The Rising Threat of the Internet of Things

By: Javen Zamojcin

In today's society, what are we willing to sacrifice in exchange for convenience through technology? As technology evolves, becomes smarter, and invades more aspects of our lives, we gain not only convenience but also risks. This new wave of technology is referred to as the Internet of Things (IoT). The Internet of Things, by definition, is a paradigm envisioning the interconnection and cooperation of smart devices over the internet infrastructure (Ziegeldorf, 2013). The Internet of Things includes a large spectrum of devices, ranging from self-driving cars, price-monitoring thermostats, to mile-counting Garmin watches. This rapid expansion of technology has proven to be very beneficial not only to consumers, but also to industry. However, in exchange for these advancements in technology, we have sacrificed security and our right to privacy. Due to the lack of regulating government standards, companies and communities have taken the implementation of security into their own hands. However, the security protocol currently implemented relies on whatever a manufacturer deems as "secure enough,” which is often unsatisfactory. Because of this loose security, many issues have developed and will continue to do so, threatening the communities associating with the Internet of Things. There is, nevertheless, a solution. Increasing government regulation of the implementation of security in the Internet of Things will reduce the growing number of threats associated with these devices.

The Questionable Security of the Internet of Things

What is the importance of introducing stronger regulations on the Internet of Things? According to the Research firm Gartner Inc., by the end of 2017, there will be an estimated worldwide total of 8.4 billion interconnected devices. Of these 8.4 billion devices, up to 70% are vulnerable to attack (McCollum, 2017). Despite it being in the best interest of companies to exercise due diligence against such vulnerabilities, there is actually little government regulation enforcing companies to do so. Until stronger regulations are introduced, consumers will continue to rely on the social expectations and reputations of companies to safeguard their security. For instance, compare the standards of a renowned company such as Google to those of smaller technology companies. Google might find it in their best interest to not let a major vulnerability be passed through its line of products. However, a smaller company may not have as much to lose in terms of reputation in order to maximize security testing. It's because of these informal expectations that technology companies don't prioritize security concerns, resulting in the majority of security issues associated with IoT devices (Pandey, 2017).

Poor practices of security implementation make IoT devices easy targets. Use of default passwords and ports, the standard of rarely or never updating device firmware, and a general dismissal of security concerns all helped contribute to one of the biggest examples of insecurity in the history of IoTs: The Mirai botnet This botnet was a massive army consisting of an estimated 500,000 infected IoT devices, all aimed to cause havoc (Kan, 2016). Using the current slack security standards to its creator's advantage, taking control of this many devices was relatively easy. In late 2016, the Mirai botnet launched its largest attack, a mass DDoS (Distributed Denial of Service) attack towards the heavily relied upon web management company Dyn. Essentially rendering the company's networks useless, though only temporarily so, this botnet caused massive problems throughout the service of the internet, which included the accessibility of popular websites such as Twitter, PayPal, and Reddit. The estimated cost of this single attack was roughly $110 million of potential revenue (Umbach, 2016). The Mirai botnet is just one of the many examples of attacks brought on by the current security standards. Such a destructive weapon could have potentially been avoided with stronger security implementation in IoT devices. More than likely, many of the owners of these infected IoT were oblivious to these malicious events, rendering them more susceptible to future attacks and making them unaware of the security lapses connected to the Internet of Things.

Privacy Problems and Security Breaches in the IoT

Part of what makes IoT devices useful is their ubiquitous data collection, allowing for applications not possible before. However, these features are examples of the growing privacy problem when security isn't implemented strong enough (Ziegeldorf, 2013). Consumers are progressively relinquishing more and more personal information without realizing the current situation of security implementation, increasing their risk for violation of privacy in events such as data breaches or uninvited device access.

Privacy violation in terms of the Internet of Things takes several forms. One form might be personal information being leaked or stored without the knowledge of the device owner. The other form, and probably the bigger cause for concern is someone's physical privacy being violated, such as the incident that occurred with the popular children's toy Cloud Pets, in February 2017 (McCollum, 2017). This stuffed animal IoT device includes a webcam allowing for owners to communicate to one another. But unknown to the products’ owners, their voice recordings, physical location, and names were being stored on openly exposed company servers. Once a hacker group discovered this simple vulnerability, they took full advantage of the device insecurities, gaining access to more than 800,000 customer's personal information and voice recordings (McCollum, 2017). This privacy violation incident is an example of how consumers cannot rely on the competency of a company's security implementation for their own privacy rights.

