Assessing Security Risks with the Internet of Things

Faith Mosemann

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2022

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____

Mike Kipreos, D.B.A
Thesis Chair

_____

David Holder, Ph.D.
Committee Member

_____

James H. Nutter, D.A.
Honors Director

_____

April 23, 2022

Abstract

For my honors thesis I have decided to study the security risks associated with the Internet of Things (IoT) and possible ways to secure them. I will focus on how corporate, and individuals use IoT devices and the security risks that come with their implementation. In my research, I found out that IoT gadgets tend to go unnoticed as a checkpoint for vulnerability. For example, often personal IoT devices tend to have the default username and password issued from the factory that a hacker could easily find through Google. IoT devices need security just as much as computers or servers to keep the security, confidentiality, and availability of data in the right hands.

Assessing Security Risks with the Internet of Things

Internet of Things (IoT) devices like security cameras, computerized door locks, smart thermostats, and even smart fridges, continually grow in popularity. Installed in personal homes to office buildings, the use of IoT devices quickly became a part of everyday life. These helpful appliances can think or predict by preprogrammed functions the user's actions or requests. IoT can eliminate minor and tedious tasks, like creating a grocery list. A smart fridge connected to Alexa, can add milk to the grocery list after the user finishes it off. It can even go ahead and place an online grocery order and set up afternoon or next day delivery to the house. Another example is for the user to connect their smart stove to an app on their phone so they can turn off the oven from another room in the house.

The possibilities are endless of creating smart devices and putting in an end to mundane tasks. However, security and privacy concerns rise with the increase of these quickly manufactured devices. Producers of IoT tend to not push frequent security patches and the company stops supplying tech support within a few years of the release date. Even in corporations, IoT can present security risks that need containment or delegation to a third party. Securing IoT devices presents a tricky challenge due to lack of security accountability in the industry as many organizations focus on sending their product out to the public as quickly as possible. Companies and individuals must consider the benefits and risks of a device to decide if it is a good addition to their network. Although they may add interesting features, individuals and companies need to consider the risks and benefits of employing such a device and configuring the necessary security measures for the integrity of their network.

Each year as IoT grows, users implement this new smart technology into their networks. These devices are more features focused instead of security (Zurkus, 2019). People buy them for

the convenience they give. Instead of someone needing to go into the next room to turn on a light switch, they can connect their lights to something like the Google Home app or ask Alexa to turn them on. Asking Alex to play a song instead of searching it on Spotify instead of having to type it. The purpose of the IoT is to make life easier. However, considering the security side of it, one could say they sometimes do the exact opposite. The companies that create these devices tend to not push out software or firmware updates as often as they should, or they discontinue servicing an old product even though it is only a few years old. A common vulnerability is the factory set default password tends to stay for the entirety of the IoT device's use. How IoT devices function is by gathering as much data possible (Zurkus, 2019). If someone does hack into a system, they could have access to enormous amounts of data. For example, a security camera (or baby monitor) collects data of people going in and out of a building and could capture access codes depending on its location.

Consumer Understanding of IoT Security

Some security professionals notice a disconnect between knowledgeable buyers on IoT and suggest a straightforward way for customers to tell the level of security IoT devices. Each IoT device has different priorities and computing abilities which means their level of security differs due to their functionality. Unfortunately, IoT technology tend to lack basic security features and detailed documentation like software updates or unique passwords (Johnson, et al., 2020). Lack of authentication and other fundamental security features can lead to a risk of man-in-the-middle attacks (when attackers steal or alter data while it is in transit). In a recent study, only a total of nine percent of customers trust their IoT device while forty-two percent of suspicious customers continue to use them (Johnson, et al., 2020). Security concerns also varies with the ages of the customers.

A necessary concern related to IoT, is that consumers have no way of comparing security features of all different devices. There is a predicted correlation between consumers discovering security issues with IoT and a drop in adoption in technology (Harper, 2016). A proposed system for consumers to understand security levels of IoT devices, is a graded scheme of one to five stars based on the security and energy levels of the device could help customers decide if the device is a good fit for them (Johnson, et al., 2020). Besides helping consumers, manufacturers would more likely put more effort into their publicly displayed product's security features. Having a quick and straightforward way to tell the security of a device is a valuable way to encourage manufactures to increase security measures in IoT.

In an experiment done in 2016, the unified theory of acceptance and use of technology (UTAUT) for security awareness used quantitative procedures to analyze the impact. Their findings surprised them because they thought users would select security as a top priority. Although participants did express a concern for a security, results showed that users expected protection of their data from the manufactures of the devices. Simply put, if the product was on the market, then most individuals trusted the company for it to be secure. The surprising factor was that although users would express concern for security, they would trade this for convenience (Harper, 2016). For example, no one enjoys memorizing multiple passwords for all their accounts they have so users tend to use a small number of different passwords over and over. This is a major security risk, but individuals do it because it is more convenient for them than memorizing hundreds of passwords. Users should not trust manufacturers or retailers when it comes to security, but instead they should do their own research and then choose the best option they can find. Even then, it should be from company that has a good reputation and that will hopefully provide tech support (and security patches) for years to come.

