Victoria Ellsworth
Dr. Ping Li
ICTN 4040
04/11/17

Internet of Things (IoT) Attacks

The Internet of Things (IoT) is based off a larger concept; the Internet of Things came from idea of the Internet of Everything. The Internet of Everything (IoE) is the idea of bringing together people, process data and things. The Internet of Everything is important because it allows us to make network connections between things that were never possible, creating a more enriching, relevant and new opportunities. The Internet of Things has allowed us to provide more physical objects connected to the internet. The growth in IoT technologies in such a short amount of time is significant and will be an important factor in knowing how to protect an organization, community and your own personal data. Understanding reasoning for IoT attacks and the preliminary measures needed protect asset will give you a better understanding and knowledge in the growing world of technology.

It is now possible for any object to be connected together or connected the internet; this statement is something that one might not think was possible 5 years ago. Now, it is becoming a reality with the how IoT has been advancing these past years. IoT devices have created a way for a computer to eliminate human interaction, but keeping the world connected. However, this has caused the issue of security technologies not being able to keep up the new ideas and material that are presented. Machine-to-Machine (M2M) is the basis of The Internet of Things in allowing devices to communicate with one another. The things that surround us are imbedded with sensors; that stores and carries valuable data. The data that is produced from these devices is what creates the common Internet of Things platform that brings all the diverse information together and creates a language for these different devices to communicate with each other. IoT devices gives us real time interaction and services through applications that we are seeing today

with our cars, in our homes and at our jobs. A simple example of an IoT device is a smart car. Now you can buy a car where from an application you can change things like the lights inside the car, check the battery, view the speed and location of the car. These are all features that have different sensors inside the object and then carry the information to the application for us to use.

According to a study done by Aruba determined that 85 percent of businesses plans to implement Internet of Things by 2019. This has created new security threats and risk, granting more vulnerabilities within organizations though. The major security breaches that have been seen with the rise of Internet of Things are external attacks like software attacks like malware or spyware. However, we will discuss some other types of cyber-attacks that have been encountered with IoT devices. Many have said from the introduction of IoT devices that proper security for these devices from the manufacturers have been absent. There are very few standards to govern how to secure IoT devices inside a network. You would think something simple like changing default passwords would be an easy solution from preventing a major attack. The lack of poor security implementation plans within organizations have led to potential attacks. “Now security firms and manufacturers are joining ranks to help secure the IoT world before it spins out of control “ (Dickson pg 2). An example of cyber-attack involving IoT devices was on the website Krebsonsecurity.com when it was hit with a distributed denial-of-service, (DDoS) attack in September of 2016. To summarize the attack; a typical DDoS attack attempts to make an online service unavailable by flooding systems with traffic. The incoming traffic can be pin pointed most of the time to one specific region; this particular attacked seems to be everywhere. The attack had hacked multiple Internet of Things device like routers, IP devices and more that were connected to the internet with weak passwords. This specific type of botnet was ran by malware and spread to new host looking for vulnerabilities. The malware was able to scan the

internet for vulnerable Internet of Things devices that were protected by factory default username and password of the devices. As risk like this arise, manufacturer have taken notice but it has not necessarily easier on the user. The manufacturers increase the complexity of the passwords, but it has become harder for the users to come up with a stronger password. Due to IoT devices having little standards it has put a negative effect on the users side leaving them possibly exposed.

DDoS attacks are just one of the many types of security attack, these types of attacks are going to grow in scale and complexity as The Internet of Things grows. Organizations who plan to implement IoT into their business have to come up with strategies and identify motives and capabilities of these attackers. Attackers have found that these devices are the perfect way to perform an attack. As the security risks arise, methodologies need to be formed to be aware, identify and find solutions. As organization are adopting Internet of Things technologies, it is adding value to the data. Abomhara and Koien list the reasons devices are valuable to attackers "most of the Internet of Thing devices are not attended to by humans creating physical access, the components communicate wirelessly making it easier to eavesdrop and the Internet of Things cannot support complex security schemes due to low power and computing capabilities."

