Securing the Internet of Things

David Light
Tufts University
December 13, 2017

Abstract

The Internet of Things plays an ever-growing part in the modern world, and the associated security concerns extend into both the home and business. The Internet of Things promises automation, convenience, and improved efficiency throughout society. However, Internet of Things devices also provide a large range of attractive targets for attackers. Home cameras and smart TVs provide eyes and ears inside of homes, and ransomware on devices from door-locks to thermostats offers attackers control of day-to-day safety. This paper explores the nature of these attacks, as well as what steps should be taken to combat them. These solutions are largely based on improving education efforts for consumers about device security and increasing pressure, through government regulation, on businesses to improve their security practices.

Introduction

The Internet of Things refers to the network of ordinary objects, other than computers and smartphones, which are connected to the Internet. An early example of an Internet of Things device is the Carnegie Mellon Coke Machine. In 1982, several CMU students connected the School of Computer Science's Coke machine to the Internet so it could be remotely determined whether or not there were any cold sodas available [1]. Nowadays, Internet of Things devices exist for nearly every purpose, from smart lights to medical

implants, from industrial controllers to refrigerators [2]. Ten years ago, the smartphone changed the world; now, smart homes are doing the same. Current estimates predict that the American household will have an average of 50 connected devices by 2020 [3]. With this multitude of devices, however, come an unprecedented number of potential targets for cyber attacks. Internet of Things devices often make particularly attractive targets for attackers, as the current (minimal) level of regulation creates little incentive for companies to spend resources improving a device's security. The Internet of Things presents a new kind of threat to society. Prior to these devices, attackers looking to cripple a city might be forced to attempt bombing a well-guarded and centralized power station. Now, those attackers may gain access to one of thousands of smart meters (used to manage power routing in real-time) and use it to control a city's entire electrical network [2].

To the Community

As Internet of Things devices become more popular and accessible, the world appears increasingly futuristic; normal people can manage their homes with a couple of taps on their phones. As is common with new technologies, many people have quickly integrated Internet of Things devices into their lives without fully considering the associated risks. The electrical grid example in the preceding section is meant to highlight the potential for catastrophe that comes with the reckless expansion of the Internet of Things. That is not to say, however, that the Internet of Things is a bad thing. I chose this topic to acknowledge some of the privacy and security concerns surrounding the Internet of Things, and to lay out some steps that individuals, companies, and government bodies can take to ensure that this technology is adopted responsibly. With proper caution and standards for security, the Internet of Things can become a healthy system in a more efficient modern world.

Threats

Within the home, the Internet of Things presents threats to both the privacy and security of individuals. One important privacy concern is the eavesdropping capabilities of certain Internet of Things devices. For instance, despite being banned in Germany, children's smart watches with such potentials remain a threat to privacy in the United States and elsewhere. These watches record and transmit audio that can be listened to through an app. As a result, these and similar listening devices are plagued by privacy and security issues ranging from parents eavesdropping on teachers, to third parties controlling usage data, to hackers gaining control of the watches and wiretapping [4]. In many places, including the United States, no regulation for these sorts of devices exists, so people are often inadvertently installing potential eyes and ears for attackers in their homes when they buy personal security cameras, baby monitors, smart TVs, and eavesdropping wearable devices. While these devices present a valid privacy concern for everyone, they should be particularly worrisome for high-networth individuals. Such homeowners may be extorted and surveilled by attackers because of their tendency to have highly connected homes [5].

For the majority of individuals, devices with serious security concerns include smart garage door openers, locks, calendars, and thermostats. The latter poses a particularly alarming threat. In a demonstration at Def Con, Pen Test Partners' Andrew Tierney presented a proof of concept thermostat ransomware [6]. He showed that if an attacker gained access to a smart thermostat, a family could be held ransom in its own home, kept at boiling hot or freezing cold temperatures until it agreed to pay the attacker and regain control of the device.

It is important to note that the risks associated with Internet of Things devices are, unlike in the examples presented above, frequently not about controlling the device itself. Internet of Things devices can ruin security without ever giving attackers eyes, ears, or physical entry into a home [7]. A criminal does not need to steal a $500 TV, for example, if he or she can instead obtain network and online credentials to directly access bank accounts.

For enterprises, the integration of Internet of Things devices, intended to increase efficiency and reduce costs, can turn an otherwise secure organization into an attractive target for would-be attackers. In a survey carried out by the strategy consulting group Altman Vilandrie & Company, nearly half of 400 surveyed IT companies across 19 industries experienced an IoT-related security breach. Of these companies, the smaller ones reported an average expense of 13% of total revenue from the breaches [8]. This loss of revenue could translate into mistrust in the Internet of Things, causing these relatively early adopters to abandon the technology. Furthermore, the risk for businesses is often much higher than that for individuals, as businesses generally have more sensitive information to protect. In fact, a company often does not even know which Internet of Things devices are in its environment. As Bob Baxley of the security firm Bastille says, "[f]or example, a facilities group installs an industrial control system that, unbeknownst to the IT security department, has an open Zigbee network enabled and accepting connection [7]." It only takes one vulnerability to risk major damages for a business.

Action Items

As a society, individuals are selectively concerned about privacy and security. For instance, the same people covering their laptop web cameras for fear of being recorded are readily installing devices like smart watches, smart TVs, and other appliances that connect to the web in an insecure way. To combat this, there needs to be a greater effort made by both individuals and institutions to educate on the dangers of these new devices. Many people are unaware of the threats that they willingly bring into their homes.

