How Many Back Doors Do Your Devices Have?

by Yosef Beck

Without uniform standards, splintered software development—and a little common sense—could ward off security concerns for a while.

When was the last time you checked the permissions your coffeepot was requesting? Welcome to the Internet of Things, or "IoT" as those in the know call it.

At a basic level, IoT means putting computing power into everyday devices and connecting those computers (big and small) to the Internet. The way the trend is progressing, everyone and everything will soon be connected, sending and receiving data.

Many of us have probably purchased an IoT device at some point, perhaps without even realizing it. A 2014 survey by the Acuity Group, "The Internet of Things: The Future of Consumer Adoption," found that 87 percent of consumers hadn't heard the term, while 64 percent had never purchased an in-home IoT device such as a smart smoke detector because they did not know they were available.

What do IoT devices promise? Let's look ahead: Your new and improved Fitbit is intelligent enough to know you did not sleep last night. It tells your coffeepot to make an extra strong cup of coffee, while it records your sleep patterns to the cloud. You're late for a meeting and run out the door, forgetting your extra strong cup of coffee. Your coffeepot logs this to the cloud as well. These and other IoT devices continue to collect and sync data to the cloud throughout the day.

At the end of the week, you get a smartphone notification summarizing your personal performance. This week, the report highlights why you did not operate at the top of your game and recommends changes for next week. One recommendation: Move an upcoming, early-morning meeting to ensure that you have time to eat a full breakfast. Based on this information, would you change your behavior the next week?

If not, these IoT devices could intelligently adjust their suggestions to increase the likelihood that you'll modify your behavior—perhaps by adjusting your alarm clock or adding extra gym time to your schedule.

The future holds the promise of amazing, connected, and smart devices, potentially helping you improve every aspect of how you manage and live your life.

As with any technology, there are plenty of opponents. There are the "change is bad" arguments, as well as fears that the technology will create more complexity and headaches than simplicity. Perhaps most importantly, some argue that security issues with IoT devices could lead to potential nightmares for manufacturers and end users.

Where does the nightmare start? For years, cars have had computers installed to help improve fuel efficiency, increase power, better control emissions, etc. Today, more and more cars come preinstalled with Internet access. This combination of computer-controlled cars with access to the Internet can lead to some amazing opportunities for humankind.

Cars would be able to interact with each other, as well as with roads, bridges, or traffic lights. This could lead to better traffic flow and routing, fewer accidents, increased awareness of upcoming hazards—such as an icy bridge, with a warning for the car to slow down—as well as many other potential improvements.

On the flip side, a hacker on the other side of the world could access your car's controls through the Internet. The hacker could lock you inside, slam on the brakes, and drive you into a wall. A terrorist organization could use this power to create incredible damage without using suicide bombers. The list of horrible scenarios is endless.

In the last year, hackers remotely controlled a Chrysler Jeep Cherokee through its OnStar technology. They hacked into a Tesla S sedan through multiple security holes. These attacks were not easy, and in some cases, took more than a year to accomplish in a lab setting. While some of the examples may be extreme, they draw attention to the importance of approaching IoT with caution.

Returning to our coffeepot example, you love the ease and simplicity of the coffeepot app (that you downloaded for free!), which allows you to remotely start brewing a cup of coffee before you walk in the door after a long day.

Little do you know, your coffeepot has been compromised through the app and, because it has access to the rest of your network, a hacker now has access to your personal server where you store scanned copies of all of your personal documents. The hacker makes a measly $100 selling your identity on an Internet forum, six months before you find out your credit score is trashed.

Obviously, there are tradeoffs. As an individual, the ability to zip through traffic in your smart car toward a cup of coffee brewed by your smart coffeepot has some allure. For businesses, IoT opens amazing growth opportunities in terms of potential products and marketplaces.

Alternatively, IoT also opens up huge security risks for both individuals and businesses. Can you imagine the horror that the CEO of Mr. Coffee, Hamilton Beach, or Cuisinart might feel upon opening up *The Wall Street Journal* and reading that coffeepots are attacking their owners?

The Internet itself is not secure, so it is hardly fair to expect that IoT devices will automatically be secure. Much like early online banking, security standards are being developed for IoT devices and their software as the technology develops. When building a product, IoT developers must think through the ramifications of their products and keep security at the forefront of their minds.

In the absence of security and device standards, there are actually two big advantages to initially taking a splintered approach to IoT device development.

The first is that the target is just not big enough to attract many criminal hackers—which is exactly why hackers more often target Windows PCs versus Macs, or Android versus Windows phones.

Second, if one IoT device has a security issue, it's probably unique to that device and does not affect all others. Again, this is similar to the fragmentation among Android devices. If Samsung Android devices have a security flaw, it does not necessarily expose all Android devices worldwide.

As end users, we need to be savvy customers by researching IoT device security before purchasing, staying up to date on software, and applying security patches and updates as soon as they are available. In the Chrysler hacking example, Chrysler addressed the vulnerability and created a security patch, which resolved the issue; however, the end user had to manually install the update.

Don't let devices access more than they need to on your network; setting up a guest network for visitors may be helpful. When available, review the permissions you grant to your devices. IoT developers should also consider this when building their devices and accompanying software, allowing the end user more granular control over a device's permissions. In the coffeepot example, you could choose to allow it to consume data from your alarm clock in order to know when to start brewing, but you could also choose to restrict it from publishing that data to the cloud.

Use common sense. If a "dumb" device works just as well as a more expensive "smart" one, why opt for the "smart" one? Perhaps the best example is the Internet-connected hot water heater. Do you adjust your water heater's temperature often enough to justify doing it with your smartphone?

Yosef Beck
yosef.beck@jabian.com

87% OF CONSUMERS HAVEN'T HEARD THE TERM "IoT," ACCORDING TO A 2014 SURVEY BY THE ACUITY GROUP.

© 2016 JABIAN, LLC. ALL RIGHTS RESERVED.