Although hacking toys may seem irrelevant to some, how security is implemented in IoT devices may actually be the difference between life-and-death. Medical devices used by hospitals and autonomous vehicles exemplify this concern. Originally intended for stand-alone use (not connected to a network), heavily relied upon medical devices are being used with little to no security implementation (Newman, 2017). Thus, hospitals and device manufacturers are creating threats throughout the entire healthcare environment. Never before has the medical community had to be concerned about the security of embedded devices such as heart pacemakers and insulin pumps (Newman, 2017). Hackers are increasingly taking advantage of the insecurities of these devices, potentially gaining access to larger networks, using ransomware to extort money, or even manipulating them to cause death in the patients. In the case of autonomous vehicles, poor security design alone can lead to disastrous consequences. Whereas self-driving vehicles aren't relevant now, by 2020, there will be an estimated 10 million self-driving cars on the road (Kornwitz, 2017). Autonomous vehicles are a particularly tricky IoT device, reliant upon an array of complicated computer interfaces and network connection. This makes them even more susceptible to technical exploits technological tampering, creating the risk for cyber threats. Given the nature of medical devices, autonomous vehicles, and other potentially dangerous IoT devices, it makes sense that a strong security protocol be required to guarantee the safety of consumers. But without solid government regulation to improve security, companies have little incentive to resolve these issues.

Current and Proposed Measures to Address Security in the IoT

With the number of insecurities found in IoT devices, what solutions are currently being utilized to address these issues? The issues found in the current implementation of security in IoT devices are nothing new to the technology and security community. Since the Internet of Things has existed, there has been at least a minimal level of informally defined security standards. These unofficial standards are usually addressed through technology and security collaborations, company security policies, and some initiative taken from leading companies.

However, even with the variety of current solutions, there is still a need for a stronger, centralized solution to take on the growing threat of the Internet of Things. The biggest issue with these current solutions is that they rely too much on market trends. That is, until money becomes an issue, companies have little incentive to address the insecurities found in their devices. Even with the disastrous potential of the Mirai botnet, neither the buyers or manufacturers of the devices involved had enough motivation to resolve the insecurities used. And with good reason, too: this attack didn’t directly affect their reputations, their money, or their bottom lines. This example shows that relying on market solutions isn't a viable option anymore. There is a need now, more than ever, for a third party such as the government to step in to raise the security standard.

Along with a centralized law being passed, a cultural change must occur within the field of security and technology. Whereas an increase in regulation in the implementation of security is the strongest solution, if companies don’t prioritize security, these issues will continue to rise. The first is that there needs to be a rise of cooperation between large IT companies and startups. With more cooperation, the availability of knowledge on security implementation will be increased. More cooperation also means those startups who may not have the resources to properly implement security could be assisted doing so, resulting in higher quality products. Second, there is a need for the quantity of data collected by IoT devices to be heavily reduced. The current amount of data collected is overwhelming and unnecessary, which is also feeding the emerging Big Data problem.

As well, the privacy of consumers has stripped away, resulting in disastrous events, such as data breaches. The third is addressing the general ignorance in the field of IoT security. Although some initiatives have been taken, with companies such as Microsoft, Breed Reply, and Indiegogo all providing educational facilities, it is important that more attention is brought to this subject. IoT educational facilities provide the means for spreading knowledge on standard security implementation and raising awareness on potential cyber-threats. As well, educational facilities give companies specializing in custom software development the opportunity to educate the community about their product's proper usage. Finally, there is a need for large IT companies to commit themselves more to developing security solutions. By 2020, 50% of IoT solutions will be developed by startup companies, often lacking expertise and function (Klubnikin, 2015).

For the government to increase standard security implementation through regulation, there must be legislation passed. To raise the standard in security, several things need to be addressed by this bill. One, there is a need for a basic framework of minimal security requirements in IoT devices. Even with very basic security standards implemented, such as requiring proper authentication and encryption methods, the potential for devices being affected by malware can be significantly reduced (Schneier, 2016). Two, companies must be held responsible for issues that arise from their device insecurities. For instance, if the company Dyn was again affected by the Mirai botnet, legal action could hold manufacturers responsible for the simple insecurities found in their devices. Lawsuits like these would raise incentives for companies to properly implement security in their IoT devices. Three, companies should be required to conform to an interoperability framework and employ security audit practices. With better device interoperability, it would be easier to utilize standardized security measure. Having to employ security audits, which are not commonly done by startups, will help ensure devices meet minimum security standards.

