The Security of IoT Devices

Courtney D. Spencer

Old Dominion University

Table of Contents

Abstract

The security of IoT devices is an important topic to discuss due to the significant presence of technology. IoT devices are everywhere you look from the car you drive to the refrigerator that you buy. These devices are always advertised to make the users life easier but the companies producing the technology are not informing the users about the security features behind it. How is the company protecting the privacy of the user? How likely is it for someone's device to be hacked? What can the average person do to further protect themselves. Cybersecurity professionals everywhere are interested in how the security on IoT devices work, it allows them to be informed and up to date on the latest technology. Knowing how these devices work will allow professional to in the field to put more security features in place to protect the user.

Keywords: IoT devices, Cyber-attacks, Network Layer, Application Layer, Privacy

The Security of IoT Devices

The trend in today's society is, easy. What can be done to make one's life easier? People are moving away from complicated, busy, and always on the go. Today, people want to enjoy the time they have with their friends, their loved ones, and make memories that are meant to last a lifetime. Now it is not a rare sight to see a twenty-three year old woman going to Italy with friends and having the time of her life. The younger portion of the population definitely has a different outlook on the world and how people should live in it. If it is not ultimately going to improve his/her life and make things easier, then it is seen as pointless and unnecessary. The world of technology has caught onto these new feelings towards life and made all the necessary adjustments. There are cars that drive for you, cameras that follow your movements so you no longer need to hold the phone, and even a toaster that can sense what you put in it and cook it based on what it is. Now, you do not need to open your refrigerator to see what is inside. Instead you perform a simple gesture like waving your hand in front of the transparent screen, the refrigerator then comes alive in a sense and allows for you to see what you have and what you need. Does this make life easier? It cuts out the need to physical take the time to open and close the door. It is therefore taking out at least one step in checking what you need for that last minute grocery store run. These touches are amazing to some and unnecessary to others however, both parties should be knowledgeable of the security features and risks that comes with having one in your household. If an individual goes forward in the decision to own a IoT device it is important to have a general understanding of the architectural features involved, the different attacks that can take place within the different layers, the type of privacy breaches that has occurred thus far and how various methods can help users in protecting themselves.

Architectural Features

Internet of things or IoT technology focuses on the inter-connection between humans and other devices to solve common goals and problems. Much like people IoT devices work best with other compatible devices and create a seamless form of communication from the physical world to the internet. The phrase IoT was thought of by Kevin Ashton from the Auto ID-center at the Massachusetts Institute of Technology. In an interview he had with the Smithsonian magazine he describes the concept as, "computers were brains without senses- they only knew what we told them". In this thought He goes on to point out the limitation that were faced due to the fact that there is a gap in the amount of information in the world to the amount of information that a person could type using a keyboard of even scan with a barcode. In the interview he makes a note of how much something as simple as a global positioning system (gps) is often largely underappreciated, yet depended on by so many and is arguably the sole source on directions. Because of the interaction between IoT devices and humans, the technology has captured the attention of researchers around the world. Computers are now able to not only sense various physical characteristics but process them and store the information on remote clouds. This plays a significant part in creating smart homes and even smart cities. To accomplish such an integration the Internet of Things technology has to not only earn the users trust but also continue to prove itself worthy of keeping it by maintaining a sense of confidentiality, integrity and availability as seen in the CIA triad as it pertains to security goals. As with anything associated with the internet, the possibility of a cyber-attack taking place is nothing new and understanding the architecture of Internet of Things Technology will help in understanding how various attacks are performed. The IoT model is made up of four main layers and although not all devices will follow the exact framework discussed, most will utilize the following and therefore can be a

bass reference when referencing different attacks. The four layers are the perceptual layer, the network layer, the support layer, and the application layer.

In the first layer, the perceptual layer, we see devices such as Bluetooth, and many different types of sensors. Sensors are suitable for sense physical conditions like weather conditions, sea levels, etc. In this layer we also see sensors like Radio Frequency Identification commonly referred to as RFID which is used to aid machines and computers in identifying objects, record metadata or control individual target through radio waves. You can see this type of technology places like hospitals where trackers are used on patients, staff, laundry, and inventory. In the Network layer, also known as the second layer in this model, information gathered using the perceptual layer and then transmitted to the main cloud fog nodes or another Internet of Things node. This is the layer where we see communication protocols, satellite network, internet, and mobile networks. Following the network layer, the support layer is then used to provide a platform for IoT applications. The application layer is the last layer for the sake of this model and provides IoT services to users for their specific needs, The interface can be utilized in different services like a smart healthcare systems, smart homes, vehicles, and much more. With the increasing of accepted IoT devices there are a number of cyber related attacks that should be noted. When you are aware of the risks that come with owning IoT devices you can appropriately choose what safety measures you choose moving forward.

