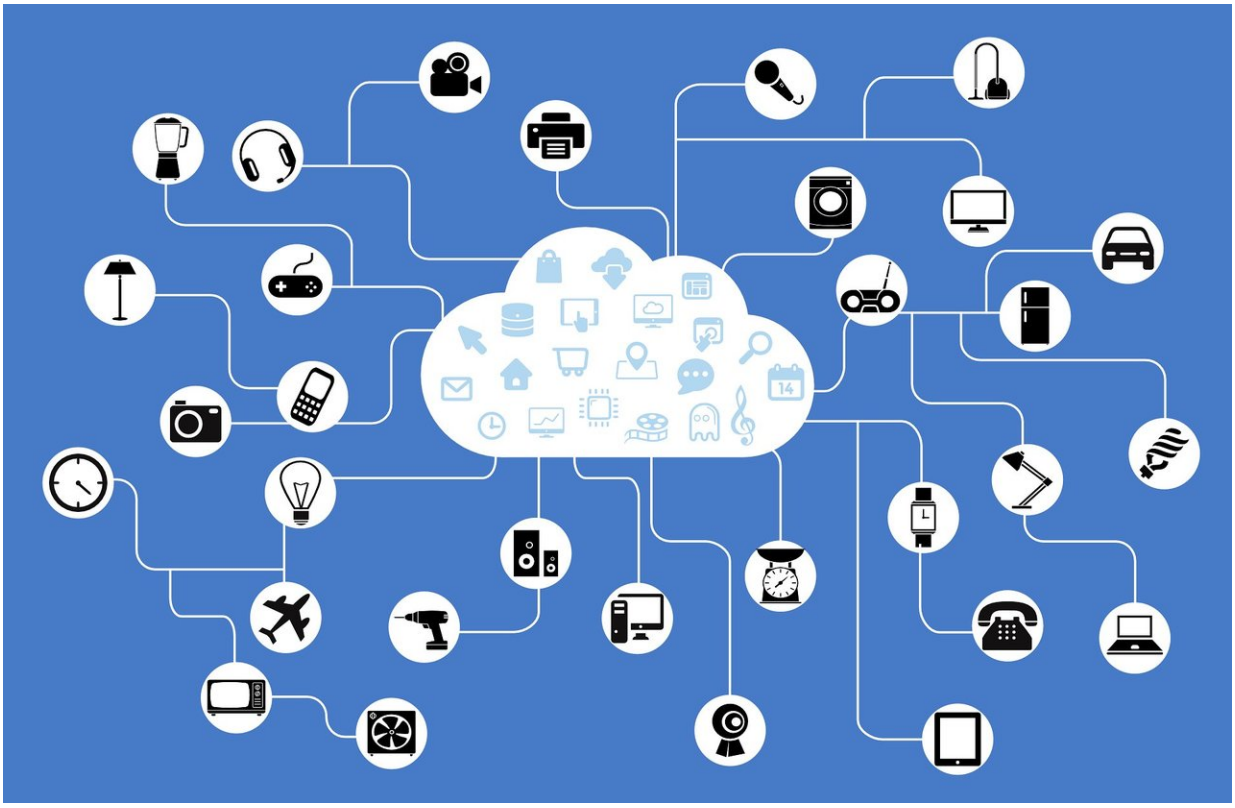
A team's tool can inspect the secret life of your smart home items

April 16 2019, by Nancy Cohen



Credit: CC0 Public Domain

An IoT message from a group of computer scientists from Princeton University and University of California, Berkeley: "Our smart devices are watching us. It's time for us to watch them."

A research team has been calling attention to security and privacy risks involved if devices are designed with poor security practices—hard coded passwords, lack of strong authentication and not running updates.

They also point to performance risks. A user may have a large number of IoT devices in his/her home competing for limited bandwidth, which may degrade the overall performance of the home network.

From bulbs, plugs and sensors to TVs and kitchen appliances, owners should know what is happening. "If you want to see the invisible activity in your home (or in your Airbnb), this is a nice option," said Kashmir Hill in *Gizmodo*. She was talking about the Princeton IoT Inspector.

(Face it, wrote Hill, "If you build it, a wireless connection will come for it. These smart devices are always on, always connected, and often up to more than you realize.")

Specifically, IoT Inspector can tell you who the IoT device contacts on the Internet, and whether the contacted party is malicious or is known to track users; how much data is exchanged (in terms of bytes per second) between the device and the contacted parties; and how often the data is exchanged. Danny Huang, a postdoctoral fellow at Princeton's Center for Information Technology Policy, is lead developer.

The team's blog description reveals its special value: ease of use. You could inspect IoT traffic in your home network "right from the browser. With a one-click install process, you can watch how your IoT devices watch you within minutes of setup."

(Hill said she road-tested it, or rather house-tested it, and found it "incredibly easy to install and use.")

Actually, the researchers have their eyes on the prize. They want to make

a difference for academic researchers as well as the consumer, to learn what minds you. They are out to measure and visualize risks. One can learn more about IoT devices and contribute to IoT research.

They are to release findings in a journal/conference publication.

They stated: "With IoT Inspector, we are the first in the research community to produce an open-source, anonymized dataset of actual IoT network traffic, where the identity of each device is labelled."

Wait, what? Will privacy be a worry for those who use this tool? IoT Inspector collects and sends the information above to the researchers only when it is running, they stated; moreover, it does not collect the actual contents of communication, personally identifiable information, such as IP address, MAC addresses of your devices, name and email.

"We used IoT Inspector to monitor a number of IoT devices in our lab."

Even if you do not want to enlist in the study their blog is worth reading to see what they unearthed when they turn the tool on themselves, using IoT Inspector in their lab. In future posts, you will get to see IoT Inspector unearthing how smart TVs contacted advertising/tracking services as they watched TV; and learn that a WiFi-enabled camera was communicating with a number of countries, including Russia, Czechia, India and Brazil.

For macOS only, you can download right away; for Linux and Windows, you join a waitlist. You can run the app on laptops and desktops.

Natasha Lomas, *TechCrunch*, said that "Up to 50 smart devices can be tracked on the network where IoT Inspector is running. Anyone with more than 50 devices is asked to contact the researchers to ask for an increase to that limit."

More information: iot-inspector.princeton.edu/
iot-inspector.princeton.edu/blog/