Gavin Unrue

5/7/20

Eng 1020

Stokely Suzan

                              A Case For IoT Device Security Regulations

1. Introduction

         Tucked deep within the ordinary suburbs of Cincinnati Ohio, Heather Schreck and her husband Adam were sound asleep when around midnight what sounded like a voice pierced the night’s silence from somewhere in their home. Being abruptly awoken, neither Heather nor Adam knew what was going on, so they decided to check the footage of the IoT-camera installed in the room of their 10-month-old baby, Emma. Opening the app on her phone, Heather was soon met with the startling discovery that despite her not controlling the camera, it was moving on its own, and soon afterwards, Heather discovered the source of the noise. From her phone Heather could hear A man’s voice shouting from the IoT-camera, yelling “Wake up baby, wake up!”. Meanwhile, Heather’s husband went to investigate the shouting and rushed towards the child’s room. As Adam entered, the camera turned towards him and directed some final obscenities at him right before he went to turn it off. When the story made the news, experts concluded that Schreck's might have prevented the IoT baby monitor from being hacked if they had changed the password on the camera and on their WIFI network. Moreover, an update which treated a vulnerability in the device should have been installed.

IoT devices like the baby monitor in the story are internet connected, sensor equipped devices which gather information about their surroundings for later analysis. Some examples of IoT devices are security cameras, smart thermostats and smart watches. As compared to modern computers, like pcs or laptops, IoT devices have little processing power; just enough to collect and temporarily store sensor information. In the case of a security camera, sensor information would be what is recorded with the camera and microphone. Because IoT devices have little processing power, they rely on larger computers connected over the internet to analyze the information they produce.  Analysis for each device may look different depending on the application of the device, for the security camera video footage might be analyzed for abnormal activity by an algorithm, so that security officers can be notified of when a break in or burglary is happening.

Although IoT regulations may hinder the pace of innovation, The government should meta regulate the sale of unsecure IoT devices by mandating a minimum of physical and network security. This regulation should occur because IoT devices are susceptible to being infected by and spreading malware, several IoT devices on the market feature exploitable communication protocols and because many IoT devices are built with exploitable hardware/firmware.

2. Malware

         A botnet is a collection of computers which have been infected by malware (viruses, worms), that are sent commands by a hacker to collectively or individually perform illicit activities. In 2016 a botnet malware named Mirai started taking over thousands of IoT devices by finding devices connected to the internet and attempting to log into them with the default usernames and passwords that manufacturers initially assign IoT devices upon their creation. Any IoT device that didn’t have its default password changed by the user was added to the botnet's control, and once a device was infected it was employed in infecting other devices. In the past similar viruses and other types of malware have caused massive amounts of damage across the globe to individuals, institutions and organizations. These examples show that with IoT’s susceptibility to malware comes the risk of financial theft, and the widespread destruction of computer networks.

         In the wired magazine article "chasing the phantom", author, journalist and Harvard undergraduate Garrett-m-Graff writes about how Zeus, or Game-Over Zeus, started spreading to computers around the world via spam emails and phishing in 2006. Once a computer was infected by Zeus, hackers would gain full control over it, allowing them to steal bank information by recording every key pressed by the user. In total, this virus allowed the hacker group “Business Club” to steal 100 million dollars from bank accounts, and throughout the virus’s lifespan Business Club became a highly organized and international entity. In 2014 the virus was completely suppressed by the FBI and researchers, and in the process of their take down it was discovered that the virus was also searching its infected computers for confidential state documents; specifically information regarding adversaries to the Russian government.

         Although the devices targeted by Mirai (IoT security cameras, routers) may not have access to bank login information like a  personal computer would, IoT devices can still be used to send spam email containing malware like the Zeus trojan virus to more exploitable computers. This means that hypothetically, a botnet which infects IoT devices could be used to create a more dangerous botnet which also infects normal computers. If this virus was like the Zeus trojan, it could once again lead to millions of dollars being stolen from bank customers, and aid the development of organized crime.  With a healthy source of income, cybercriminals could start up other illegal enterprises in the real world or even over the dark web; a hidden form of the internet where drugs, hacking services and sex slaves are sold.