However, even those who do know that Internet of Things products have suboptimal security measures occasionally buy the devices anyway. In some cases, it is because people do not feel as if they have another option, seeing as many manufacturers currently do not take great measures to ensure the security of their devices. A company will always choose

to ship a product if a deadline is approaching, making it a decision between shipping and securing [7]. To combat this, companies that *do* take heightened security efforts should lead a movement to educate the public. By communicating the security advantages of their products, such businesses put market pressure on competing firms to step up their products' security. For instance, given a choice between two similar baby monitors, which parents would choose one that risks broadcasting a video of their child for strangers to see? This solution addresses the argument of security through obscurity. People could argue that, as individuals, it is extremely unlikely to be attacked through an Internet of Things device. No matter how small the probability, however, few people are likely to choose the baby monitor that allows strangers to see and talk to their children at night. Once individuals have been educated about the severity of such risks, it is their responsibility to (1) avoid insecure Internet of Things devices, (2) keep owned devices up to date with the latest patches, and (3) change device passwords regularly.

From an industry perspective, hardware and software developers need to take several steps to ensure that Internet of Things devices are as secure as possible. For instance, devices should be designed to do the intended bare minimum: limit any and all superfluous capabilities [2]. Additionally, creators need to ensure that simple security measures are in place, as there is no excuse for the countless Internet of Things devices with default credentials. Requiring users to set their own when first bringing a device online can prevent many low-effort attacks. In short, the same and best security practices that are well-known for personal computer and mobile devices generally apply to the Internet of Things, so companies that take steps to implement these practices can greatly improve the security of such devices as a whole. This is easier said than done, however, as companies who prioritize functionality over security and privacy will make the most money in the absence of regulation that forces compliance.

While there are many organizations that have taken steps to establish security standards and frameworks for the Internet of Things, these efforts are decentralized and ultimately

insufficient. For example, while the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) are working on developing such standards, there is no universal, certifiable rule for security in the industry [2]. Therefore, individuals and businesses installing Internet of Things devices must currently put in a lot of independent research to determine a device's security. The next logical step, it would seem, is for governments worldwide to develop their own regulations. While market competition could incentivize some necessary security changes, many security holes go beyond the influence that consumers have on businesses. For instance, a home DVR could have been part of the Mirai botnet, but many people may not take action so long as the device works. Thus, for these kinds of collective action problems, government regulation is required. Administration for technology of this nature is not unprecedented. Historically, in the United States, new technologies such as automobiles, airplanes, radios, and televisions have spurred the formation of new regulatory policies and agencies [9].

Overall, a mix of low awareness, apathy, and a lack of supervision has created an environment in which Internet of Things security is simply not a priority for either consumers or producers. By educating buyers, introducing market incentives and competition, and regulating Internet of Things security through government bodies, protection for the Internet of Things can be driven to the same baseline standards that exist for personal computers and mobile devices.

Conclusion

This paper explored some of the security and privacy risks associated with Internet of Things devices for both individuals and businesses. In its current state, the Internet of Things is a toxic force that presents, through negligence, a plethora of security risks that increase vulnerabilities on all levels of society. As discussed, however, it is not an inherently harmful innovation and can be a positive stepping stone into a futuristic world with the relatively simple steps that have been suggested. By promoting awareness about

potential security concerns, increasing incentives for companies to improve device security, and implementing standards and certification for Internet of Things protection through governmental regulation, the Internet of Things can be secured. Though the addition of Internet-connected devices automatically translates into higher security risks, the Internet of Things appears to be here to stay. Therefore, these changes can, at least, bring the Internet of Things up to the existing, accepted security standards of computers and phones.

References

[1] CMU Computer Science Department. "CMU SCS Coke Machine." *CMU SCS Coke Machine Home Page*. N.p., 14 Feb. 2005. Web. 13 Dec. 2017.

[2] Mortleman, Jim. "Secure IoT before It Kills Us." *ComputerWeekly.com*. Computer Weekly, Jan. 2017. Web. 13 Dec. 2017.

[3] Shaw, Mary. "Consumers Want “Internet of Things” to Become the “Internet of Intelligence”."*BusinessWire*. N.p., 15 Nov. 2017. Web. 13 Dec. 2017.

[4] Diaz, Jesus. "When Is The U.S. Going To Ban The Internet Of Things For Children?" *Co.Design*. Co.Design, 21 Nov. 2017. Web. 13 Dec. 2017.

[5] Boyer, Sam. "Hacking the Internet of Things." *Insurance Business*. Insurance Business America, 7 Dec. 2017. Web. 13 Dec. 2017.

[6] Raywood, Dan. "Thermostat Hacked to Run Ransomware." *Infosecurity Magazine*. Infosecurity Group, 07 Aug. 2016. Web. 13 Dec. 2017.

[7] Zorz, Mirko. "Internet of Fail: How Modern Devices Expose Our Lives." *Help Net Security*. Help Net Security, 27 May 2016. Web. 13 Dec. 2017.

[8] Sun, Leo. "10 Jaw-Dropping Facts About the Internet of Things." *The Motley Fool*. The Motley Fool, 25 Nov. 2017. Web. 13 Dec. 2017.

[9] Kerner, Sean Michael. "IBM's Schneier: It's Time to Regulate IoT to Improve Cyber-Security."*EWEEK*. QuinStreet Enterprise, 11 Dec. 2017. Web. 13 Dec. 2017.