Aug, 2017
Volume 12, Issue 8

Connected Home Devices: The Internet of Things

COLUMBUS STATE UNIVERSITY

Monthly Security Tips

From the desk of Thomas F. Duffy, MS-ISAC Chair

What is the Internet of Things (IoT)?

We have become more connected than ever before. A little over ten years ago, we only accessed the Internet through a laptop or a desktop computer. Then, we added phones and tablets to our list of connected devices. Today, we have even smaller connected devices, such as fitness trackers and smart watches. According to ABI Research, there will be over 30 billion devices connected to the Internet by 2020. The list of Internet connected devices, or "things", keeps growing. Kevin Ashton, co-founder and executive director of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), first mentioned the term Internet of Things (IoT) in 1999, but the first device to be connected to the Internet was actually a Coke machine at Carnegie Mellon University in the early 1980s. Programmers could connect to the machine over the Internet, check the status of the machine, and determine whether there would be a cold drink waiting for them. Today, IoT consists of everyday devices that are connected to the Internet, such as fitness trackers, vehicles, smart televisions, doorbells, light bulbs, home security systems, thermostats, and refrigerators. Basically, if it is not a computer, smartphone or tablet, *and* it connects to the Internet, it can be called an IoT device.

What are the issues with IoT devices?

Many people know they should install anti-virus (AV) software on their computers and be careful of what websites they visit or software they download. Unfortunately, most people probably do not consider their IoT devices to be a security threat. These devices are more accessible and make our lives more integrated, but many of the companies behind these new devices are not designing them with security in mind. For example, many IoT devices have default passwords that are well known and *cannot* be changed, or cannot be changed easily. They also can be difficult or impossible to update to mitigate known vulnerabilities, or have no settings to customize security.

Our dependence on Internet-connected devices has grown faster than the means, and/or awareness, to secure them. Leaving IoT devices unsecured, as with any Internet connected device, is like leaving the back door to your house unlocked. It gives attackers access to your personal information and the potential to further compromise other devices on your network. It

also gives attackers the means to propagate their attacks onto others by using your insecure devices to attack other networks and devices.

How can you secure your IoT device?

So, what can you do to enjoy the functionality of IoT devices and remain more secure at the same time? The following tips may help you in these endeavors:

- Know what IoT devices are connected to your network. It is possible that there are devices connected to your network that you do not know about.
- Consider only purchasing devices that you *need to use*. Some Internet-capable devices may be nice to have, but provide limited benefit and reduce your security.
- Isolate IoT devices from other devices on your network by creating a separate Wi-Fi network just for them. This protects your other devices if your connected IoT devices are compromised.
- Update the device's software, if possible. If you update your device regularly, this will reduce the chances of a successful attack.
- Replace default passwords with unique and strong ones of your choosing. Passwords should have upper and lower case characters, numbers, and special characters, with at least 10 total characters.
- Configure security and privacy options, such as enabling encryption and limiting the information your devices share.
- Replace insecure IoT devices with more secure ones. Seek out reviews on these devices that address security features and patching support to determine which ones may have a reasonable baseline of security.