Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 5

What's Hiding in the Internet of Things

By: Alan Zeichick

I can't trust the Internet of Things. Neither can you. There are too many players and too many suppliers of the technology that can introduce vulnerabilities in our homes, our networks – or elsewhere. It's dangerous, my friends. Quite dangerous. In fact, it can be thought of as a sort of Fifth Column, but not in the way many of us expected.

Merriam-Webster defines a Fifth Column as "a group of secret sympathizers or supporters of an enemy that engage in espionage or sabotage within defense lines or national borders." In today's politics, there's lot of talk about secret sympathizers sneaking across national borders, such as terrorists posing as students or refugees. Such "bad actors" are generally part of an organization, recruited by state actors, and embedded into enemy countries for long-term penetration of society.

There have been many real-life Fifth Column activists in recent global history. Think about Kim Philby and Anthony Blunt, part of the "Cambridge Five" who worked for spy agencies in the United Kingdom in post-World War II era; but who themselves turned out to be double agents working for the Soviet Union. Fiction too, is replete with Fifth Column spies. They're everywhere in *James Bond* movies and John le Carré novels.

Let's bring our paranoia (or at least, my paranoia) to the Internet of Things, but start by way of the late 1990s and early 2000s. I remember quite clearly the introduction of telco and network routers by Huawei, and concerns that the Chinese government may have embedded software into those routers in order to surreptitiously listen to telecom networks and network traffic, to steal intellectual property, or to do other mischief like disable networks in the event of a conflict. (This was before the term "cyberwarfare" was widely used.)

Recall that Huawei was founded by a former engineer in the Chinese People's Liberation Army, and was heavily supported by Beijing. Also there were lawsuits alleging that Huawei infringed on Cisco's intellectual property – i.e., stole its source code. Thus, there was lots of concern surrounding the company and its products.

Those concerns continued for decades. Even as late as 2014, publications like IEEE Spectrum wrote articles that continued exploring this topic, such as "U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks." Based on those concerns, many government agencies refused to purchase routers and other critical network equipment from non-U.S. companies – and many enterprises followed suit.

Of course, this is multilateral. I'm sure that foreign governments are convinced that U.S. enterprise-grade hardware and software is capable of spying on them, or might contain a shut-down switch in the event of cyberwar. If you were in charge of IT within a country currently in conflict with the United States or NATO, would you want your critical networks controlled by Cisco or Juniper, your servers running on Microsoft, your phones controlled by Apple, your firewalls powered by Palo Alto? Probably not. In fact, you might even be suspicious of any device labeled "Intel Inside."

Were I in charge of technology or information security for, say, China, Iran, North Korea, or Russia; yeah, I'd be looking for home-grown products where any malware or

unfortunate Easter eggs were planted by my own agents, not my global adversaries.

Hijacking the IoT for State-Sponsored Purposes

Discussions, at least in the United States, about having products co-opted by hostile state actors have gone on for decades. As mentioned earlier, they first came to my attention with Huawei about 20 years ago. I didn't think about it too much until the many revelations by Edward Snowden about how deeply embedded (literally and figuratively) NSA back doors were within telecommunications products and networks. Still, it was all spying, which of course every government was believed to be doing.

And thus, every networking device in our home, in our office, in our service provider network, can be and should considered as a member of a Fifth Column – a potential spy, a potential thief, a potential troublemaker that can be accessed and controlled by foreign governments who get their claws (and code) into the devices' firmware via back-doors and hidden functionality. To be clear, these devices are becoming omnipresent, they never sleep, are always listening, and are recording and reporting back to cloud data centers where the information is correlated, analyzed, and actioned.

Hey, you can't be too paranoid, as The Guardian revealed in its February 2016 story, "The government just admitted it will use smart home devices for spying." The story quotes testimony by the U.S. Director of National Intelligence, James Clapper: "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."

Around the same time, a study from the Berkman Center for Internet and Society at Harvard University went deeper into the subject with its detailed report, "Don't Panic: Making Progress on the Going Dark Debate," which focuses in large part on government actions to force tech companies and service providers to provide surreptitious access to devices, networks and data.

