Can You Trust Your Fridge?

TODAY'S INTERNET OF THINGS IS FULL OF SECURITY FLAWS. WE MUST DO BETTER

By Alan Grau • Illustration by J.D. King

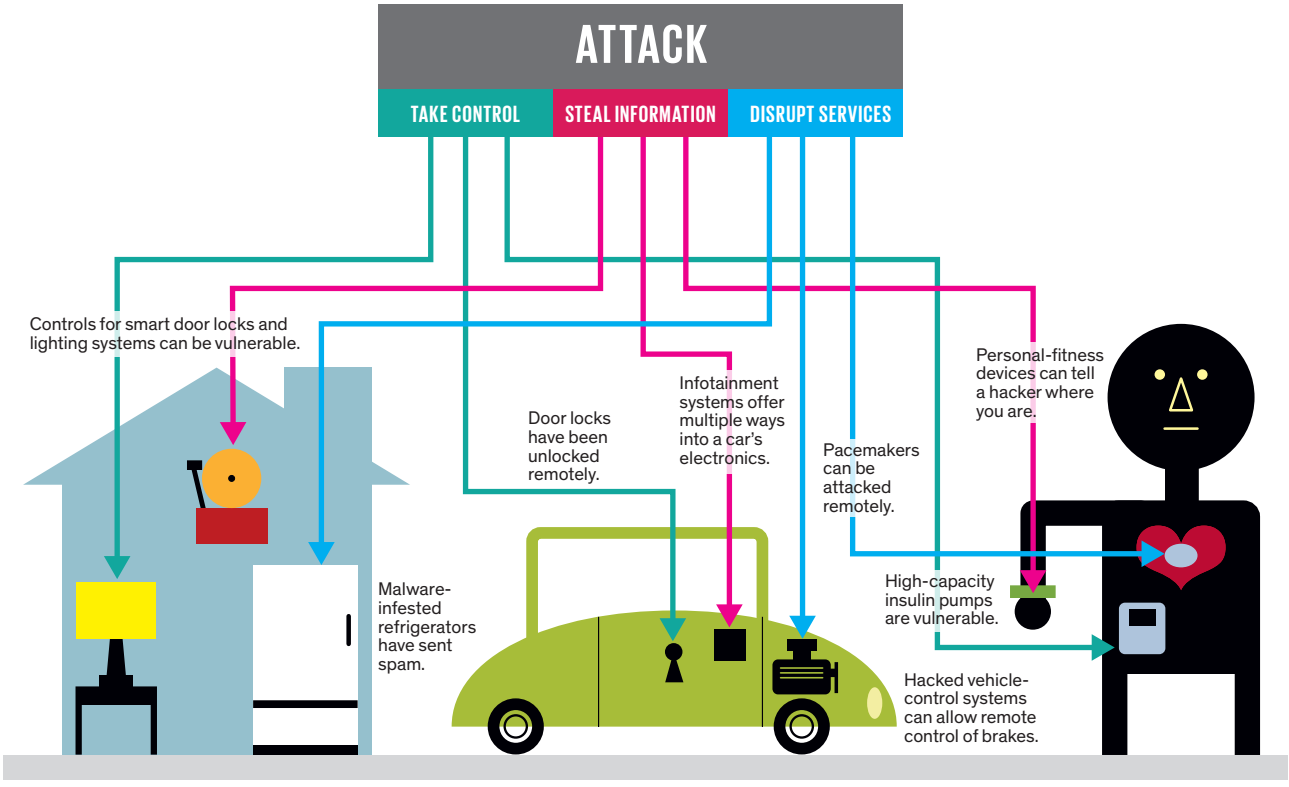
Imagine a criminal using your nanny cam to watch your house or to scream at your child—or even to post footage of your home on a crime boss's website. And suppose your refrigerator were spewing spam e-mail, enraging people you'd never even met.

The Internet of Things has been touted as many things. But what you haven't heard is that it could be your worst enemy. Yet all of these incidents have actually occurred, according to news reports. And it's likely that even more disturbing transgressions have been taking place unbeknownst to homeowners. For example, researchers have discovered that in some cases, they can hack the Internet of Things to intercept each document you print and divert it to a remote site, use your smart TV to bug your house, and even control the traffic light on the corner outside your home.

For although the Internet of Things offers great convenience by linking our gadgets—an estimated 50 billion of them worldwide by 2020—it can also let hackers take control of your house, your car, and even your body.