         Another example of destructive malware is the 2017 NotPetya worm, which author and senior journalist Andy Greenburg writes about in the wired article,  “The untold story of NotPetya”. According to the Greenburg, NotPetya was created by state sponsored Russian hackers, and after infecting a single computer, it would spread to every other computer on its network. After compromising a network, the worm would encrypt the boot record of all the computers on it; rendering them useless. After being released, a total of 10 billion dollars in damages were inflicted to banks, hospitals, airports and power companies, and an estimated 10 percent of computers in Ukraine were destroyed.  In addition, the network of a Dutch shipping conglomerate was infected with the virus causing them to shut down for a few days. If not for a lone backup of the network, a portion of the global supply chain would have been down for several weeks or months.

         If the Mirai botnet malware contained code similar to the NotPetya worm it would infect not only one IoT device at a time, but entire computer networks at a time. Once entire networks are captured, computers within said networks could be used to search for and infect other vulnerable devices over the internet; leading to explosive self-propagation. This means that IoT increases the potential spread of computer destroying malware like NotPetya. Even if these IoT enhanced cyber weapons are not directed towards the United States, their damages can indirectly impact the U.S; case in point the disruption to the global supply chain. In the event that the supply chain is disrupted there might be mass food shortages across the nation, civil unrest and shortages in medical supplies.

3. Communication protocols

         Using self-propagating malware isn’t the only way hackers can exploit IoT vulnerabilities to steal customer information; enter SQL injection attacks.  SQL, or Structured Query Language, is a programming language which tells databases what information to return when you visit a website. The information returned could be a variety of things, ranging from the amount of money in a bank account to the health conditions of a hospital patient. A SQL injection attack (or SQLIA) is an attack where a hacker tampers with a URL’s SQL code to retrieve unauthorized database information, modify database entries or to delete information.

         In a conference paper by the Institute of Electrical and Electronics Engineers (IEEE), Dr. Pankajdeep Kaur writes : “On 7th March 2014, Hopkins security staff publicly revealed that their Biomedical Servers had become a victim of SQLIA…compromised details of about 900 students  … privileges are limited to only one person i.e.; administrator…for attacker it is very easy to hack that one account and get all the privileges.…One of the biggest reasons for …SQLIA lies in unsafe architecture. One of the biggest factors for safe and secure architecture is proper validation of data values”. (Kaur et al.)

         As an example of the many documented cases of SQL injection attacks, the personal information of students attending John Hopkins University was leaked on the internet due to a SQL vulnerability in their website. As Kaur states in the paper, one of the reasons why security breaches like this occur is because websites do not filter or check user URLS for malicious code; allowing hackers to make their own URLS containing SQL commands to access unauthorized database content. Additionally, since some databases are used to store user login credentials, SQL vulnerabilities could also lead to hackers changing the login information of a powerful user, such as an administrator, to completely take over a website or server. Another reason behind the persistence of this vulnerability is the fact that it is very difficult to detect once it occurs. For a SQLIA to be detected, a website’s entire database must be scanned for abnormalities, which may not be an easy task for larger websites.

         Since IoT device manufacturers are rushing production to get a market advantage, they are leaving out basic security measures in the devices. Because of this, any apps, websites or web-based interfaces associated with these IoT devices may contain security flaws; i.e. SQLIA vulnerabilities.  This means that as a result of industries using unregulated IoT devices more and more, the chances of a web-based security breach will increase.

         Weak application security in IoT devices impacts almost every industry in which the devices are used, but in particular it is a major issue for hospitals because they are highly susceptible to cyber-attacks. According to a study conducted by Veracode, A cyber security company owned by Broadcom, eighty percent of web applications implemented in health care were also found to be very vulnerable, with many featuring weak encryption algorithms. This may allow hackers to ease-drop on network traffic and decrypt information with little difficulty. A few years after the study was published and the assessed industries were informed of their security weaknesses, it was found that only 43 percent of the vulnerabilities found in health care applications were fixed.

         Since the cyber security of hospitals isn’t as prioritized as it is in financial industries, they are more likely to either purchase unsecure products. If IoT enabled smart beds or patient monitors used by hospitals have weak application security, hackers could target their databases and extract every user’s login information. From here, if one hospital employee used the same login on said IoT device for their work account, hackers could gain access to critical information. While not everyone uses the same password for multiple accounts, it only takes a few employees to neglect their digital security for large scale data breaches to occur.

         Since hospital patient records contain valuable information such as credit card numbers, health conditions and social security numbers, they are a target for hackers who want to commit identity theft. With stolen social security numbers, names and birth dates, a hacker could sign up for credit cards and rack up large expenses on them. Additionally, if a victim had any ongoing medical prescriptions, hackers could present stolen info at a pharmacy to illegally obtain pills and other medicine. By selling these prescription drugs, a hacker or criminal organization might make a fair amount of money; adding a financial incentive to targeting hospitals. Another potential malicious use of stolen data is doxing; the act of publicly releasing personal information. Hypothetically an extremist group or individual could hack into a hospital, target users of a specific country or race and then steal information like addresses and phone numbers to be released online for other like-minded individuals to do with as they please.