Structure of IoT Devices

To understand the lack of security involved with IoT devices, one needs to understand the structure of these IoT devices. When analyzing a smart home, there are four parts of a smart home to consider and they are the service platform (the service provider for the Internet), smart device (IoT system), home gateway (modem) and a home network which is the router and wireless access points that the IoT technology connects to (Romano, 2019). All these parts are what makes an IoT device such as Alexa able to function. Every smart device's architecture differs based on the operating system (OS) that includes an application layer, framework layer, module core library and the OS kernel layer. The application layer has the applications that the device must fun, the application framework is the libraries and managers that monitor activity and install packages and the module core library stores middleware, input/output (I/O) configurations, and display (Romano, 2019). Authentication is one of the basic ways in securing IoT systems like verifying the integrity of the firmware image by using a hash chain. The hash is a unique value of the firmware file that cannot be replicated by hackers so system administrators can make sure that the firmware file is not a hoax.

Additionally, to help system administrators and consumers to judge how severe the threat level of cyber-attacks, the United States Federal Government created the FIPS 199, which measures the impact on the system from low (limited effect on the system), moderate (significant affect) and high-level as severe effects (Romano, 2019). When cyber-attacks are released to the public, the report will include what level the attack was and therefore, system administrators can help prioritize what attacks to focus on. Knowing the basic structure of smart devices and how the government ranks cyber-attacks, can help consumers and system administrators to choose the best device for their business.

IoT devices rely on a Bluetooth connection to communicate and use a protocol called Bluetooth Low Energy (BLE) to carry out their tasks. In September of 2020, a vulnerability concerning IoT devices reconnecting to each other was labeled as BLE Spoofing Attacks (BLESA). IoT devices implement BLE protocol due to its energy efficiency and simplicity, but its vulnerabilities are: "authentication during device connection is optional and not mandatory... [and its] specification has two possible authentication procedures when the client connects to the server after pairing and authentication can be avoided" (Montalbano, 2020, para. 11). Authentication should never have an opt-out option. IoT devices are designed to easily disconnect and reconnect between sensors for monitoring and sending data to servers. When a device connects to the server it receives its attributes so it can connect in the future. There is no security precaution against this because the server is made to connect with other BLE enabled devices. In a BLESA, the IoT device attacking connects to the server to receive its necessary attributes (which are in plaintext). After this, the imposter device clones the server's MAC address and starts broadcasting its spoofed packets to clients. This Bluetooth vulnerability was found in Linux, Android, and iOS devices. The IoT device and server "development team said it would replace the code that opens its devices to BLESA attacks with code that uses proper BLE reconnection procedures that are not susceptible to attacks" (Montalbano, 2020, para. 15). Apple was the first to release a patch for it several months later.

Manufacturer Vulnerabilities

IoT systems are usually vulnerable due to bugs found in the software or possibly in the hardware as well. For these systems to be considered secure, the security in the hardware (implementation, embedded systems, tamper proof and resistant), in the services and the digital rights management must be addressed (Lee et al., 2019). Companies should focus on achieving

secure application execution (SAE) and platform specific execution (PSE) for their systems so their customers confidence rest in knowing that their data is safe. Although SAE focuses on no code executed code being skipped, there are ways to get around this such as using a JUMP instruction that allows for code to be legitimately skipped.

However, if used illegitimately, code could not be executed due to modifications or deletion (Lee et al., 2019). In this study, researchers focused on securing PSE which is securing bonding hardware and software together. It seeks to ensure that only applications from authorized parties can execute (Lee et al., 2019). However, the two existing problems in this method is that PSE only ensures the current application is executing correctly and it also does not test the identity of the author of the code, and it ensures that only the applications personalized to the device by an authorized party, but it will not look at the legitimate applications failing to operate normally (Lee et al., 2019). Although PSE and SAE start from a solid foundation, they are not fail-proof and need some adjusting. By adding security checks using the function pairs CALL and RETURN, each function could be recalled again to see if by using a check value, if the functions had run or not. This method is focused on solving any vulnerabilities in the design aspect of code. Other aspects like securing the location of the hardware and encryption of data transmitting should also be evaluated.

In another instance, a flaw in the design of a module used commonly in IoT devices was discovered in August of 2020, that if exploited, attackers could completely shut down an entire city's electricity or overdose a patient. This vulnerability is in the Cinterion module which is in IoT devices that send and receive data over wireless networks. Although they were developed by a Thales (a company that designs electrical systems for aerospace markets) with a well-known reputation, if the vulnerability in the Java code was exploited, data like passwords, encryption

keys and certificates and even control the system remotely (O'Donnell, 2020b). The company immediately sent word to their customers and clients about the vulnerability and issued a patch to fix the issue. Basically, the string that stored these values, could accept characters such as double forward slashes instead of one and periods this would bypass the programmed security check. Attackers could access hidden files that only administrators should be able to access.

This IoT module was found across utilities such as medical devices that could tell a nurse to administer a higher amount of insulin and cause the patient to overdose or to cover up vital signs. Researchers discovered that a malicious actor could cause blackouts in the city and/or damage the electrical grid with this vulnerability and if the equipment is used in medical devices or industrial hardware, they will have a harder time applying the patch (O'Donnell, 2020b). To put in perspective how many IoT devices there are globally, researchers predict that by 2025, that the number will reach 55.9 billion (O'Donnell, 2020b). If even a fourth of these devices had this vulnerability, and the administrators of the distributed system did not push the security patch, a high number of individuals could be in danger. Just because a IoT device is from a trusted manufacturer does not mean there is no possibility of security weaknesses. Ultimately, the system administrator should choose the most secured device they can find but they should also place their own security measures for a layered security approach.