The study concludes, in part, that end-to-end encryption and other technologies for obscuring user data are unlikely to be adopted ubiquitously by tech companies due to their own economic self-interest. Therefore, "Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel."

There are plenty of avenues for state intelligence and counterintelligence agencies to get into the IoT, and therefore, into our homes, offices, automobiles and civic infrastructure.

The report continues with a real-world example: "The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications. A ten-year-old case involving an in automobile concierge system provides an early indication of how this might play out. The system enables the company to remotely monitor and respond to a car's occupants through a variety of sensors and a cellular connection. At the touch of a button, a driver can speak to a representative who can provide directions or diagnose problems with the car. During the course of an investigation, the FBI sought to use the microphone in a car equipped with such a system to capture conversations taking place in the car's cabin between two alleged senior members of organized crime."

In other words, there are plenty of avenues for state intelligence and counterintelligence agencies to get into the IoT, and therefore, into our homes, offices, automobiles and civic infrastructure. Remember how in movies, government agents would routinely sweep their hotel rooms for bugs? That's so old school, when today you have microphones and cameras in connected cars, phones, tablets and televisions. When the next wave of connected devices include always-on and always-listening devices from Amazon and Google. Can you hear me now?

Sloppiness Beats Malicious Behavior

Still, my concerns became mainly about state-sponsored espionage or terrorism, through back doors and dormant malware lurking inside the devices. What I didn't expect is that the Fifth Column could be hijacked by other players, raising the threat exponentially, thanks to the vast numbers of network-attached devices that enable the IoT. What's more, that Fifth Column has become a threat not only due to maliciousness in the

design of those IoT products, but also careless. Sloppy programming. And a lack of thorough testing.

Case in point: On October 21, 2016, numerous high-profile websites such as Twitter, Spotify, Amazon and WhatsApp, were hit with a serious (and successful) Distributed Denial of Service (DDoS) attack. Who was behind the attack? Nobody is sure, at least as far has been publicly disclosed – it might have been state-sponsored actors, or it might have been ordinary hackers demonstrating their tech prowess. The attack vector, however, was a nasty piece of malware called Mirai, which apparently works by continuously scanning the Internet for IoT devices with factory default administrative passwords.

Once Mirai finds those devices, attackers can then attempt to take over those devices and alter their firmware to turn them into botnet zombies able to do, well, just about anything. In this case, Mirai captured over 100,000 webcams, digital video recorders (DVRs) and other low-intelligence devices and turned them into DDoS attackers, all targeting Dyn, a DNS server based in New Hampshire.

Mirai wasn't able to take over webcams and DVRs because the manufacturer of those devices inserted a back door at the behest of a government's spy agency. Instead, the manufacturer of the device circuit boards and firmware, Hangzhou Xiongmai Technology, was simply careless in not requiring customers to change default passwords, thus enabling Mirai's botnets. Xiongmai is the OEM for cameras and DVRs sold by many other companies; I'd never even heard of them prior to this. And thanks to them, and to other careless manufacturers, the IoT can be turned against us… by anyone with access to the Mirai source code. Oh, did I mention that the Mirai source code is freely available on the Internet?

But, let's not be too hard on poor Xiongmai. Other IoT devices have been proven to be hackable – and once such hacks are discovered, they can be weaponized and packaged for use by any motivated script kiddie, whether it's a state actor, disgruntled hacker or for-profit criminal gang.

In a disturbing paper called "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," four researchers show how to create a Fifth Column using nothing more than Internet-connected light bulbs. Here's how they start:

Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will spread explosively over large areas in a kind of nuclear chain reaction, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform.

In a disturbing paper called "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," four researchers show how to create a Fifth Column using nothing more than Internet-connected light bulbs.

The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes, enabling the attacker to turn all the city lights on or off, permanently brick them, or exploit them in a massive DDOS attack.

Watch their videos…. the Cambridge Five would be envious of their mischief. For now… I'm unplugging my Internet-connected light bulbs. Perhaps you should too.