Package Delivery and Security in IoT Devices

An STS Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Arthur Given
Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signed: A.J. Given Date 13 May 2022
Arthur Given

Approved _____ Date 13 May 2022
Richard D. Jacques, Ph.D., Department of Engineering & Society

Introduction:

With the start of the Covid-19 pandemic, Americans began ordering more goods online. Just between the beginning of March 2020 and the middle of April 2020, ecommerce increased 30% in the U.S.(Rattner, 2020) Coupled with this increase in ecommerce, the U.S. has also seen a large increase in "porch piracy" or packages stolen from people's porches or front yards after delivery, but before they can be brought inside.(Asymkos, n.d.) Some companies have created smart Internet of Things (IoT) devices that aim to combat porch piracy such as the ring doorbell and other smart cameras. In fact, the number of IoT devices connected to the internet is expected to be several billion in the next few years (Jan Saleem & Ahsan Chishti, 2021). However, many IoT devices contain serious cybersecurity vulnerabilities that allow malicious actors to gain unauthorized access to the IoT devices themselves as well as other devices on the user's home network. This applies not just to IoT devices aimed at preventing porch piracy, it applies to many of the rapidly expanding number of IoT devices in use throughout the world.

The technical project report details the design, implementation, and fabrication of a multi-tiered user access system. While the system has many use cases, we applied the design to a package delivery box. However, the electronic components can all be removed from the package box and rehoused to use the system in a doorjamb to control access to a room or building. The goal of this package box application is to create a safe delivery area that allows user to receive deliveries that cannot be stolen easily. To accomplish this, the system allows the owner to remotely generate single use and time limited passcodes from their phone while also being able to manage these passcodes and review footage of passcode use. Other products have attempted to solve the porch piracy problem through different means. The "Ring Doorbell" is a smart home

doorbell with a camera that allows the owner to access live real-time and recorded video of their front porch. While the idea of being filmed while stealing may deter some porch thieves , it does not prevent the physical act of stealing a package. The system we developed keeps the package secured in a box, which in theory can be constructed to provide a greater barrier to the physical act of theft such as having to physically break open the box.

This STS research paper explores issues surrounding cybersecurity in IoT devices. The paper examines why IoT devices are more vulnerable to cyber-attacks than traditional computers and the social factors that exacerbate these vulnerabilities. These social factors include the lack of consumer education and awareness of security-based issues, especially in the case of IoT devices. In addition, the relatively small number of laws that regulate cybersecurity standards in the United States do not provide sufficient protection to consumers who have little knowledge that would help them determine what makes an IoT product insecure and how to mitigate those risks. My research found that the United States needs extensive consumer protection regulations for IoT devices that will ensure people will be able to use IoT devices securely without having an advanced knowledge of security or information technology.

Literature Review:

This paper discusses common cybersecurity practices or lack thereof in the development and manufacturing of IoT devices through the lens of the Social Construction of Technology. This STS framework asserts that technology is shaped by society. . In the case of IoT devices, due to their rising popularity, much of the United States is included in that user pool. As discussed previously, the number of IoT devices and the number of users continues to increase. However, these users do not necessarily have the technical understanding to be critical of their

devices, and in many cases do not use them correctly. These users are currently shaping the future of IoT technology, but manufacturers are not accounting for their behaviors in a manner that ensures their security.. This research examined a number of social factors that affect this including public knowledge and government regulation.

Methodologies:

To gather evidence for this paper I used the standard University of Virginia Virgo database as well as the specialized Web of Science database to find journal articles related to the subject. Because this field is so quickly evolving, news articles from reputable news sources that interview industry professionals on this subject were also included. These sources describe the current state of the industry through the eyes of consumers and developers of IoT devices. Multiple laws governing IoT devices were also researched at the state and federal level to understand exactly how the IoT industry is being regulated in the United States today. While there are many laws pertaining to cybersecurity in the United States, few of them are unrelated to the field of IoT.

Social Construction of Technology and Security:

The STS theory of social construction of technology uses the idea that technology is shaped and given significance by the people who use it. Understanding how IoT devices and networks are constructed requires a specialized collection of knowledge that most users do not and cannot be expected to possess. Issues with social construction of technology begin to occur when the users lack the knowledge to understand what security threats their IoT device exposes them to..

IoT devices that are used in the home such as baby monitors, cameras, smart refrigerators, , etc., The primary purpose of each device is convenience. It has been discovered that when home users purchase IoT devices, the potential for security threats and breaches is not a primary concern. Most consumers are much more concerned with how the device will add convenience to their life rather than how it could expose them to cyber-threats. In addition, normal everyday users do not have the knowledge to figure out or understand which of their IoT devices may be vulnerable and which may have already been compromised.