IoT Attacks

Another IoT device, a third-party smartwatch created by a Chinese developer made for people with dementia with reminders such as taking medication. Features also included reminders of everyday tasks and tracking their children. Unfortunately, researchers: "discovered an unrestricted server-to-server application programming interface (API) behind the app that allowed them to carry out a number of malicious activities" (O'Donnell, 2020a, para. 5). The

API was set up with a string hardcoded into it which could allow someone to remote in and for the API to automatically assume it was a trusted server. It could then send any commands through JavaScript. The attacker could make a phone call, send a message, fake a message from a parent or access the camera (O'Donnell, 2020a). One of the most destructive things about the hack is that an attacker could send a message to the user to take their pills and could lead to an overdose. Also, the credentials to the MySQL database where it stores passwords to accounts and emails were open source and in plaintext. After the vulnerability was discovered, the developers closed it, but they did not reveal how long the vulnerability stayed open. Situations like this happen often with cheaper IoT devices and often the customer remains unaware unless it reaches the news.

Often, the term node hijacking, is when an attacker takes over one IoT device (a security camera for example) and uses it to attack or infect another node on that system. Usually, attackers hack a node by creating a Distributed Denial-of-Service (DDoS) attack. In one case, attackers took over, "100,000 home IoT devices like televisions and fridges and then used these devices to target individuals and businesses with malicious emails" (Alani, 2018, p. 141). In 2017, a hijacked IoT botnet called Mirai infected windows based IoT devices because of developments of malicious software that infected personal computers. It was discovered that Mirai spanned over, "164 countries… and went from 213,000 to 483,000 devices in two weeks" (Alani, 2018, p. 141). Another attack is called a reflective attack where the attacker sends a request with a spoofed IP address for all devices to respond directed to a targeted IP address. In this approach, the attacker does not directly attack, but instead amplifies traffic from other devices to inflict more damage (Alani, 2018). One proposed design of securing IoT devices is to split an encrypted key among each IoT device and have devices communicate with each other

while using a key distribution arbiter (KDA) to decrypt the key. This can fight against brute force attacks, however, concerns like too many requests of the key could possible slow down the network.

A known botnet (hijacked devices working together maliciously) called Mozi, originally took over routers from Netgear, D-Link and Huawei and DVRs, but expanded to IoT systems. Lack of command-injection (CMDi) security is a common vulnerability found in IoT devices due to lack of security in the web and debugging interface (Seals, 2020c) Due to Covid also moving more activities and jobs online, malicious actors put their sights on hijacking or exploiting IoT systems. Both Mozi and Mozi's botnet counterpart, Mirai, focus on using the CMDi to first get into IoT's device web interface, then change PHP modules to allow for remote execution for the hackers. This usually looks like Mozi or Mirai pushing updates when it is CMDi. This botnet does brute-force attacks against Telnet credentials by going through a hardcoded list (Seals, 2020c). After Mozi botnet cracks into the device, it binds its local UDP (User Diagram Protocol) port 14737 while killing any processes that use ports 1536 and 5888.

In Mozi's code, there is a hardcoded distributed hash table (DHT) that acts like a lookup service for P2P nodes to find and communicate with each other on Mozi's P2P (peer-to-peer) network (Seals, 2020c). After the new node receives an ID (20 bytes) it will send an initial HTTP request to register itself on the P2P network, and therefore the botnet. Another popular botnet called the DDG, is a P2P network dedicated to coin-mining. These are just some of the ways that hijacked IoT devices can create a botnet and do whatever request they are programmed for such as coin-mining or becoming a hostile network.

Even well-known companies such as Microsoft, are not exempt from attacks on their IoT devices. In Microsoft's operating system for its IoT networks is Azure Sphere (released in 2018)

and has a secured microcontroller unit (MCU). Remote code execution bugs allowed for privilege escalation flaws and impacted the entire cloud security platform. The first two bugs affected Azure Sphere 20.06 and could process heaps of data stored in memory and make it executable (Spring, 2020). The second code execution vulnerability found in Azure Sphere 20.07 was if a local attacker used a shell code to process nonwritable memory and then exploiting a vulnerable application that hides in Azure Sphere and processed within Microsoft's custom Linux based OS (Azure Sphere). In another high-severity vulnerability found in Azure Sphere 20.06, allowed for privilege escalation and for multiple applications to receive the same unique identifier (UID) numbers. All that an attacker had to do was to broaden the attack surface by modifying the "uid_map" file (Spring, 2020, para. 20). Security patches did eventually solve these vulnerabilities, but the public is reminded that just because technology is from a well-known corporation, does not mean their devices are flawless.

Another vulnerability, called the Ripple20, infected millions of IoT devices that used TCP/IP software library. The TCP/IP protocol allows devices to connect to the Internet and other networks and is implemented in many devices from printers, medical to industrial equipment. (Seals, 2020a). Hence why this bug is called the Ripple20 because the effects rippled across equipment in different industries and people affecting all. The main concern with this vulnerability is that it allowed people to enter from outside of the network (meaning they did not even have to be on site to receive access). The Ripple20 bug is nineteen different vulnerabilities that varied from allowing remote code execution, sending malformed IPv6 packets, infecting Domain Name System (DNS) services and taking over the devices sent the requests. Four of these vulnerabilities from the Ripple20 bug, scored a ten out of a ten on the CVSS severity scale, the fifteen had a score of 3.1 to 8.2 (Seals, 2020a). Most of these vulnerabilities are zero-day

attacks (meaning that cybersecurity specialists have not seen this attack before or presented in this way). These types of attacks are typically harder to contain and recover from because cybersecurity specialists and system administrators are figuring out what to do as the attack is going on. Each level of hardware and software capabilities should have precautions to protect against attacks and keep data secure when at rest and in transport. In this case, companies such as Intel, HP and CERTCC pulled together to issue alerts to their users to update their devices as soon as possible. Administrators should stay up to date with alerts and check for security patches to deploy on their devices to avoid something like a zero-day attack. It is also recommended for IoT devices (unless necessary for their functions) to be continually connected to the Internet. Only having them online for short periods of time, when necessary (for updates for example or sending data), can cut down on attacks.

