Is someone watching you online? The security risks of the Internet of Things

21 March 2016, by Patryk Szewczyk And Nikolai Hampton

Internet connected devices like webcams are the tip of the iceberg when it comes to the Internet of Things. Credit: DAVID BURILLO/Flickr, CC BY-SA

The range and number of "things" connected to the internet is truly astounding, including security cameras, ovens, alarm systems, baby monitors and cars. They're are all going online, so they can be remotely monitored and controlled over the internet.

Internet of Things (IoT) devices typically incorporate sensors, switches and logging capabilities that collect and transmit data across the internet.

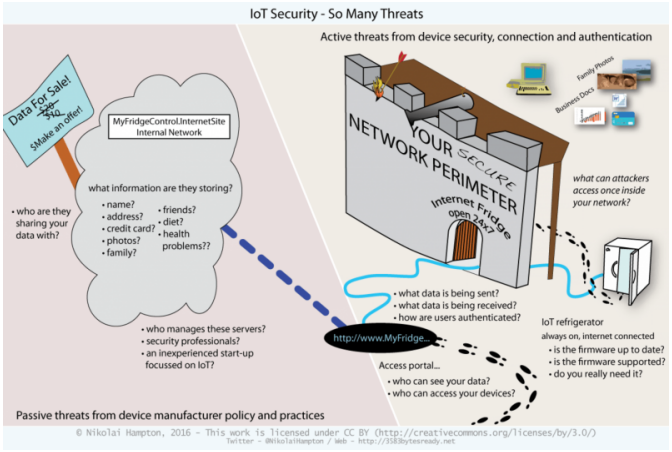
Some devices may be used for monitoring, using the internet to provide real-time status updates. Devices like air conditioners or door locks allow you to interact and control them remotely.

Most people have a limited understanding of the security and privacy implications of IoT devices. Manufacturers who are first-to-market are rewarded for developing cheap devices and new features with little regard for security or privacy.

At the heart of all IoT devices is the embedded firmware. This is the operating system that provides the controls and functions to the device.

Our previous research on internet device firmware demonstrated that even the largest manufacturers of broadband routers frequently used insecure and vulnerable firmware components.

IoT risks are compounded by their highly connected and accessible nature. So, in addition to suffering from similar concerns as broadband routers, IoT devices need to be protected against a wider range of *active* and *passive* threats.



There are many security threats to the Internet of Things.

Active IoT threats

Poorly secured smart devices are a serious threat to the security of your network, whether that's at home or at work. Because IoT devices are often connected to your network, they are situated where they can access and monitor other network equipment.

This connectivity could allow attackers to use a compromised IoT device to bypass your network security settings and launch attacks against other network equipment as if it was "from the inside".

Many network-connected devices employ default passwords and have limited security controls, so anyone who can find an insecure device online can access it. Recently, security researchers even managed to hack a car, which relied on readily accessible (and predictable) Vehicle Identification Numbers (VINs) as its only security.

Hackers have exploited insecure default configurations for decades. Ten years ago, when internet-connected (IP) security cameras became common, attackers used Google to scan for keywords contained in the camera's management interface.

Sadly, device security hasn't improved much in ten years. There are search engines that can allow people to easily locate (and possibly exploit) a wide range of internet-connected devices.

Passive threats

In contrast to active threats, passive threats emerge from manufacturers collecting and storing private user data. Because IoT devices are merely glorified network sensors, they rely on manufacturer servers to do processing and analysis.

So end users may freely share everything from credit information to intimate personal details. Your IoT devices may end up knowing more about your personal life than you do.

Devices like the Fitbit may even collect data to be used to assess insurance claims.

With manufacturers collecting so much data, we all need to understand the long-term risks and threats. Indefinite data storage by third parties is a significant concern. The extent of the issues associated with data collection is only just coming to light.

Concentrated private user data on network servers also presents an attractive target for cyber criminals. By compromising just a single manufacturer's devices, a hacker could gain access to millions of people's details in one attack.

What can you do?

Sadly, we are at the mercy of manufacturers. History shows that their interests are not always aligned with ours. Their task is to get new and exciting equipment to market as cheaply and quickly as possible.

IoT devices often lack transparency. Most devices can be used only with the manufacturer's own software. However, little information is provided about what data is collected or how it is stored and secured.

But, if you must have the latest gadgets with new and shiny features, here's some homework to do first:

- Ask yourself whether the benefits outweigh the privacy and security risks.
- Find out who makes the device. Are they well known and do they provide good support?
- Do they have an easy-to-understand privacy statement? And how do they use or protect your data?
- Where possible, look for a device with an open platform, which doesn't lock you in to only one service. Being able to upload data to a server of your choice gives you flexibility.
- If you've already bought an IoT device, search Google for "is [your device name] secure?" to find out what security researchers and users have already experienced.

All of us need to understand the nature of the data we are sharing. While IoT devices promise benefits, they introduce risks with respect to our privacy and security.

This article was originally published on The Conversation. Read the original article.

Source: The Conversation