Because security is not a priority of the end users, the creators of IoT devices do not ensure that these devices are as secure as they could be. Often, IoT devices are shipped with the default credentials still in use (Griffiths, 2019). These default credentials can allow malicious users to gain remote access to the IoT device since most users do not have the motivation or knowledge to change the credentials. While this could easily be fixed by randomizing the logins during production, there is very little incentive for device producers to put time and effort into these security measures as they have little effect on how a product is used or how well the product sells (Griffiths, 2019).

In 2020 a class action suit was filed against Ring, the manufacturer of IoT devices that allow for two-way communication between the device and the user and includes a camera, which allows the user to view footage from their smartphone. The lawsuit alleged that Ring's lax security measures allowed malicious actors to gain access to their devices. This access included viewing live camera feeds, listening to the users' conversations, and playing sound from the two-way audio feature (Paul, 2020). These users were only aware that their devices had been compromised because the hackers used their microphones to play audio. It is reasonable to assume that many more devices were compromised, and many other users were spied on in their

homes but were never aware of the intrusion. Ring responded by asserting that the users who were hacked were likely using insecure passwords and encouraged users to enable two factor authentication, which uses a second form of authentication in conjunction with a username and password, for their Ring devices (Wolfe & Ries, 2019). Because the users of the device have a focus on convenience and usability, many users did not change the default password and did not enable two factor authentication. As a result, the product was much less secure than the designers intended. Many of these issues could be fixed by requiring certain precautions be taken by users rather than just recommending them. The end user could be required to choose passwords with a specific level of strength and requiring two factor authentication for logins from devices at all times. These requirements would make it significantly harder for a hacker to guess insecure and/or default passwords.

The use of default credentials has worse implications, though. In 2016 a botnet called Mirai was uncovered that controlled roughly 600,000 IoT devices (Kambourakis, 2017). A botnet is a collection of devices to which the controller has no right. A malicious actor gains control of that device and use its computing time for whatever purpose they desire. Having access to one device is bad enough and allow the hacker to control all functions of that device and access any data on the device. But control of a botnet the size of Mirai allows the hacker to execute distributed denial of Service (DDoS) attacks on various parts of the internet, effectively shutting down whichever service is being targeted. Many IoT devices are part of a botnet, and the owner does not know because the device remains functioning normally but is being controlled from a remote Command and Control server. One of the most common ways that Mirai infected devices was by using default usernames and passwords to log directly in, but it also exploited other issues with lightweight IoT firmware.

The Mirai botnet was only the beginning, though. Other botnets based on Mirai such as Hajime have also been discovered (Kambourakis, 2017). These botnets come directly out of the social construction of technology. Although the IoT devices were not manufactured to be part of a botnet, their weak security allowed hackers to shape them into a hacking tool for botnets and DDoS attacks.

Another common issue with IoT security is the use of outdated software that has been shown to be insecure. While failing to update any software can result in security risks, the software of IoT devices is especially vulnerable when left running an old version because of how commonly they are targeted by hackers (Hernández-Ramos et al., 2020). Known vulnerabilities in specific versions of software are widely catalogued across the internet. One such online database is "exploit-db.com," a free website easily accessed by anyone on the internet. This database allows a potential hacker to search for a specific version of software and find the known vulnerabilities. Should a malicious actor learn what version of software is running on the IoT device, which can, in many cases, be easily determined by using a simple network scan to access the database which tells the hacker exactly which features they can exploit in the device and how to do it. When this tool is coupled with other tools that write malware and payloads for hackers, a malicious actor with limited knowledge of cybersecurity can gain access to IoT devices. One such tool is the Metasploit framework, that allows a would-be attacker to specify a target and choose from a list of known vulnerabilities to exploit. Next, the attacker chooses their intended effect from a series of pre-written payloads, or they add their own payload.

Each part of the previous scenario displays how the end users shape technology. Even though there may or may not have been an updated version of software created for an IoT device, many users will not install the update. Because of this, there is little incentive for

companies making IoT devices to update their software in already released products or to remove known vulnerabilities, which is becoming more common (Schneier, 2018). As a result, a penetration testing tool such as Metasploit, that is intended to evaluate systems for known vulnerabilities can be used maliciously by hackers who may not even know how vulnerable the software is.

To change how society shapes and uses these IoT devices, the end users need to be made more aware of the most common ways in which their devices can be exploited. While companies may not want to blatantly point out that their device can cause security threats , it is necessary for them to equip users with knowledge that will affect how they use the device. The suggestion that the user enable two factor authentication does not necessarily change their behavior but making two factor authentication the default method for logging-in could increase the number of users protected. Software updates that are critical to security should be automatically applied to a constantly connected device, preventing it from being exploited through well-known and widely published vulnerabilities.