IoT Challenges

While the number of IoT devices continue to grow not all devices have the same level of vulnerability as others. It is estimated that the number of IoT devices that connect to the Internet have exceeded 23 billion (Alani, 2018). These devices, especially wearable ones, like smart watches for example, store large amounts of private data and have sensors to consume input. The most common security challenges that IoT faces is object identification and authentication. An imposter device can try to connect to a security camera for example and try to push updates or excel privileges to reach other gadgets. Other security concerns are, “data protection, threats to availability (attacks of DoS [denial of service] and DDoS [distributed denial of service]), unauthorized access, man in the middle (MITM) attacks, compatibility threats, application threats” (Alani, 2018, p. 140). These attacks pray on vulnerabilities in IoT devices and the goal

of system administrators and hopefully manufactures is to create ways to secure their networks for access for authorized users only.

The trickiest thing about IoT devices that make them hard to secure, is that they are all different from their physical appearance to their purpose and where they are hosted. It is said that IoT is one of cybersecurity biggest challenges and most embarrassing failures (Giaretta et al., 2019). However, they tend to lack basic security configurability and are mostly blamed on the manufacturers who left those options out in the design phase. Other times, it depends on the nature of the device and its different goals, hardware, software, sensors, communication protocols and computing power. Their range is broad making it challenging for network administrators to create a secure infrastructure that would eliminate these concerns (Giaretta et al., 2019). Some administrators try to host these IoT on the cloud which can cause problems in performance.

An approach called Fog computing has helped to move: "services from the cloud to the edge of the network… install a dedicated device [Fog node] which centralizes all sensor data, time-bound tasks, and data traffic gatekeeper… [and] network policies and real-time policy enforcement techniques based on traffic monitoring" (Giaretta et al., 2019, p. 2). This centralized device acts as the doorway for traffic between nodes (almost like a firewall). However, the problem of lack of security from the manufacturer level to the growth of complexity in IoT systems, is a big demand for system administrators to keep data traffic secure. Problems such as hard coded default passwords or the only option to login into the device is admin level (devices should always be set with the bare privileges to accomplish the task and access granted as needed).

Although this may not seem like a big deal, if there is only one login level available, it is impossible to do a technique called layered security. Layered security is multiple measures of security in place to add difficulty and deterrence of hacking. This lack of security configuration is blamed on the manufacturers and gives system administrators a challenge to properly secure their devices. Other vulnerabilities from IoT can include: “privacy leaks, insecure network communications and/or protocol, vulnerable cloud/web services, insecure mobile application, vulnerable system/firmware, insufficient security configurability” (Giaretta et al., 2019, p. 4). These vulnerabilities put all data gathered by the distributed system at risk for interception and can often act as a gateway into a whole network for an attacker. In turn, these insecure measures on small devices can drastically impact data of a company like business transactions, personal identifiable identification, usernames, and passwords, or even to create a group of hostile IoT gadgets called a botnet. Manufacturers should discuss with their clients and customers about how they are using their devices and what security measures they would like to see in place, to create a solution that works.

How IoT Differs from Computers

Some individuals compare the security of computers to the IoT and consider, if computers can have reliable security, then why not their smart fridge? Well, IoT has different pieces compared to a computer such as the operating system and other physical limitations. Even security solutions that are commonly applied to the Internet such as cryptography cannot be applied to IoT devices due to constrained resources in the size of technology. Another complication is if the device has sensors and radio frequency identification (RFID) because they receive more input (Weiqiang et al., 2019). However, a promising and low-cost solution for securing IoT is physical unclonable function (PUF) which is a: “hardware-based security

primitive and can be used to generate a key online or a uniquely identify an integrated circuit (IC) by extracting its internal random differences using so called challenge response pairs (CRPs)" (Weiqiang et al., 2019, p. 1). Security focuses on hardware or software or both. This hardware focused approach, physical unclonable function (PUF), generates a key and identifies circuits for devices to connect and share information more securely.

Security Solutions for IoT

Correspondingly, IoT devices communicate to each other and the Internet while collecting and storing data. What makes securing IoT a struggle is that sensitive information (such as encryption keys, digital signatures, login credentials) must be distributed across devices and then be available to retrieve later. It is too dangerous to store this sensitive data on one device incase that one is jeopardized it would compromise an entire network. If the data is shared across devices there is still a possibility of attackers compromising multiple devices of them and creating a botnet. One solution presented in 2019, for sharing confidential information on IoT systems had two features: (1) incorporate Threshold Secret Sharing (TSS) to split the data among devices on the system and (2) then to retrieve it collaboratively by the devices (Bu, Isakov & Kinsy, 2019). Because the secret (key) is split among the IoT system, this can even help system administrators to identify the compromised devices while keeping the secret unknown to the attackers.