The vulnerabilities lie all around you. A recent HP Research study reported that the average Internet of Things gadget has an astounding 25 security flaws, and 70 percent have at least one such vulnerability. Many of these problems may yield to solutions like those adopted by the personal computer industry decades ago. As I'll explain later, there are also some that require new approaches that take into account the vast scale and narrow profit margin of the emerging world of Internet-augmented products.

LET'S START WITH YOUR HOME. Your smart meter—if you don't have one, you soon will—can turn off selected appliances, such as air conditioners, whenever the power network is close to being overwhelmed. That's fine. What's not so fine is if a hacker gets into your home's smart meter and makes it cut off elec-



NO PLACE TO HIDE: With the Internet of Things spreading throughout our homes, cars, and even bodies, new vulnerabilities seem to emerge almost daily. The smart locks and security systems in your home could be disabled by a would-be burglar. Your car could be forced to unlock its doors and start its engines; a thief would only have to get in and drive. Implanted pacemakers and insulin pumps are also vulnerable to hacking.

tricity to security systems. That would certainly simplify a burglary attempt. A Web-connected security system could also be hacked directly, with a hacker using a brute-force attack to guess your password. In fact, a Russian website may have already done the job. The site, which was recently shut down, provided links to 73,011 locations with unsecured security cameras in 256 countries. In an unrelated incident, a hacker in Cincinnati compromised a baby monitor and used it to scream at a sleeping infant.

Or perhaps you have the latest smart locks, the kind that let you use your smartphone at a distance to open the front door for a guest. Perhaps you also have Web-connected lighting systems. Wouldn't a would-be burglar love to unlock the doors, turn off the lights, and disable your home security?

Now consider your car. It has or soon will have the ability to record and report diagnostic information, remotely start and turn on the heat when signaled by your cellphone, and use integrated GPS, map, weather, and traffic data to select the best route. But these capabilities also mean that hackers can remotely flash your car's lights, enabling them to identify it on your street, unlock the door, start the engine, and drive it away. Hackers might even gain control of the car while you're driving it, thanks to malware that infected the car when it communicated with a computer back in the repair shop. In February 2014, the U.S. Department of Transportation began working on a regulatory proposal that would require all new vehicles to be equipped with car-to-car and car-to-infrastructure communication capability, providing yet another path for reaching into automobiles remotely.

Your body itself may not be safe from hackers. Already patients are being monitored and even treated with medical devices like pacemakers and insulin pumps, ventilator systems and blood chemistry monitors. These products are connecting to the Internet because it's so much better to monitor patients in their homes than in medical facilities. But if a personal health device connects to the Internet, it can be hacked.

In an episode of the TV show "Homeland," a murderer kills remotely by accelerating a heart pacemaker—a trick that hasn't been reported in real life but has been demonstrated in the lab. In fact, doctors disabled the wireless capabilities in the pacemaker of former U.S. vice president Dick Cheney to protect him from such malfeasance. If this kind of attack happened to an implanted pacemaker, we might never know; it might be impossible to distinguish between a product malfunction and a cyberattack. Researchers have also demonstrated that insulin pumps, used to help control diabetes, can be remotely instructed to pump out all their insulin at once, killing or severely injuring the user. The same applies to pain medication pumps.

More subtle hacks might be tried to avoid arousing suspicion. A criminal might tweak a monitoring system so it would report that a dangerously sick patient was just fine.

ICONS: J.D. KING

INFILTRATING THE INTERNET OF THINGS (or IoT, for short) doesn't necessarily require a dedicated computer coder gone bad, willing to devote long hours to finding a vulnerability. These days, an amateur hacker can download existing tools and use them to conduct a basic attack. On the other end of sophistication, organized crime and nation states have entered the hacking game.

Unlike business computers, which for decades have been sheltered behind corporate firewalls and intrusion detection and prevention systems (IDPS), the products now being linked to the Internet are frequently on their own. A Columbia University study that ran a set of attacks against business systems and embedded systems in such consumer products as home entertainment systems, webcams, and Wi-Fi access points found problems in just 2.46 percent of the business products—and a whopping 41.62 percent of the consumer products. Even in those products that do have shields, the protections are often not enabled or are undermined by the use of default or weak passwords.

Too many manufacturers worry more about getting a product to market quickly than securing it. In some cases, a manufacturer has taken an apparatus designed for use in a private network and simply connected it to the Internet without building in any protection to speak of. It's also true that the devices themselves are often so small that it's hard to build in the right protection.