In addition, another side-effect of hospital data breaches is the financial burden it places on working class citizens. In an article in the Colorado newspaper “The Gazette” ,  journalist Erin Prater details the effect of five hospital data breaches which have occurred between 2011 and 2017.

         In the article she writes: “In November 2015…More than 2 million potentially affected… This information may have included diagnoses…  and insurance information …21st acknowledged that it may have not carried enough insurance to cover all liabilities resulting from the attack and said it would be responsible for "deductibles and any other expenses that may be incurred in excess of insurance coverage”.

         When the number of people affected in data breaches runs in the millions, hospitals lose large amounts of money in lawsuits and HIPPA fines. In the quote, the fees incurred are so great that the hospital in question runs out of insurance money to pay them, and the remaining cost becomes their financial responsibility.  One strategy to deal with sudden losses in business revenue is to drive up product prices or lay off employees. In the event of such attacks, hospitals may increase the cost of their services. Normally hospital bills are extremely expensive so a raise in price may prove to be problematic for working class citizens.  In addition to SQL injection vulnerabilities, IoT devices are also prone to being hacked over Bluetooth. Bluetooth is a short-range wireless communication protocol which a handful of IoT devices use to transmit data to other devices. In volume 7 of the Journal of Sensor and Actuator Cetworks, Lonzetta Angela documents these security weaknesses.

She writes that although the newest version of Bluetooth is very secure, the previous versions suffer from a wide range of vulnerabilities. For example, in Bluetooth versions 2 and below transmitted data is only protected by a short pin number. This means that a hacker could easily find out the passcode by trying every possible number until one works, aka a brute-force attack. This would allow them to spy on Bluetooth communications.  Moreover, during the pairing process between two devices, unencrypted device identifiers or names are broadcasted so that a device can verify which device it is connecting to. Hypothetically a hacker could eavesdrop on the two connecting devices to find out one of their identifiers, and with the passcode they could imitate one of the connecting devices.  As a result, this device would connect to the hacker instead of the target device, and the hacker would be able to send and receive data to one of the devices. Oftentimes, these vulnerabilities present themselves in IoT devices.

         When making cars with Bluetooth capabilities manufacturers will often set the default connection passcode as 0000 or 1234. As a result, a group of researchers were able to use this default code to connect to random cars who were not currently connected to a Bluetooth device. Upon connecting to a vehicle, the researchers could hear everything that was happening in the car and send their own audio over the car speakers. Smart watches also suffer from pin-code related vulnerabilities. Because the pin codes on smartwatches are so short, researchers were able to use a brute-force attack to gain access to said passwords. Due to the fact that data is encrypted with this password, this allows them to spy on any outbound smartwatch data, like text messages. In addition, certain smart locks have been observed to  send unencrypted passwords over Bluetooth while unlocking a door. As a result, hackers could intercept these passwords, and unlock doors protected by these devices.

         Even if a bank or company implemented secure technology and avoided using IoT devices, an employee using  unsecure consumer IoT devices would still put the whole system at risk. Hypothetically, a hacker could target an employee who had access to a database and who was also an avid user of IoT devices. By exploiting either smartwatch or vehicle Bluetooth flaws, a hacker could spy on their personal life and study their daily schedule. Then at a time the hacker knows said employee will be away from home, they could hack into their smart-lock and search the house for a password book; enabling them to login to a company database. Even if such an employee only used one or two consumer IoT devices, Bluetooth security flaws could be used in conjunction with other hacks to gain access to sensitive information.

         Moreover, banks or databases are not the only targets: in 2010 a computer worm named Stuxnet was found in the computer systems of an Iranian nuclear facility, which commanded their uranium centrifuges to destroy themselves by over-spinning. Nuclear power plants and classified military  networks use computers which are air-gapped, meaning that they are isolated from the internet to discourage hacking attempts. With less ways to attack these high value targets hackers need to find more creative hacking methods, such as social engineering. Bluetooth vulnerabilities may give hackers more versatility in conducting these hacks.

