Website rates security of internet-connected devices

3 September 2019

A row of cameras is among the internet-connected devices whose security has been assessed by researchers from Georgia Tech and the University of North Carolina. Credit: Allison Carter, Georgia Tech

If you're in the market for an internet-connected garage door opener, doorbell, thermostat, security camera, yard irrigation system, slow cooker—or even a box of connected light bulbs—a new website can help you understand the security issues these shiny new devices might bring into your home.

Consumer-grade internet of things (IoT) devices aren't exactly known for having tight security practices. To save purchasers from finding that out the hard way, researchers from the Georgia Institute of Technology and the University of North Carolina at Chapel Hill have done security assessments of representative devices, awarding scores ranging from 28 (an F) up to 100.

Their site, https://yourthings.info, shows rankings for 45 devices, though a total of 74 have been evaluated. That's hardly a complete roundup of the tens of thousands of device types available, but the big idea behind the project is to help consumers understand important issues before connecting a new IoT helper to their home networks.

"A lot of people who purchase these devices don't fully understand the risks associated with installing them in their homes," said Georgia Tech Graduate Research Assistant Omar Alrawi. "We want to provide insight by providing security ratings for the devices we have tested."

Voice-activated personal digital assistants are among the most common home IoT devices, but if not properly installed, they can provide unwanted access to the home networks to which they are connected, warned Manos Antonakakis, a cybersecurity researcher and associate professor in Georgia Tech's School of Electrical and Computer Engineering.

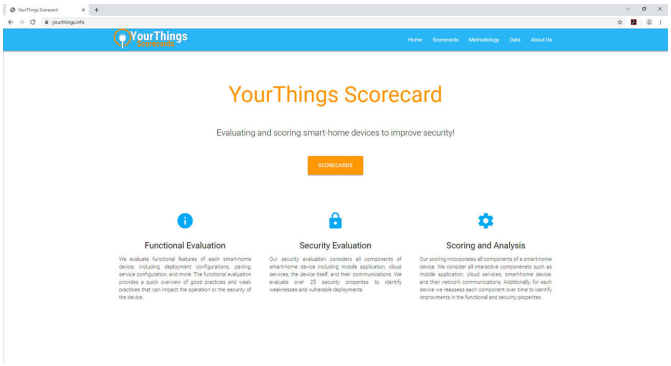
"If you have an IoT app that is vulnerable, whoever has access to that app not only has access to your personal information, but could also jump into your home and eavesdrop on your conversations," he said. "Anything that is connected in the home in proximity to the personal assistant could also interact with it. If there is vulnerable software running on the device, it could be exploited within the home network."

One problem is that most home networks were set up for simple tasks like sharing printers, so they lack the kind of security controls found on enterprise systems at businesses, noted Chaz Lever, a research engineer in Georgia Tech's School of Electrical and Computer Engineering.

"The home network is beginning to look a lot like enterprise networks with a range of services that have to be protected," Lever said. "But the average consumer is not going to be equipped to do that. They don't have an IT staff that is doing audits and securing the devices. If these devices are not secure out of the box and there aren't easy ways to secure them, they can open the home up to a new

vector of attacks."

To give consumers helpful advice, the researchers developed a framework for analyzing security components of the devices. In what is believed to be the first effort to objectively assess the risks of IoT equipment, they examined the devices themselves, how the devices communicate with cloud servers, the applications running on the devices, and the cloud-based end-points.



Homepage for the Internet of Things security website developed by researchers from Georgia Tech and the University of North Carolina. Credit: Georgia Tech

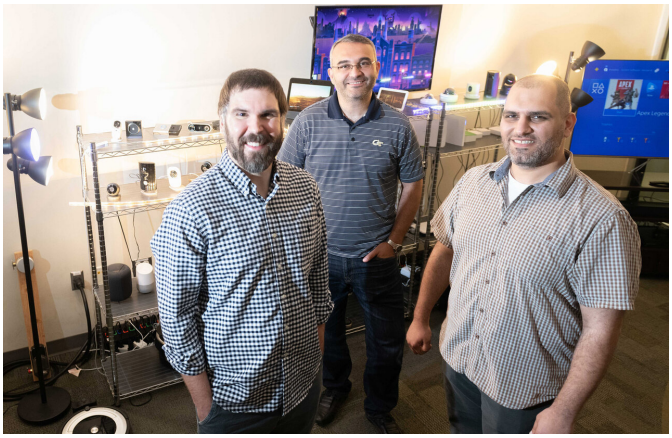
"The more services running on the device, the higher the probability that some of them will be vulnerable to attack," Antonakakis said. "Providing many services may be attractive from a marketing perspective, but if you have multiple services, the risk increases."

In their study of IoT devices, the researchers found wide variations in security depending on the manufacturer. In some cases, equipment made by small and lesser-known companies performed better than devices made by larger companies.

"There are some devices that do security really well, and other manufacturers should learn from those exemplary devices," Alrawi said. "We saw the full spectrum of good and bad, and sometimes we were surprised at the results of our evaluation."

Because they are designed to be installed by consumers, these IoT devices must be easy to use. However, sometimes ease of use is the enemy of security. An example is a service known as UPnP, which makes devices known to the network during installation so communications can be established.

But a device announcing itself on the network can attract attackers, Lever noted. "It's helpful for the devices to communicate what they do, but that opens up vulnerabilities. The choice of protocols affects not only the device, but also the security of the network on which it is running."



Georgia Tech researchers Chaz Lever, Manos Antonakakis and Omar Alrawi are shown with a collection of internet-connected devices they have assessed in their lab. Credit: Allison Carter, Georgia Tech

Internet-connected light bulbs are unlikely to have a long service life, but that's not the case with expensive appliances like internet-connected refrigerators. Antonakakis worries that these devices could become security risks without regular updates.

"Ideally, the consumer shouldn't have to be aware that their refrigerator needs updates that have to be downloaded to the device," he said. "We want that to happen automatically and securely. Why should anyone have to know how to patch their refrigerator?"

While the notion of hacking a slow cooker might

seem amusing, the devices have heating elements that could cause a fire if a malicious actor turned up the temperature. Attacks can also affect more than a homeowner. In 2016, the Mirai botnet took advantage of unsecured Internet-connected cameras—many of them baby monitors—to create a massive distributed denial of service attack that left much of the internet unavailable.

Beyond educating consumers, the researchers hope to encourage better security by device manufacturers by tracking security trends over time.

"We hope to inspire both technical and policy next steps," said Antonakakis. "There is a need for establishing policy and standards. We want to raise the security level of all these devices. There is a lot more that could be done."

Provided by Georgia Institute of Technology