In a distributed system such as the IoT, TSS is set up by the administrator who takes a part of the secret and gives pieces of it to the devices. Only when the secret is reconstructed collaboratively by the subsets of holders and the size reaches a minimum number (called the threshold) can it be decrypted. If the number does not reach the threshold, the secret remains encrypted and safe from retrieval from hackers (Bu, Isakov & Kinsy, 2019). This type of key

management is common in wireless sensor networks. A key is shared among nodes and must be retrieved collaboratively for a digital signature or other cryptographic functions (Bu, Isakov & Kinsy, 2019). If a corrupted node is discovered than the system will revoke and replace it by the number of healthy nodes required to reach the threshold. However, TSS is not invincible. It is vulnerable to man-in-the-middle (MITM), share manipulations, leak of secret or retrieval of the incorrect secret. Usually, the TSS can keep the privacy of the secret if the system is below the threshold, but it cannot guarantee the integrity of the secret. It can also only detect if there are cheaters, it cannot identify the number of cheaters in the system (Bu, Isakov & Kinsy, 2019). The ultimate key to securing of IoT is properly securing and encrypting the secret that is to be share among the distributed system.

In one experiment with a IoT system of heat sensors in case of a fire building which would measure the fire intensity at various locations and motion sensors to detect human presence. This distributed system was nicknamed Odysseus (Bu, Isakov & Kinsy, 2019). When a client would request data from the group of sensors, the secret (encryption key, signature, or login credential, etc.) would be used to access the sensor data. The dealer and clients could be trusted but the sensors were not secured. Because of this, a secure protocol for the privacy and integrity of the secret and error tolerance was necessary. It ensured the integrity of the key even if attackers created ways to forge fake secret keys. This scheme for Odysseus could also detect and identify cheating and compromised nodes (Bu, Isakov & Kinsy, 2019). This research done on the Odysseus system can help other distributed systems to be more secure using TSS and helping to ensure the integrity of the shared secrets.

Another approach, called the “vanish” approach, is when a hijacked node is discovered and therefore the threshold cannot be reached, but instead of replacing it with a healthy node, it

makes the secret key disappear (Bu, Isakov & Kinsy, 2019). Another popular IoT system is bank card payment systems which use the Hardware Security Module (HSM). Some are produced and distributed by certification authorities (CAs) and registration authorities (RAs) to create and distribute secret keys via a public key infrastructure (PKI). Using a multi-part user authentication scheme, which is "usually threshold secret sharing—namely DNS Security (DNSSEC) uses DNS servers to connect users and their Internet destinations) securely [and] verified. Root key is then split and shared among seven holders all over the world. If there is an attack, five or more holders can come to a United States base and reconstruct the root key by using their shares to restore Internet connections" (Bu, Isakov & Kinsy, 2019, p. 2). This of course is an extreme way to keep distributed systems (IoT) secure which makes sense for systems like bank card payment systems in this case.

VLAN Solution

A common fix, especially for businesses, is to configure a Virtual Local Area Network (VLAN) on their Local area network (LAN) for the devices to solely run on instead of having the IoT devices on the sector as other departments in the business (Zurkus, 2019). Therefore, if someone hacked into that VLAN to access the cameras, they could not reach other parts of the network because the network is segmented. IoT devices are also created to work together with each other which can cause them to be, "susceptible to botnets that can use their computing power for DDoS [Distributed Denial of Service] attacks, crypto jacking, and other schemes" (Zurkus, 2019, para. 5). Due to the enormous amounts of devices, it "opens up new attack vectors for criminal hackers to exploit, such as the IoT-based distributed denial-of-service (DDoS) attack on Dyn [Inc.], which brought down Twitter, SoundCloud, Spotify, Reddit, and a host of other sites" (Weiqiang, et al., 2019, p. 2). Although their futuristic appeal and

convenience can appear useful, their features of broad connectivity and data sharing is a big security risk that must be addressed.

IoT Encryption Methods

One proposed method of encryption for IoT devices is using the Elliptic Curve Cryptography (ECC) for asymmetric encryption and signature schemes and is recommended by NIST for eight-bit AVR processors found in the IoT platform (Zhou et al., 2019). The eight-bit AVR processors are sold at a low price, have high performance and low energy consumption. Due to IoT's limited computing power, storage, and energy consumption increases the difficulty of encrypting and decrypting data. The most recent method of the ECC is SM2 and uses a set public key cryptographic algorithms using the elliptic curve method. The ECC method, chooses at random points on the curve to create keys from. This reduces storage and transmission requirements while also providing the security needed for data in each of three stages (transit, storage and in use). The results concluded that this study, the elliptic curve cryptography used co-Z along with the Montgomery ladder algorithm to create the fastest NIST P-256 and SM2 curve implementations on an eight-bit AVR processors (Zhou et al., 2019). Because it works faster and the code is smaller than other proposed solutions, for any company running this type of processor should investigate this security solution and see if it is the right fit for them and their company.

The most efficient and low-cost approaches analyzed so far is called is called XRBR and XRRO PUF which only requires 12.5% of hardware compared to other PUFs tactics analyzed where the key is stored in non-volatile memory (NVM) (Weiqiang et al., 2019). This science of securing IoT using this approach is detailed and involves algorithms but basically the physical unclonable function (PUF) extracts the unique value from integrated circuits from process

variations that occur during the manufacturing process and quantify internal mismatches using binary sequences. Each computer chip is unique almost like a fingerprint even if their structure is an exact replica of one another, the PUF will be able to tell the differences. This PUF is electrical and is automatically generated and disappears if there is no power which is more secure than storing a key in non-volatile memory (NVM) (Weiqiang et al., 2019). This is a good technique for IoT devices because no other device can clone their chip and therefore each value from the circuit is different. Hardware costs are also low for this security technique.

