power of Bloomberg with you.

Install Bloomberg for Chrome

Rios says he doesn’t care how manufacturers or hospitals fix the problem, so long as they do something. The Hospira saga convinced him that the only way for that to happen is to continue to pressure manufacturers, calling them out by name until they’re forced to pay attention. That automated medicine cabinet wasn’t the only device he’d found with a hard-coded password; along with research partner Terry McCorkle, Rios found the same vulnerability in about 300 different devices made by about 40 different companies. The names of those vendors weren’t released when the government issued its notice about the problem, and Rios says none of them has fixed the password problem. “What that shows me,” he says, “is that without pressure on a particular vendor, they’re not going to do anything.”



Since the FDA's Hospira advisory was issued this July, boxes of medical devices have continued to arrive on Rios's doorstep in Half Moon Bay. The boxes crowded his office so much that he's been forced to store them in his garage. No one is paying him to try to hack them, but he's covering the expenses. "I've been lucky, and I've done well, so I don't mind for me to buy a \$2,000 infusion pump and look at it," Rios says.

For novice independent researchers, however, access to medical devices can be a forbidding barrier to work in this field. Infusion pumps are relatively affordable, but MRI machines, for example, cost hundreds of thousands of dollars, if not more. And radiological equipment requires a special license. To encourage more research on devices, Rios is trying to establish a lending library of medical equipment; he and a group of partners have begun lobbying hospitals for used devices, and they're hoping to crowdsource the purchase of new ones.

The buzz that surrounded the Hospira advisory this year might have done more to attract new researchers to the field than anything Rios could do. Kevin Fu, a professor of engineering who oversees the Archimedes Research Center for Medical Device Security at the University of Michigan, has been investigating medical device security for more than a decade, and he's never seen as much interest in the field as he's noticed this year. "Every day I hear of another name I hadn't heard before, somebody who hadn't been doing anything with medical devices," Fu says. "And out of the blue, they find some problems."

On a sunny fall day in Half Moon Bay, Rios grabs an iced coffee at a Starbucks in the city center. He's fresh off a week of work in Oklahoma—one of those assignments he can't talk about—and he's looking forward to some family time. Maybe in a spare moment, he'll grab one of the devices in his office and see what flaws he can find inside it.

One of those machines is exerting a powerful pull on him, as if begging to be hacked. After he was released from the hospital last year, he surfed around online and found the same CareFusion pump that had been tethered to him for two weeks. It now sits near a filing cabinet in his office.



Take the power of Bloomberg with you. is l
Install Bloomberg for Chrome



FEATURED IN BLOOMBERG BUS
2015. **SUBSCRIBE NOW.**
PHOTOGRAPHER: GRAEME MITCHELL

“It’s next,” Rios says.

Editor: Bryant Urstad
Design and Illustration: **Steph**
Glitches: **Toph Tucke**



Take the power of
Bloomberg with you.

Install Bloomberg for
Chrome