And most IoT products, even if secured, have no way to automatically update their security software when vulnerabilities are discovered. As things now stand, bad actors can exploit any vulnerability they find for as long as the 10 or even 20 years the devices remain in use.

The situation has got to change. Product makers—and the people who use these gadgets—have to protect against hacking. And it is possible to do it.

HACKERS WHO ATTACK ALL THESE SYSTEMS—home, car, and health—are typically trying to do one of three things: take control of the apparatus, steal information, or disrupt service.

Taking control of the apparatus means somehow logging in as an authorized user, perhaps by figuring out the password, finding a backdoor, or compromising the authentication mechanism. Strong authentication methods—such as randomly generated passwords; secure, token-based authentication; biometric authentication; and certificate-based authentication—can make this much more difficult.

Stealing information can mean eavesdropping or getting into the systems and collecting data, such as patient information from a medical device or credit card numbers from a TV used for home shopping. It can also mean using a product like a phone system, printer, or video camera to collect and transmit data. Disrupting service usually means flooding a system, such as a home-security or vehicle-control system, with messages in order to make it unable to function.

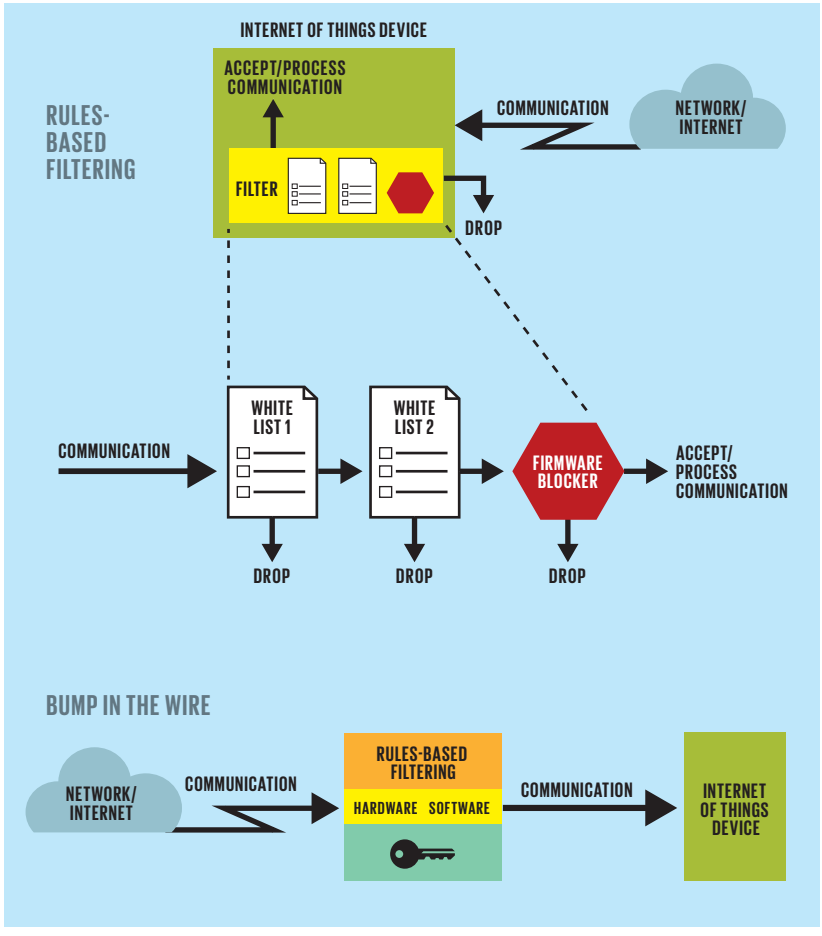
The simplest way to stop all these attacks is by preventing hackers from communicating with the gadgets they are trying to hack. And that means using a firewall and an IDPS.