Authentication

IoT based wireless sensor networks can use authentication protocol like a symmetric key to help secure data. In one type of IoT, Wireless Sensor Networks (WSN) are composed of miniature sensor nodes that take data from their surroundings and send it to back to the server. These sensor networks are the foundation of the IoT, but one high cause for concern is authenticating remote users to access said data from these sensors. One study suggested using enhanced symmetric key-based authentication protocol for IoT-based Wireless Sensor Networks (WSN). This would provide: “user traceability, stolen verifier, and DoS attacks… [and] has a 52.63% efficiency compared to baseline protocol” (Ghani et al., 2019, p. 1). These WSN vary from each other in size, architecture, and deployment. Typically, they link with wireless using RFID interface and sensors which typically allow this system to be deployed at a low cost. Because it is so widely used, it is a good target for hackers.

However, due to the WSN physical limitations, it is hard to create security that will not drain the sensors power or waste energy which would lead to a shorter network life. The symmetric key approach (examined in a simulation using BAN logic), “enhanced authentication protocol that resists all known attacks… determines computation efficiency, analyses how much

data is exchanged during transactions and analyzes it with existing protocols" (Ghani et al., 2019, p. 2). In this procedure, the gateway node sends a smartcard to the user by using a secure channel "then a session key [symmetric] has been exchanged between the sensor node and the user" (Ghani et al., 2019, p. 7). The four phases of this proposed secure connection are: "registration, anonymous authentication and key exchange phase, password update and new node addition" (Ghani et al., 2019, p. 3). Breaking each of these steps down involves algorithms that prove why it is necessary to securing the connection between nodes and the remote user by using exchanges of keys, updating passwords, and adding a new node. However, this principle revolves around the session key being exchanged securely. Hackers are always improving their skills and therefore system administrators must be on the look for new ways to strengthen their security for their distributed systems.

Identifying Hijacked Systems

Knowing how to successfully identify hostile or hijacked IoT devices can stop businesses from crumbling and keep private data in the right hands. In one study, researchers used a method based on identify-based broad encryption (IBBE) algorithm to create a detection method for Distributed Denial of Service (DDoS) attacks for industry IoT (IIoT). IIoT is like IoT and is an application of IoT in industrial production and manufacturing and can be seen in mining, agriculture, oil, gas, and other utilities (Sha et al., 2019). Common threats that occur against IoT is DDoS attacks that happen on the virtualization layer while vulnerability exploits happen in the device layer.

The IBBE algorithm was analyzed to see how well it protected components in their EscaperCOP (their detection method for attacks across the layers), detection library and control command library (Sha et al., 2019). Through a series of tests, the IBBE algorithm proved to be

effective with a good detection ratio. The scheme would detect illegal host-to-guest and guest-to-device controls and runs across three layers in the IIoT environment (Sha et al., 2019). In their experiment, guest-to-host DDoS attacks were discovered because of the Detection Libraries (DL) and by using the IBBE algorithm to encrypt the DL and the Control Command Library (CCL). Although this procedure sounds complicated, it is basically using encryption for the DL and CCL so only authorized devices can connect and this prevents DDoS attacks.

IoT's Lack of Security Impact

Like any cybersecurity breach, jobs, company's reputation and sometimes even lives are at risk. It is estimated by the Gartner research firm, that by 2024, 75% of top companies will go out of business for cyber-physical security (CSP) incidents particularly if they involve deaths (Seals, 2020b). Cyber-physical security (CSP) includes distributed systems like IoT along with operational technology (OT) that control physical systems. IoT usually acts as an entry way to operational technology. Particularly due to the new 5G expansion and innovations such as self-drive cars and remote surgery, it is predicted that companies will spend more money and focus less on security (Seals, 2020b). By 2023, fatal casualties will reach to more than $50 billion including costs of compensation due to loss-of-life, insurance, fines, and a tarnished reputation (Seals, 2020b). To combat this, security rules and regulations grow from the government (like from CISA) to hold CEOs accountable. It is recommended that companies do a risk assessment of their organization (list assets, rank their risk and probability of threats) and create a plan on how to move forward while keeping security in the fore front of their mind.

IoT Security Experiments

A popular defense system for networks, is called an Intrusion Detection System (IDS) which uses behavior analyses to alert the system administrator of any abnormal behavior. In one

study, computer scientists tried to implement something similar, but for alerting possible intrusions in IoT systems. They based their solution off the Distributed Network Protocol (DNP3) layers in the Supervisory Control and Data Acquisition (SCADA) systems (Yin et al., 2019). The current DNP3 method is a widely used network protocol for smart grid communication networks (such as IoT) and particularly in oil/gas, water utilities and wastewater technologies (Yin et al., 2019). Antivirus software for IoT devices will not work because antivirus uses pattern matching and matching files in the system with known malware (signatures).

So, they proposed an intrusion detection system based on the DNP3 protocol where an engine parses the packet format and then learns from the sample if the frame protocol has been compromised or not (Yin et al., 2019). By using four different types of attacks (modification, interception, interruption, and fabrication) their proposed method detected intrusions on the SCADA system based on an IoT smart grid and successfully classified them with detailed information about the compromised fields from the DNP3 packet (Yin et al., 2019). Their research showed that a key to stopping cyber-attacks in IoT systems, is to create something like an IDS that can alert system administrators alerted of possible attacks like an IDS.