The data that is collected from these devices raises a large concern, how is this data being used and by who? As this large pool of data expands increasing traffic visibility will be important because with new devices come new locations. In the attack of krebs on security site, it was first assumed that the traffic flowing was from a generic routing encapsulation (GRE) packet from a point-to-point link that they knew did not share data over the public network. Organizations need to identify that this can be done with basic elements of security like filtering and authentication. The problem is keeping the authentication and access easy but is needed to establish a secure

connection between the devices and the service it is providing. Another way to limit access is by cutting down on the number of endpoints or users because having too many endpoints or user can lead to a vulnerability. It has seems like organizations end up with more than they can manage that they can no longer maintain to apply simple security settings. Creating security patches like VPN and APNS can stop a man-in-the-middle (MITM) attack. MITM attacks are harder to detect due to the malicious attacker is between the two parties, gaining access to unauthorized data. The parties do not realize that they are not communicating with the correct party. Luckily using VPN allows you to send and receive data on a public network but as if you were on a private network with all the security features, so even if data were intercepted it would be encrypted.

The biggest problem used to be to how to get devices connected but that is no longer the issue. We now have devices like refrigerators or vending machines connected to the internet but are not built the same way computers and laptops are built with security features. The Internet of Thing's network architecture consisting of the sensor, network and application layers they are not equipped yet to protect data. It is now the consumer's job to take preventative actions to protect any assets. A physical attack targets the hardware of the device, which could be the sensor in the device that carries the data. As it was mentioned before because IoT devices have eliminated the need for human operation this opened the opportunity for unauthorized access to be established. Physical attacks can involve malicious code injected into the sensors node. Another simple solution to protecting yourself is turning off devices that are not in use to be proactive towards potential threats. Universal Plug and Play (UPnP) is a technology that is featured on some IoT devices; which is typically connected through the router leaving the network vulnerable due to it leaving a virtual port open. These devices are new to our networks,

which has caused us not to view them as a threat. As The Internet of Things and RFID have developed together, spoofing or cloning has become a threat to the Internet of Things architecture simply by gaining access from copying or impersonating an RFID signal. Software attacks are one of the most common types of security attacks. Specifically a malicious software that is designed to attack IoT technologies until you pay up the ransom has created Ransomware of Things. This happened early this year in Austria where hijackers compromised the electronic key system and the computers at hotel. This caused guest to not be able to access their rooms and the hotel having to pay the attackers to hand back over them system. The lesson learned from this particular attack was that attackers are willing to attack everyone and anyone even in compromising more in numbers.

These are just the current findings of how to protect the data privacy and prevent any possible security risk from reaching an organization's asset. The idea of an object connected to the internet benefits outweigh the risks right now. IoT is still new to the information security world. The consumers have to be look for the flaws of this new technology to reduce threats and gain more knowledge of how to take the next step to stop the cyber-crimes and attacks so can take full advantage of what Internet of Things has to offer. I hope that this has given a basic understanding of what The Internet of Things is and more knowledge of IoT devices being risks and potential threats that can be encountered.

References

Abomhara, Mohamed, and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." *Journal of Cyber Security and Mobility* 4.1 (2015): 65-88. Web. *

Gigli, Matthew, and Simon Koo. "Internet of Things: Services and Applications Categorization." *Advances in Internet of Things* 01.02 (2011): 27-31. Web. <http://file.scirp.org/pdf/AIT20110200005_90413785.pdf>. *

Krebs, Brian. "Krebs on Security." *Brian Krebs*. N.p., n.d. Web. 11 Apr. 2017.

Journal, IOT. "Hackers Used the IoT to Create an Unprecedented DDoS Attack-Now What?" *Hackers Used the IoT to Create an Unprecedented DDoS Attack-Now What? - IOT Journal*. IoT Journal, n.d. Web. 11 Apr. 2017.

Journal, IOT. "New Study Examines Mass Adoption of IoT Technology." *New Study Examines Mass Adoption of IoT Technology - IOT Journal*. IoT Journal, n.d. Web. 11 Apr. 2017.

Dickson, Ben. "Why IoT Security Is So Critical." *TechCrunch*. TechCrunch, 24 Oct. 2015. Web. 11 Apr. 2017.