A firewall acts as a gatekeeper, blocking traffic that should not be permitted to pass through. An IDPS monitors the computer

EMERGING STANDARDS FOR IoT SECURITY

Security standards for IoT products are evolving. Most of the current standards came out of a specific industry or application—for example, the North American Electric Reliability Corp. has set critical infrastructure protection (CIP) standards to secure the electric grid, the U.S. Food and Drug Administration has a set of guidelines to help product makers better protect patient health and information, and the National Institute of Standards and Technology has created the somewhat broader Cybersecurity Framework to help the financial, energy, and healthcare industries. Some relate peripherally to the Internet of Things. But new standards specifically targeted at the IoT are beginning to emerge. These include:

- **The Industrial Internet Consortium:** The Industrial Internet describes a world in which physical manufacturing and other machinery connects with sensors and software that gather data, analyze it, and use it to adjust the machinery—essentially, the nonconsumer IoT. The IIC was created to make sure that products from different companies can easily share data; its members will be building security protections into its reference architectures.
- **The Open Interconnect Consortium:** This group of technology companies, such as Cisco, Intel, and Samsung, is developing interoperability standards for the IoT and will consider security as it does so.
- **The International Standards Organization's (ISO) Special Working Group on the Internet of Things:** This group is assessing existing standards that might apply to the IoT along with current efforts to develop standards; it plans to help guide their evolution to better account for security. For example, this may mean that the world's most widely adopted family of information technology security standards, ISO 27000, gets an update that will make it able to work better with the IoT.
- **IEC 62443/ISA99, Industrial Automation and Control System Security Committee:** This committee develops security standards and technical reports that define procedures for implementing secure industrial automation and control systems.
- **A number of IEEE standards address elements of security that can be applied to the Internet of Things,** including IEEE P1363, a standard for public-key cryptography; IEEE P1619, which addresses encryption of data on storage devices; IEEE P2600, a standard that addresses the security of printers and copiers; and IEEE 802.1AE and IEEE 802.1X, which address media access control security.



DEFENSIVE WEAPONS: Rules-based filtering [top] uses a small set of policies—such as no unauthorized remote updates of embedded firmware—to block dangerous commands from getting past a simplified firewall. Rules-based filtering systems can also consult white lists of trusted computers so that only "good guys" have access to certain functions. A "bump in the wire" approach relies on a small, dedicated piece of hardware and software that sits between an IoT device and the Internet; a bump in the wire can shield devices that don't have built-in protection.

system and the network to which it is attached to detect, block, and report suspicious activity. But the software for firewalls and antivirus programs takes up a lot of storage space and requires a lot of processing power to run. Most things in the Internet of Things can't handle the software.

WE HAVE TO TAKE A DIFFERENT APPROACH. For the most part, the gadgets that make up the Internet of Things are what we call embedded systems—that is, dedicated computers that perform specific functions within more complex systems. For instance, they might control the operation of a machine within a water-processing plant, manage the lighting of a smart home, or monitor an organ in the human body. Limiting the function means they can be small, fast, and efficient.

The security systems must be just as specialized, protecting only against the specific attacks to which the equipment is vulnerable. Yet we don't want to completely reinvent the wheel each time we create a new smart thermostat or television, so we also need a system that's flexible enough to shield devices as diverse as automobile communication gateways, home printers, and smart door locks.

To do this, you need to pay as much attention to what you omit from the embedded security system as to what you include. What we don't need are systems with powerful processing engines and large databases of virus signatures and other chunks of code that act as fingerprints to help detect known threats. Instead of databases, IoT security can use rules-based filtering.

To understand how this works, let's look at a home printer; it's similar to a lot of other IoT devices. A printer has only a few communication ports and a limited number of communication protocols. It supports both print commands, which may be sent from any other device, and administrative commands that are accepted only if received from a few predetermined computers. A small set of simple firewall policies known as a white list is all it takes to enforce these two distinct communication policies. One set of white-list rules allows communication from any device that knows the printing protocols. Another white list specifies that administrative commands will be processed only if they are from a machine on the white list. An additional rule blocks print commands that contain embedded firmware updates to make sure that malicious users cannot modify the behavior of the printer.

The complete firewall policy may consist of as few as 5 to 20 rules as opposed to the 200 to 2,000 rules of a typical business computer's firewall. This smaller, faster, simpler approach to an IoT security system does not compromise security; it allows anyone to print with the machine while preventing malicious users from changing settings, downloading firmware, or performing other harmful actions (like sending copies of anything you print to a third party). Other, specific sets of rules could protect door locks, cars, or pacemakers.

SOME OF THE MAJOR PLAYERS in the embedded-systems market—Green Hills, Intel, McAfee, Mentor Graphics, Renesas, Wind River, and Zilog—are already incorporating such embedded security technology into the hardware and software building blocks used for IoT devices. These companies typically don't make the connected products themselves but rather the processors and operating systems used to build IoT equipment. But given that some devices in the Internet of Things are rarely replaced, it will likely take a decade or two—or more—to bring all systems up to modern security standards. New systems

ILLUSTRATION BY Mark Montgomery

will likely have higher levels of security, but vulnerabilities are bound to exist for the foreseeable future.