Securing IoT Using Blockchain

Another technique to secure IoT systems is to take a chapter out of what is allowing secure transactions of cryptocurrencies and even some government networks, called blockchain and applying it to this smart device environment. The core of this blockchain system is simply a way that records each action (transactions) and spits out a unique value (the standard for Bitcoin is 256 bits long now) called a hash. Since a hash is one-way, it is impossible to reconstruct the original value from the given hash. The value associated with the hash could be of any length

(for example, the text of an entire book) and the hash would still be whatever standard it is set to (so in this case, 256 bits long). The hash produced would also be unique from any other hash created before or after itself. The formula is insanely complex, and it is constantly updating the hash with each edit made on the system. This technique called Proof of Work, is often used to show data has not been tampered with (like showing a laptop has not been touched since the crime scene for a court case). These hashes are called blocks and that is how the name blockchain came into being. With the growth of powerful computers, these blocks are created at a pace that puts hackers and even botnets (hijacked devices working together often without their owner's knowing) at a very low probability of solving the hash.

Now putting blockchain in a IoT system presents some challenges such as the high computing power needed that would slow down the entire network, additional hardware, and an increase in costs (Maelli et al., 2020). In an experiment, the proposed hybrid blockchain design called HyBloSe for IoT systems, has a secure-by-design blueprint and allowed for cloud-based logic which would eliminate the drawback of the resources (like time and speed) needed to create the hash for the Blochian (Maelli et al., 2020). In a procedure called Public Smart Building Contract (based off Delegated Proof of Authority [DPoA]) instead of Proof of Work, defines the function of each device in the system and in case of exploitation would restrict the access and movements of the hacker. DPoA changes the authority of which nodes can mine on an hourly basis (and does not choose the nodes that were working previously). If an attacker would hijack a node and then request for data when it is not that node's turn to mine, a security alert would be sent to all other nodes in the system.

This security procedure would mean for the nodes to create an entire new path of data travel (called a fork) excluding the suspicious node. Besides the security measures in place for

this system design, it is also energy efficient because only two nodes an hour is working so the energy consumption stays low. Also, in this blockchain theory for the IoT system, it also uses a combination of a Private Moving and public blockchain to ensure integrity and guarantee privacy. The private blockchain can only be created by the secure nodes by the Public Smart Building Contract and then periodically the same hash is written on public blocks and the old parts of the blockchain is then removed. This procedure satisfies privacy requirements because their data is only available temporarily and then erased. The blockchain is also only accessible by being inside the building (Maelli et al., 2020). HyBloSe tackles all security concerns in a way that requires low power and uses the blockchain technology for nodes to impersonate one another. Algorithms and quantitative research show that this HyBloSe system module is one of the best approaches for securing an IoT system.

IoT Devices Benefits

One new development that has come out due to smart devices, particularly speakers such as Alexa and Google, can help bring insight to legal cases. The first case where a smart speaker was analyzed was in 2016, was when a man was accused of murdering his wife and the police requested the transcript of conversations from the couple's Alexa via Amazon. At first Amazon refused, but finally released the data when the husband gave Amazon permission to give it to the police. This recording proved his innocence and the case labeled as an accident (Fussell, 2020). Since that case, IoT devices (besides cell phones) are the next thing police look for when examining a crime scene. Due this procedure now becoming protocol, police and other governmental agencies have templates now addressed to companies like Amazon and Alexa requesting data from these smart speakers. These requests are prioritized by the highest priority coming from Homeland Security and then divorce and civil cases are ranked low (Fussell, 2020).

IoT speakers can confirm or disprove a suspect's alibi especially if they live alone. In another case, police found drugs in a house with multiple residents. They got access to the logs, and by analyzing recent Google inquiries from voice recognition creating profiles, the police identified their suspect (Fussell, 2020). Not only is IoT devices changing convenience, but even the investigation of crime scenes and in court.

Future of IoT

Looking to the future, the possibilities of IoT systems are practically endless. Inventors look for any type of activity that can be automated such as public transportation or how goods are delivered. The topic of smart cities continues to grow as cities like Toronto implement their own Intelligent Transportation Systems Centre and developed a system called MARLIN-ATSC (Multi-Agent Reinforcement Learning for Integrated Network of Adaptative Traffic Signal Controllers) that improves traffic flow by using smart signals that process traffic information locally (Sharma et al., 2019). These smart signals controlled by the MARLIN-ATSC system, were installed at sixty downtown intersections at rush hour and reduced delays by forty percent and cut travel times by 26% (Sharma et al., 2019). Similarly, Singapore adopted an IoT Intelligent Transport Strategy (IoT-ITS) that increased the average car speed to seventeen miles-per-hour compared to the average car speed in London at ten miles-per-hour (Sharma et al., 2019). An intelligent IoT-ITS can also help emergency and government services respond quickly to accidents and for them to have a citywide visibility to avoid congested areas.

Some futuristic opportunities that ITS technology could possibly give is to adjust speed limits and signal timing based on its surroundings, guide drivers to empty parking space by using smart signs, make public transportation convenient and reliable and monitor structural integrity of buildings and bridges (Sharma et al., 2019). The possibilities of IoT-ITS and smart cities are

endless and will likely become a reality soon. With these new possibilities also comes the high priority of security and organizing and analyzing big data for it to be helpful.

