VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

If It Connects to the Internet, It's a Computer

Jonathan McCune, Software Engineer

Jonathan McCune is a Software Engineer on Google's Security Team. He was previously a Research Systems Scientist for CyLab at Carnegie Mellon University. He earned his Ph.D. degree in electrical and computer engineering from Carnegie Mellon University, and received the A.G. Jordan thesis award. He received his B.Sc. degree in computer engineering from the University of Virginia.

Jonathan's interests include research and production aspects of secure systems, trusted computing, virtualization, applied cryptography and spontaneous interaction between mobile devices. Jon enjoys spending time with his family, especially activities outdoors and involving bikes.

Resources to educate users on best practices for computer security now exist. Examples of such practices include using unique passwords and avoiding questionable websites. However, all of these practices assume that users are accessing these sites from an uncompromised computer. Keeping one's computers in an uncompromised state remains a significant challenge.

In my house, we have two laptops. One is my work laptop, and the other is a personal laptop shared by my wife and me. These are two "real" computers, which I diligently keep up to date. (Applying updates in a timely fashion is among the best actions one can take to keep their devices secure.) However, if I look at the *Connected Devices* web portal available on my cable modem, it also includes two smart phones, two tablets, a WiFi base station, a printer, a Chromecast and a bathroom scale. That's 10 devices. Counting the cable modem itself, that's 11. In an office setting, these can include printers and copiers, video conferencing equipment, badge readers, fire alarms, HVAC system components and power backup systems. Are those real computers? Who or what is keeping them up to date? Do I even care?

A decisive trend in the electronics industry is to attach previously stand-alone or analog devices to the Internet, giving rise to the buzzword "Internet of Things." Further examples include refrigerators, smart thermostats, home burglar alarm systems, clothes washers and automobiles. While this enables new levels of convenience and automation, each one of these devices decidedly is a computer running a surprisingly large amount of software. Many of these devices are produced by companies whose core technical competencies may not include software security or being a good steward of user data, and thus it remains highly uncertain what keeps them up to date and secure.

Unfortunately, **you should care**. Today it is not safe to assume that the vendors of these various devices are following best practices, or even any practices, to keep their devices up to date and secure. The modern internet is a hostile place, and anything attached to the internet that is widely used will attract the attention of those with nefarious intent. It is actually quite common, in the sphere of attacking computer systems, to exploit one poorly-managed device to gain more direct access to a properly-managed device that contains valuable data. So the bathroom scale gets compromised, which then neuters any firewall protections that the internet service provider was implementing on the user's behalf in the cable modem. The attackers can then probe the laptop for weaknesses unimpeded.

Today, users are left as the party responsible for the security of the devices purchased. They are not qualified for this, nor is there any fundamental reason why they should need to be. Product vendors need to support and maintain their systems and products. Truly savvy companies streamline update processes to the point that they go unnoticed (e.g., taking effect silently each time the device restarts or its battery runs out). Truly incompetent companies do not provide any updates at all, leaving users with nobody watching their backs. Unfortunately, it's not easy to tell the difference without significant expertise. Further exacerbating the situation is today's competitive electronics marketplace, where many companies are too preoccupied pitching the newest device to stand behind the one they sold just one or two years ago.

This is where I would like to offer a few words of advice but, unfortunately, it is all but impossible for the average person to adequately ensure the security of their devices. For better or worse, many of the underlying technical problems more closely resemble procuring a source of clean drinking water than they do developing a cure for cancer. "There are no silver bullets, only lead." Technical complexity makes a one-size-fits-all solution infeasible. Economic realities force companies to cut corners. The lack of legal protection for users makes remediation tedious at best and Sisyphean at worst.

I encourage the motivated (i.e., sufficiently frustrated) reader to aim high with their response. Do not simply endeavor to secure one's own devices, or make product choices based on vendors' reputations for support and maintenance. Ask questions of vendors. Return poor quality products. Blog about your bad experiences. Learn about the open-source alternatives and ask vendors why they bother with a proprietary solution. Make clear that you care. Then you are not just one consumer, but someone possibly in a position to influence the behavior of a vendor. V