Attacks by layer

In each of the four layers that were previously discussed there are plethora of attacks that can be performed, In the Perceptual layer an attacker can perform attacks like node tampering, side channel attacks, malicious code injections, Mass node authentication, and even physical damage. In node tampering the attacker can have their own physical access to sensor nodes and

go on to replace the full node or even part of the hardware. In performing this action he/she can cause for the altercation of sensitive data to gain access to the node. Side channel attacks can be carried out when an attacker information from sensor nodes like power consumption, and electromagnetic radiation to attack encryption mechanisms. Malicious cod injection can be carried out by simply taking a piece of malicious code and inserting it into a node that will now give him/her unauthorized access to the system of their choice. Physical damage is likely to occur in an internet of things device with attacks like denial of service. In the network layer security we see challenges such as heterogeneity problems, network congestion, RFIDs interferences, eaves dropping attacks, and sybil attacks. When a large number of devices are trying to preform authentication measures, it cause an overwhelming amount of sensor data to be processed and causes network congestion. An RFID interference attack can be accomplished on the network layer by corrupting radio frequency signals with noise signals also cause a denial of service attack. Eavesdropping occurs when there is traffic sniffing in a wireless area. Much like packet sniffers the attacks goal is to gather information on the network using some type of sniffing tool. In a sybil attack a malicious node acts like the other nodes and then continues to distribute distorted routing information. The support layer deals with things like data security, interoperability, and visualization security. This layer plays a crucial role in ensuring the data stays confidential and secure as long as its in the cloud. Using a variety of different tools we can detect data migration from the cloud and file and database activity. Interoperability and portability is a problem that cloud vendors are facing for users who want to migrate from one cloud to the next. In virtualization security the techniques used vary with different cloud vendors and is very important in cloud audits. In the application layer we see more of the human factors being targeted in attacks like phishing, data access and authentication and different type of

malware attacks. Phishing attacks involve using infected emails or web links to steal user credentials and with that gaining access to their systems. With all the attacks that can be performed at each of these layer it is equally important that not all the attacks mentioned will have catastrophic results. They all vary in impact levels from low to high and should be considered when looking at which attack is being carried out. Below is a table illustrating a few attacks and their corresponding impact levels.

Table 1

IoT Attacks and Impact

Attacks	Impact
Node Tampering	High
Fake node	High
Side channel attack	Medium
Physical damage	Medium
Malicious code injection	High
Protecting sensor data	Medium
Mass node authentication	High
Heterogeneity problem	High
Network congestion problems	Medium
RFIDs Interference	Low
Node jamming in WSN	Low
Eavesdropping attack	low
Denial of service	High
RFID spoofing	High
Routing attacks	High
Sybil Attack	High
Data Security	High
Interoperability and portability	Medium
Business continuity and disaster recovery	Medium
Cloud audit	Medium
Tenants security	High
Virtualization security	Medium
Data access and authentication	High
Phishing attacks	Medium
Malicious active X scripts	High
Malware attack	High

Note. Data for the IoT Attacks and Impact is from the International Journal of Computer Science and Information security (IJCSIS)

Privacy Concerns. The saying that "Ignorance is bliss" is one that is repeated time and time again yet to this day still holds true. The saying goes to say that the more you know the more responsibility you tend to have and the saying holds true even when it comes to internet of things devices. In the world of cyber security the more knowledgeable on how certain attacks are performed and the number of vulnerabilities that are exposed, the more you try to create a secure environment for not only you but your loved ones and anyone else who you may have on your personal networks. The problem is that IoT devices are not solely for cybersecurity professionals who have the knowledge and capability to take something that may not be the most secure and turn it into something that is safe enough to hold sensitive information. With user unawareness, improper device updates and a lack of efficient security protocols, privacy is a significant challenge that internet of things devices are faced with.

Each time an IoT device comes out to the public, it as advertised as simply, easy, and more important trustworthy. Now, when consumers are beginning to use their new devices wether that be for their own personal enjoyment such as in the home or for professional use they are required to trust the not only the devise but the services as well. They are have to trust that the IoT device they have are going to only do what it is made for and nothing else. They have to trust that there are no vulnerabilities, and the company is staying up to date on all attacks that could potentially come their way. Consumers are required to trust that the corporation producing the Internet of Things technology care about the protection of the user's privacy just as much as the user does. The harsh reality is that many devices in the Internet of Things are designed to be produced on a large scale and because of all the similar characteristics between devices, it magnifies the magnitude of any vulnerability. This also happens to be one of the main reasons

why there is so much hesitation on the full adoption and integration of Internet of Things technology.

Privacy Breaches. Users are not wrong in the concerns they voice when society attempts time and time again to make a push for the full integration of IoT devices. On December 4, 2019 a ring camera that was placed in eight-year-old Alyssa's room was hacked and used in a malicious way. The hacker tried to coerced the little girl into performing destructive actions like "mess up her room" and "break her tv. Thankful the little girl went to get the help of a trusted adult and the situation was handled by her parents. The Washington Post covered this incident and also makes note that this was not the first time Ring users have had an incident similar to Alyssa's occur. Many parents including Alyssa's are using the Ring camera as well as many others to be able to keep an eye on their children when they are not physically in their presence. The incident shocked parents across the world, and unfortunately if the story has not pushed the company to do more in regards to security features in their products another incident similar to Alyssa's can happen again.