         This is a serious issue because the threat of State sponsored cyber-attacks against critical U.S infrastructure was already present before the popularization of IoT devices. In the New York Times, Nicole Perlroth, a graduate of Princeton and Stanford University writes about Russian hacks directed towards U.S infrastructure.  Perlroth writes that in a new report by the Department of Homeland Security it’s been revealed that Russian hackers have been targeting facilities which control critical infrastructure such as power plants and water control systems. The report states that Russian hackers were taking pictures of machines used in nuclear plants and collecting information about how energy facilities work.

         Moreover, computer and forensic analysis has indicated that Russian actors have been mapping out the corporate and computer networks of multiple power stations. Officials believe that the aim of these hacking attempts is to disrupt access to resources in the case that conflict between the States and Russia breaks out; as to give Russia the upper hand. Considering that Russian hackers hacked into a Ukrainian power plant in 2016 and successfully shut off power to 200,000 citizens, these reports have serious implications. In the case that an attack against a power grid were to succeed, hospitals would lose the ability to care for patients, fuel and water systems wouldn’t work due to being electrically powered and all contact to emergency services would go offline. Even if a blackout attack were to last only for a couple days, billions of dollars in produce would be lost, people would die and the U.S would be vulnerable to further attacks.

 4. Hardware/firmware

         IoT device vulnerabilities don't just stop at SQLIAS and malware-botnets, another way that hackers can gain access to log-in credentials and other valuable information is through exploiting security flaws in the hardware of IoT devices. In an IEEE journal article, Omer Shwarts writes about the ways in which IoT devices can be physically hacked into. Shwarts explains that A UART port is a communication wire left on most IoT devices after being manufactured, which is used to access its code interface for debugging purposes and for developer interaction. when an IoT device turns on (or boots), the device typically loads all of its necessary files and goes into a login screen. However, since most IoT devices are left without a boot-loader password, a hacker has the ability to modify its startup sequence through its UART port and gain a high level of control over the device. From here hackers can use this access to transfer over a copy of the devices file system, which contains an encrypted version of the devices passwords and WIFI login credentials. After these files are recovered, a special program is used to randomly guess the decryption key and access the passwords, which in the article worked for 11 out of the 16 devices tested.

         Typically all of the information you send and receive online is protected with an encryption protocol called https. With access to an IoT device’s WIFI login credentials hackers are able to perform an “evil twin attack”, to side-step https and view everything you send online.

In this attack, the hacker creates a WIFI hotspot with the exact same name and password to trick people into connecting to it instead. Once a user connects to their network, the hacker has control over inbound and outbound network traffic. When a user attempts to connect to a secure webpage, the hacker can send them an unencrypted version of the page while they connect to the secure page themselves. When the user inputs information into the page, the hacker records this unencrypted info and sends it to the encrypted page to provide a response to the user.

         This means that the hacker is able to act as a middleman between the webpage and the user and collect any information the user types online. This information can range from company login information to things as simple as a social media post.  Because many IoT devices like security cameras and smart doorbells are publicly accessible, it’s very possible that their hardware vulnerabilities could be exploited in part of a larger hack. For example, a group of hackers being paid to damage a rival company’s reputation could climb up to a rooftop camera, hack it and identify a building’s WIFI password. From there, they could set up an evil twin WIFI network, extract employee login information, and gain access to their database. With access to the database, the hackers could delete customer information or even leak it publicly.

         In addition, although most IoT hardware vulnerabilities stem from the fact that manufacturers are rushing production, some may even occur as the result of supply chain attacks. In a BBC report, journalist and University of Warwick graduate Vaswani Karishma writes that recently the U.S placed a ban on all business with one of the largest telecoms equipment companies in the world, Huawei. This is because there are laws in China requiring all individuals and businesses to comply with national intelligence work and fears have cropped up that the government may require Huawei to add hackable security flaws or code backdoors into their products; allowing international spying. These fears are not unfounded however as Huawei has been accused of stealing robot designs and other material from companies such as T-Mobile, Cisco, Motorola  and Nortel.

         Since IoT device manufacturers are encouraged to spend as little as possible during the IoT device development process on cyber security, it’s unlikely that they would detect hidden security flaws implemented by third party processors or components. Furthermore, while making a product, it is actually cheaper in some cases to subcontract or hire other companies to do a part of the work; whether this be manufacturing, advertising or making designs for the product. Having multiple third parties involved in the design process substantially increases the risk of a backdoor being installed, a risk that IoT manufacturers might not even think to mitigate. Considering the anticipated explosive growth of the IoT market in the next few years, this could mean that thousands of devices with code backdoors could be installed throughout the country; allowing for said third parties to exploit them in ways discussed throughout this paper.

