***Securing the Internet of Things***

By Nathan Betz, Chris Moore, and Roman

ITC 134: Introduction to Development Software

Introduction

*The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data (Ranger par. 1).*

Pretty much there are robots in everything and they are all connected to each other in the hive-mind of the internet. Of course, some of these things are obvious: phones, tablets, desktop computers*—*these household and handheld objects are now ubiquitous, everyday tools in work, education, and home life. The ‘Internet of Things’ or IoT, denotes the increasing popularity of taking other common tools and making them web-accessible and web-controllable.

Additionally, popular consumer products like Google’s Home and Amazon’s Echo allow users to control household operations like music and lighting, to plan their schedule or just figure out what the weather is going to be.

*The IoT was initially most interesting to business and manufacturing, where its application is sometimes known as machine-to-machine (M2M), but the emphasis is now on filling our homes and offices with smart devices, transforming it into something that's relevant to almost everyone (Ranger par. 9).*

Per Steve Ranger’s above article and quote, consumers can expect more devices to become web-integrated in future, whether it be cars and airplanes, household instruments, or work tools. This will allow companies to update and create useful APIs for said devices, and to monitor the IoT in order to track usage and make improvements. It is not unreasonable to expect this trend to grow into most industries and facets of our culture.

Cyber Security Risks

*The Gartner* [*report*](http://www.gartner.com/newsroom/id/3598917) *predicts over 20 billion connected things by 2020, all of which represent a portal to the network which can be hacked or compromised (Eastwood par. 6).*

When you have more devices connected to the network, there are more entry points for hackers or those who would use said devices to illegally access networks and steal information. The rapid growth of networked computer systems means that no one has done the groundwork of making sure that all the hardware connected those systems are impervious to attacks. While many of the new devices will have security measures built in, many old hardware systems (newly connected to the internet) will be very vulnerable.

When thinking about cyber security, it’s easy for your mind to default to the cliched, rogue hacker, hunkered down in some basement in Russia. However, the much more likely threat comes from corporations looking to mine your data and invade your privacy in search of a competitive advantage over other corporations, among other motivations. The problem is that much of this data collection is not technically illegal. Consumers who can’t be bothered to read the terms and conditions of every product or service they use (a nearly impossible task), can unwittingly have their every move tracked by the purveyor, or worse, have their information mined by an number of third parties. With the IoT expanding into every facet of our lives, there is little information about our lives that can’t be tracked, stored, and sold to the highest bidder (Eastwood, Feb. 2017).

Currently, the biggest threat to individuals that is posed by the IoT is a purely data driven one. By expanding your personal network, you risk exposing your personal information. However, as the IoT proliferates into physical structures, it’s time for us to think about physical safety. Specifically, home security systems and cars have begun to be connected to the internet and even remotely controlled via the web. This connectivity, while convenient, exposes those structures to hackers. While the thought of having your credit card number stolen is scary, it pales in the face of home invasion or losing control of a vehicle while you’re inside. Extreme measures need to be taken to secure the physical safety of consumers using these connected structures, and the corporations putting out these devices can’t necessarily be trusted to put in the additional time and expense to make sure that happens. Unfortunately, regulations and laws tend to be reactive, rather than proactive. Ultimately, it’s up to consumers to be extra careful when connecting their home or vehicle to the internet.

Conclusion

The Internet of Things has come a long way toward making our lives more convenient, but that convenience comes at the price of security, especially while the IoT is still burgeoning. Each connected device represents another pathway for hackers or corporations to access your personal information. As the IoT expands into our homes and modes of transportation, we also expose our physical safety to network vulnerabilities. When it comes to our data integrity and physical safety, it’s not enough to trust manufacturers or lawmakers to keep us safe. We need to take their own precautions as connectivity permeates our everyday lives.

***Works Cited***

Eastwood, Gary. “5 of the biggest cybersecurity risks surrounding IoT development” *Networkworld*. IDG Communications. 27 June 2017. <[https://www.networkworld.](https://www.networkworld.com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html)

[com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html](https://www.networkworld.com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html)>.

Eastwood, Gary, and IDG Contributor Network. “4 Critical Security Challenges Facing

IoT.” *Network World*, Network World, 7 Feb. 2017, [www.networkworld.com/article/ 3166106/internet-of-things/4-critical-security-challenges-facing-iot.html](http://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html).

Ranger, Steve. “What is the IoT? Everything you need to know about the Internet of Things right now” *ZDNet*. CBS Interactive. 21 Aug. 2018. <[https://www.zdnet.com](https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/)

[/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/](https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/)>.