Conclusion

The IoT has brought more range on what technology can do and it continues to grow. Individuals save time by asking their smart device to do small and repetitive tasks that they would otherwise need do themselves. Extra security measures such as the blockchain method or putting them on their own virtual local area network (VLAN) can keep data in its three stages (in transit, rest and in use) more secure. To increase security readability and understanding, the government should create a security standard that IoT manufacturers must uphold when it comes to their products. All this information combined, can help consumers make the best purchase that fits their needs. If it is a business, a risk assessment of the company's infrastructure and assets will show if it is worth the implementation of IoT products. Technology is constantly changing, and consumers and system administrators need an idea the level of risk and security they are receiving from a device or service. Future research in this area could look like exploring and testing new ways of using blockchain or other ways to reduce latency of data transmitting or encryption can drastically impact the future of securing IoT devices. Ultimately, the challenge of securing IoT is between the priorities of doing their task and taking time for encryption and decryption. If someone were to find a fast and easily implemented solution, IoT would be a more secure infrastructure.

References

Alani, M. M. (2018). IoT lotto: Utilizing IoT devices in brute-force attacks, *Association for Computing Machinery*, 140-144. https://doi.org/10.1145/3301551.3301606

Bu, L., Isakov, M., & Kinsy, M. A. (2019). A secure and robust scheme for sharing confidential information in IoT systems. *Ad Hoc Networks, 92*, https://doi.org/10.1016/j.adhoc.2018.09.007

Fussell, S. (2020, August 23). Meet the star witness: Your speaker. *Wired.* https://www.wired.com/story/star-witness-your-smart-speaker/

Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., Rahman, A. U., & Najmus Saqib, M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. *International Journal of Communication Systems, 32*(16), https://doi.org/10.1002/dac.4139

Giaretta, A., Dragoni, N., & Massacci, F. (2019). IoT security configurability with security-by-contract. *Sensors, 19*(19), https://doi.org/10.3390/s19194121

Harper, A. A. (2016). *The impact of consumer security awareness on adopting the internet of things: A correlational study* (Publication No. 10196140) [Doctoral dissertation, Capella University]. ProQuest Dissertations and Thesis Global.

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PloS One, 15*(1), https://doi.org/10.1371/journal.pone.0227800

Lee, R. P., Markantonakis, K., Akram, R. N. (2019). Ensuring secure application execution and platform-specific execution in embedded devices, *ACM Transactions on Embedded Computing Systems, 18*(26). https://doi.org/10.1145/3284361

Maselli, G., Piva, M., & Restuccia, F. (2020). HyBloSe: Hybrid blockchain for secure-by-design smart environments, *CryBlock '20: Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 23-28. https://doi.org/10.1145/3410699.3413793

Montalbano, E. (2020, September 16). Bluetooth spoofing bug affects billions of IoT devices, *Threat Post*. https://threatpost.com/bluetooth-spoofing-bug-iot-devices/159291/

O'Donnell, Lindsey. (2020a, July 10). Smartwatch hack could trick dementia patients into overdosing, *Threat Post*. https://threatpost.com/smartwatch-hack-could-trick-dementia-patients-into-overdosing/157352/

O'Donnell, Lindsey. (2020b, August 19). Researchers warn of flaw affecting millions of IoT devices, *Threat Post*. https://threatpost.com/flaw-affecting-millions-iot-devices/158472/

Romano, N. (2019) *Securing Our Future Homes: Smart Home Security Issues and Solutions*. (Publication No. 864) [Senior Honors Theses, Liberty University]. Scholars Crossing: The Institutional Repository of Liberty University.

Seals, T. (2020a, June 16). 'Ripple20' bugs impact hundreds of millions of connected devices, *Threat Post*. https://threatpost.com/millions-connected-devices-ripple20-bugs/156599/

Seals, T. (2020b, September 7). CEOs could be held personally liable for cyberattacks that kill, *Threat Post*. https://threatpost.com/ceos-personally-liable-cyberattacks-kill/158990/

Seals, T. (2020c, September 17). Mozi botnet accounts for majority of IoT traffic, *Threat Post*. https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/?utm_source=cybermap&utm_medium=sm-project&utm_campaign=news-block

Sha, L., Xiao, F., Huang, H., Chen, Y., & Wang, R. (2019). Catching escapers: A detection method for advanced persistent escapers in industry internet of things based on identity-based broadcast encryption (IBBE), *ACM Transactions on Embedded Computing Systems, 18*(29). https://doi.org/10.1145/3319615

Sharma, N., Shamkuwar, M., Singh, I., Balas, V., Solanki, V., Kumar, R., & Khari, M. (2019). The History, Present and Future with IoT, *Internet of things and big data analytics for smart generation, 154*. Springer. https://doi.org/10.1007/978-3-030-04203-5_3

Spring, T. (2020, August 25). Four more bugs patched in Microsoft's Azure sphere IoT platform. *Threat Post*. https://threatpost.com/four-more-bugs-patched-in-microsofts-azure-sphere-iot-platform/158643/

Weiqiang, L., Zhang, L., Zhengran, Z., Gu, C., Wang, C., O'Neill, M., & Lombardi, F. (2019). XOR-based low-cost reconfigurable PUFs for IoT security, *ACM Transactions on Embedded Computing Systems, 18*(25). https://doi.org/10.1145/3274666

Yin, X., Liu, Z., Nkenyereye, L., & Ndibanje, B. (2019). Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. *Sensors, 19*(22). https://doi.org/10.3390/s19224952

Zhou, L., Su, C., Hu, Z., Lee, S., & Seo, H. (2019). Lightweight implementations of NIST P-256 and SM2 ECC on 8-bit resource-constraint embedded device, *ACM Transactions on Embedded Computing Systems, 18*(23). https://doi.org/10.1145/3236010

Zurkus, K. (2019, January 14). Can Smart Home Leaks Lead to Major Cyberattacks? *Security Boulevard*. https://securityboulevard.com/2019/01/can-smart-home-leaks-lead-to-major-cyberattacks/