Effects of Regulations on IoT Cybersecurity:

In addition to the users, the laws, and regulations of different countries around the world also shape how IoT devices are designed. Currently there are very few laws in the United States that regulate the cybersecurity of IoT. The most recent law that regulates the IoT cybersecurity federally in the United States is the “IoT Cybersecurity Improvement Act of 2020”. This law requires the National Institute of Standards and Technology (NIST) to develop a set of minimum standards for cybersecurity in IoT devices. These standards are used to evaluate the devices’

security. Government agencies are prohibited from purchasing or using any IoT device that does not meet these standards (Robin, 2020). While this act is a step froward in regulating security in IoT devices, it does not actually place any restrictions on the security measures included in IoT devices produced and sold in the United States. While this law does affect how government users are able to use IoT devices and will shape IoT devices used by the government, it may not necessarily affect consumer focused manufacturers who are not concerned with catering to a government agency. The standards set by NIST may also improve security measures by creating a system of best practices for developers to follow. However, without proper motivation that shapes how consumers use or can use devices, it is unlikely that manufacturers will go out of their way to include these enhanced security features in their products.

In 2018 California passed a law regulating manufacturers of "connected devices". This law requires what it calls reasonable security features to be included in all devices connected to the internet. While much of the wording is vague and subject to interpretation, it does require that devices that are equipped for authentication should be manufactured with default passwords unique to each individual device. Those devices must also require the user to change the password before the device can be activated for use (Irwin, 2018) . The act of requiring these security features changes how the technology is made, and in turn changes how it is used. While this is a step in the right direction, this law is only applicable to the state of California. California which has a large presence in the technology industry. There are plenty of IoT manufacturers in other States and in countries who will remain largely unaffected by this law. For widespread change to be made in the United States, federal regulations would need to require this law and prohibit the import or sale of products manufactured elsewhere that do not

meet security the specified standards. These standards also need to be expanded to encompass more of the glaring security flaws discussed previously.

Conclusion:

Throughout this paper I have described the various flaws in the cybersecurity practices for IoT devices in conjunction with the increasing number of IoT devices in this country. If these security flaws are not rectified, much of the internet and people's privacy and security will be placed at increasing risk. While many of the poor practices would be easy for the manufacturers to fix, I have shown that there is little to no motivation for these manufacturers to change their products. For these manufacturing practices to improve device security features, manufacturers need to be given the motivation to do so.. This motivation could take many forms and does not in any way have to take the form of just one practice. This includes creating meaningful legislation that sets specific requirements for manufacturers that ensures that users that are not technically versed will be able use IoT devices without being exposed to undue cyber threats This also includes consumer education which could take the form of mandatory warnings conveying the risks to the user in an unavoidable manner and correctly indicates what threats an IoT device could potentially have .

References:

Asymkos, S. (n.d.). *Americans lost $5.4 billion in stolen packages this year, survey finds*. Yahoo News. Retrieved February 28, 2022, from https://www.yahoo.com/now/americans-lose-54-billion-in-stolen-packages-213320756.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_refer

rer_sig=AQAAAGtsrP5IGD-_ZIVJqFHFmqhFLtnc6wtS-INchgyaa81s2cTyi78ddYhQJt6A4Z1yPrFmt5qL8TMxtAzZG8il3Juc77leTOe2mYb7HFNeuj-IZIUY4706SpBzxdgYetssQxjiZDPOkkX5KMPX9KjVeudfavk3pyaATsOrkYOe8_UR

Griffiths, J. (2019, February 1). *'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out*. Cnn.Com. https://www.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl/index.html

Hernández-Ramos, J. L., Baldini, G., Matheu, S. N., & Skarmeta, A. (2020). Updating IoT devices: Challenges and potential approaches. *2020 Global Internet of Things Summit (GIoTS)*.

Irwin. (2018, September 28). *AB-1906 Information privacy: Connected devices*. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1906

Jan Saleem, T., & Ahsan Chishti, M. (2021). *Big Data Analytics for Internet of Things* (First Edition). Wiley.

Kambourakis, G. (2017). The Mirai Botenet and IoT Zombie Armies. *IEEE Military Communications Conference*.

Paul, K. (2020, December 23). *Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs*. Theguardian.Com. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats

Rattner, N. (2020, June 10). *As coronavirus restrictions drag on, Americans shift online spending from stockpiling to entertainment*.

https://www.cnbc.com/2020/04/19/coronavirus-what-americans-are-buying-online-while-in-quarantine.html

Robin, K. (2020). *IoT Cybersecurity Improvement act of 2020*. Congress.Gov. https://www.congress.gov/bill/116th-congress/house-bill/1668

Schneier, B. (2018, November 10). *We need stronger cybersecurity laws for the Internet of Things*. Cnn.Com. https://www.cnn.com/2018/11/09/opinions/cybersecurity-laws-internet-of-things-schneier/index.html

Wolfe, E., & Ries, B. (2019, December 14). *A hacker accessed a family's Ring security camera and told their 8-year-old daughter he was Santa Claus*. Cnn.Com. https://www.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html