There are two approaches for securing existing systems. For newer products that support software updates or those that are still being developed, the manufacturer can build a firewall and security capabilities into the product's software. The makers of gadgets like the Nest thermostat can take this approach. Many older systems have communication capability but don't support software updates—say, older hospital-monitoring systems and older factory-control systems. Here it may be possible for consumers or the product manufacturer to add a firewall through the "bump in the wire" approach. This refers to a box sitting between the target apparatus and the Internet that contains hardware and software to shield the device from attack. My company, Icon Labs, makes such a system, the Floodgate Defender. Tofino Security and Innominate Security Technologies offer similar products.

As equipment becomes more secure, this approach may no longer be needed, but it provides an immediate solution for vulnerable items.

A FIREWALL, HOWEVER, isn't enough to protect the Internet of Things against hackers. That's because manipulation isn't the only problem—there's also eavesdropping.

Data encryption is therefore needed also. Smart locks and heart pacemakers need strong passwords, the kind that include letters, numbers, and perhaps special characters as well. Even better, products should include certificate-based authentication—that is, an electronic document that identifies an individual, a piece of equipment, or some other entity addressing the gadget. This technology is used today in point-of-sale terminals, gas pumps, and ATMs, and it will likely be incorporated into future versions of home medical devices and home security solutions. It hasn't reached these products yet in part because manufacturers haven't invested in the up-front engineering effort necessary to make this kind of security work with their hardware.

One reason for the lag is the market itself. These are high-volume, low-margin products, so the cost of additional memory and a faster processor could make a product less competitive. Even worse than cost, though, is the problem of integrating a product with the other Internet-linked products in a home. For example, if a smart door lock uses certificate-based authentication, then the smartphone that communicates with the door lock must also handle such authentication. Working this all out in a way that is easy for the consumer to use will take time.

To make the Internet of Things even more secure, product manufacturers can integrate a device-management agent into their products. This piece of software would allow the product to communicate with a security management system, like the McAfee ePolicy Orchestrator. The agent would report things like failed access attempts and attempted denial-of-service attacks.

It could also be used to update security software as threats emerge. Again, the trick is going to be getting this to work without making the devices that use it a lot more expensive and unduly complicated. Industry is just starting to work on this approach.

In the meantime, there are a few things you can do to protect your connected gadgets. If you are on a personal computer or mobile device, make sure that any available firewall and antivirus software is activated and up-to-date. Make sure you scan your system regularly to identify and remove any malware or possible intrusions. A computer infected with malware or breached by a hacker can be a launching point for attacks against the IoT equipment in your home, or it may store passwords for IoT products that the hacker can use.

If your apparatus allows you to set user names and passwords, make sure to turn that capability on and also create passwords that are not easy to guess. Don't use your name, your kids' or spouse's names or birthdays; do use unique spellings, number combinations, characters, and symbols, such as ampersands, question marks, or asterisks. I know, you've heard this all before, but it bears repeating because too many people still are setting their passwords as "password."

Finally, watch out for phishing and social engineering. Hackers are very clever when it comes to sending e-mails and messages that ask for user names and passwords. Be very suspicious. If you get a phone call asking for this confidential info, don't give it. Make sure you hang up and then call the number of the business or organization that the caller had claimed to represent. Don't use any phone number the caller may provide.

The situation will get better. Manufacturers are becoming more aware of the need to protect their Internet-connected products. Research is under way to develop new biometric authentication methods for the mobile devices you use to control your Internet of Things, providing authentication based on retinal scans, hand geometry, facial recognition, and other hard-to-spoof human attributes. The fingerprint authentication introduced in Apple's iPhone 5s is a huge step in the right direction.

And consumers are slowly developing good judgment. By combining commonsense methods with state-of-the-art security technologies, we can prevent hackers from turning our devices against us.

In the not-too-distant future, self-driving cars, wearable gadgets, and smart homes will communicate without our constant monitoring, automating many of our everyday tasks. Robots—guided by GPS beacons and connected sensors—will assist in firefighting, law enforcement, and search-and-rescue operations. Wearable and implanted health-care systems will take care of us outside of doctors' offices. But we will be unlikely to use any of these amazing new technologies if we don't remove the fear of cyberattack and build what is truly an Internet of *Secure* Things. ■

POST YOUR COMMENTS at http://spectrum.ieee.org/internetofthings0315