6. Counter argument

         One argument against government regulation over the IoT device market is that it would slow the pace of innovation and that it it’s unnecessary since the market will regulate itself. However, in the Oxford book of regulation, economist Martin Cave details the shortcomings of such an argument. He writes that there are three forms of regulation: self-regulation, meta and standard regulation. Self-regulation usually entails a company subjecting their work process or end product to restrictions or limitations in order to attain some type of goal. Because companies typically have a more intimate knowledge of their industry than government regulators, self-regulation allows them to create realistic and cost-effective goals to reach. Meta regulation is where companies are able to self-regulate, but they are overseen by government regulators and are sometimes held responsible for not meeting their self-imposed benchmarks; i.e. hefty fines. Meta regulation combines the industry-knowledge benefits of self-regulation with the accountability of standard regulation.

In the chapter, four examples of power companies self-regulation and meta regulation are given, with each attempting to reduce their environmental impact. In two of the examples provided, the catalyst for companies to start self-regulation or meta regulation programs are horrible accidents endangering public safety. Three fourths of the programs failed to produce any significant progress towards goals of reducing emissions or cultivating better safety practices. However, one did extraordinarily well due to the fact that a firm’s failure to reach agreed upon benchmarks would be punished by a regulatory committee.

         Unfortunately, for a company to take self-regulatory actions it requires its consumers to find issue with the apparent quality of the good/service itself or to be involved in an accident involving the good/service.  Since IoT security can be an esoteric subject with a high information barrier,  the common consumer or small businesses will likely trust any company that claims to produce secure devices. This leaves industries such as IoT immune to self-regulation until security breaches and large-scale IoT hacks occur. Moreover, even if the IoT market did start to regulate itself government-based accountability programs would need to be implemented for any real change to occur.

6. Conclusion

         The standard protocol for devices or machines which have the potential to cause harm if poorly manufactured is to mandate that basic security features are present before said product is sold. For example, automobiles and aircrafts are subject to numerous safety regulations with the aim of reducing the amount of harm done to their user base. IoT devices are no different than any other contemporary technology or machine, and to ensure that they are safe to use by businesses or consumers regulation is necessary.  Without regulation, unsecure IoT devices have the potential to cause massive financial losses to users,  instigate organized crime and encourage politically motivated cyber-attacks. Even if regulation is a deterrent to the growth of an emerging technology, if security is not built into IoT devices then the losses procured by cyber-attacks will begin to slow the demand for IoT devices altogether.

7. Works cited

“Kaur, Pankajdeep, and Kanwal P. Kour. SQL Injection: Study and Augmentation, **2015 International Conference on Signal Processing**, IEEE ,2015”

“Graff, Garrett M. “Inside the Hunt for Russia's Most Notorious Hacker.” Wired, Conde Nast, 27 June 2017, www.wired.com/2017/03/russian-hacker-spy-botnet/.”

“Shwartz, Omer, et al. "Reverse Engineering IoT Devices: Effective Techniques and Methods." IEEE Internet of Things Journal, vol. 5, no. 6, 2018, pp. 4965-4976.”

“Perlroth, Nicole, and David E. Sanger. "U.S. Says Hacks Left Russia Able to Shut Utilities: National Desk." New York Times, 2018.”

“ Prater, Erin. "5 Data Breaches Healthcare Providers Will Find Frightening." *Gazette, The: Web Edition Articles (Colorado Springs, CO)*, 4 Apr. 2017. *Access World News*”

“Lonzetta Angela, et al. "Security Vulnerabilities in Bluetooth Technology as used in IoT." Journal of Sensor and Actuator Networks, vol. 7, no. 3,MDPI AG ,2018, pp. 28.”

“Greenburg, Andy , The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Sandworm, Wired, 08/22/20,”

"Government Sector Ranked Last in Remediating Web and Mobile Application Vulnerabilities: Veracode's 2015 State of Software Security Report Benchmarks Risk Profile for 34 Industries Across Seven Vertical Markets.", Software World, vol. 46, no. 4, 2015, pp. 22”

“Baldwin, Robert, Martin Cave, and Martin Lodge. The Oxford Handbook of Regulation. Oxford University Press, New York Oxford 2010.”

“Vaswani, Karishma, “Huawei’s Founder Speaks To BBC”, YouTube, uploaded by Huawei, Feb 24 2019, www.youtube.com/watch?reload=9&v=vxoeLLq14zI”