What are the minimal security requirements in order for an IoT device to be "secure"? There will never be an absolute solution for any security needs; the most secure infrastructures have risks still. However, implementing even basic standards can dramatically reduce the current threats being found in IoT devices. Simple features that would boost security commonly agreed upon by security experts include implementing secure device booting, resource access control, network authentication, and local network firewalls (Klubnikin, 2015). Secure device booting occurs when an IoT device is launched for the first time and its software undergoes digital verification to make sure no other program will run on that device in the future. This feature would prevent malware from running on basic IoT devices, such as the one involved in the Mirai botnet incident. Resource access controls are a mandatory control feature embedded into a device operating system, restricting the functions of both hardware and IoT applications so that only actions essential for their performance are allowed. These features are similar to secure device booting. Also essential is requiring secure network authentication is essential, which prevents malware infected IoT devices from connecting to networks and allowing malware to propagate. Lastly, implement local network firewalls, in which each individual IoT gadget is equipped with local filters to analyze the data it is going to process before redirecting the data packets to the parent network (Klubnikin, 2015). Implementing these four basic security features in IoT devices is the minimum-security standard needed to battle current threats. What might be some issues found in increasing government regulation opposed to market solutions? One issue is that even though the United States would have more secure devices, this won't stop companies from producing in other countries or simply importing because the cost would be lower than implementing proper security (Schneier, 2016). As mentioned, the cost of IoT devices will increase. Currently, many of the current IoT devices available are equipped with slow processors, less memory, and short battery lives (Klubnikin, 2015).

In the process of requiring more security implementation, there will definitely be a demand for more powerful hardware, which will definitely raise its price and the cost of these devices. Yet, for technology companies, the main resistance to increasing government derives from concerns about limiting product innovation. Part of what drives market solutions is the concept of innovation, making devices cheaper and allowing for clever product solutions. With increasing regulation in the implementation of security in device design, companies might be less willing to take creative risks and become more limited in their product development.

Conclusion

The Internet of Things has progressively been introduced into our daily lives over the recent years. As these devices become more relevant, and more threats from slack security arise, there develops an urgent need for stricter protocols and stronger security. Without proper security implementation, consumers sacrifice not only their rights to privacy but also their right to safety. For the bar of security implementation to be raised, there must be more centralized regulation as well as a cultural change in the technology community. Rather than allow market solutions to control the security standards, increasing regulation from the government will be more effective at addressing and reducing the rising threats from the Internet of Things.

References

Garmin Express. Screenshot of Garmin Express Homepage. Taken Jan. 31, 2018.

Jelnick, Tom. CloudPet database hacked, what you need to know, YouTube. Retrieved Jan 31, 2018, from https://www.youtube.com/watch?v=Vom5P-AYsSw

Kan, M. (2016, October 26). DDoS attack on Dyn came from 100,000 infected devices. Retrieved December 12, 2017, from http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html

Klubnikin, A. (2015, December 24). The Internet of Things: Security Challenges, Solutions and Trends. Retrieved December 12, 2017, from http://r-stylelab.com/company/blog/iot/the-internet-of-things-security-challenges-solutions-and-trends

Kornwitz, J. (2017, February 16). The cybersecurity risk of self-driving cars. Retrieved December 12, 2017, from https://phys.org/news/2017-02-cybersecurity-self-driving-cars.html

McCollum, T. (2017, March 23). The Dark Side of the Internet of Things. Retrieved December 13, 2017, from https://iaonline.theiia.org/2017/Pages/The-Dark-Side-of-IoT.aspx

Newman, L. H. (2017, June 03). Medical Devices Are the Next Security Nightmare. Retrieved December 13, 2017, from http://www.wired.com/2017/03/medical-devices-next-security-nightmare

Pandey, A. (2017, June 27). The Insecurity of the Internet of Things (IoT). Retrieved December 13, 2017, from go.galegroup.com/ps/i.do?p=ITOF&sw=w&u=lom_mtu&v=2.1&it=r&id=GALE%7CA497103316&asid=bc6f7a6b28249a99479f4a3432bde2b

Schneier, B. (2016, November 10). Regulation of The Internet of Things. Retrieved December 13, 2017, from http://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

Thomson, L. (2016, March & april). Insecurity of the Internet of Things. Retrieved December 13, 2017, from go.galegroup.com/ps/i.do?p=AONE&sw=w&u=lom_mtu&v=2.1&it=r&id=GALE%7CA467336866&asid=50a2a27c9e92a3758592dff48000fe97

Umbach, Rich. “Mirai Botnet Attack Costs Companies Hundreds of Millions.” Effortless, 15 Nov. 2016, effortlessoffice.com/mirai-botnet-attack-costs-companies-hundreds-of-millions

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2013, June 10). Privacy in the Internet of Things: threats and challenges. Retrieved December 13, 2017, from http://onlinelibrary.wiley.com/doi/10.1002/sec.795/full