While not privacy breaches have such negative outcomes, the fact is that there is a privacy none the less. In Arkansas v. Bates the police were investigating a murder case and trying to gather evidence as to what happened the night Victor Collins died. The defendant James Bates owned an Amazon Alexa Echo in the kitchen and the police were able seize the device along with his phone and file a preservation request from Amazon. When the defendant gave the manufacturer permission to turn over any audio recordings they were then able to gather evidence from the Echo Dot and use it as evidence in the murder case.

The cases do not have to include audio messages to be used in gathering information. In a different murder case right before Christmas in 2015, a women, Connie Dabate was shot in her

basement by her husband, Richard Dabate in Ellington Connecticut. The witness was something that the husband looked over as being an important piece of evidence in his own murder case, a Fitbit exercise tracker. The tracker is worn on the wrist monitors from things like the person's heartrate, to their sleep schedules, their locations and distances, and everything in between. What it wasn't meant to do was be factored into criminal encounters. The husband tried to tell police his wife died in a tragic home invasion after his wife returned home no later than 9 am. He then goes on to say that the intruder shot his wife and left after leaving him tied up and unable to move. However after searching Connie's fitness tracker the data proved that his wife was still moving around the house between 9:18am and 10:05am. After looking into the case more the police discovered the husband was having an affair and wanted get the money from his wife's life insurance policy. Richard was charged with Murder and the Fitbit played a vital role in getting justice for Connie Dabate.

Internet of Things technologies can vary depending on what they are being used for and many people tend not to realize just how many things are connected to the internet and are considered to be IoT devices. In this day age there are the obvious ones like phones and Echo Dot's but there are less noticeable ones like biometric identifiers and even pacemakers. In Middletown, Ohio a fifty-nine year old man, Ross Compton was charged with aggravated arson and insurance fraud after he discovered a fire in his house. Compton claimed that he gathered a few of his things and escape through a window that he broke with a cane. He claims that the fire wasn't started by him but police came to a different conclusion. From looking and the heart monitor he had a cardiologist reviewed his heart rate and cardiac rhythms and stated that is was "highly improbable" that a person with Ross's condition could gather the items and escape in

such a short period of time. In addition to the findings that the cardiologists discovered from his pace maker, the police also said they found gasoline on Compton's shoes and articles of clothing.

In all of the cases previously mention whether the results were good or bad resulted in some type of privacy concerns being raised. It is argued that many internet of things devices, not exclusively the ones that have been discussed, present first and fourth amendment issues and privacy rights. According to the constitution:

> "The First Amendment provides that congress make no law respecting an establishment of religion or prohibiting its free exercise. It protects freedom of speech, and press, assembly, and the right to petition the government for a redress of grievances," And "the Fourth Amendment protects citizens from unreasonable search and seizure. The government may not conduct any searches without a warrant, and such warrants must be issued by a judge and based on probable cause."

In the cases and many more people are questioning what exactly constitutes as privacy and what exactly are they signing up for when all they are trying to accomplish is an easier, more convenient, and safer form of life.

Methods to help protect the user. With internet enabling devices becoming such a target for cybercriminals, how can users expect their information to be protected moving forward? Internet of Things technology has brought researchers from around the world together to try and find various ways to deter attacks and keep consumers sensitive data secure. Some say that deploying different encryption techniques could be a way to deter attacks. Continuously enforcing strong and updates encryption techniques in both the cloud and regular device environments. This would allow for the data in the cloud or device to be unreadable by the attacker. Other mitigation techniques rely on the user as well as the manufactures. This involves

the increasing the amount of updates that are pushed to the products. In doing this, the hope is not take some of the known vulnerabilities and help bridge that gap. Instead of huge updates that are few in between, sending smaller patch updates at a more frequent pace.

Conclusion. The future of Internet of Things devices is promising in the hopes that manufactures along with consumers will both do their part in creating a safe and secure environment. The reality is that there will always be an individual with malicious intentions trying time and time again to steal whatever sensitive information is available. It is our job as cyber professionals, as individuals that care about the safety and privacy of our loved ones, and simply as decent human being to continue leaning and developing our new technology in a way that makes life easier without sacrificing privacy and security. It is a fight that will more than likely continue until the end of time as most good vs evil battles tend to do. If an individual goes forward in the decision to own a IoT device it is important to have a general understanding of the architectural features involved, the different attacks that can take place within the different layers, the type of privacy breaches that has occurred thus far and how various methods can help users in protecting themselves. Cars will be smart, houses will be smart, the way we do healthcare will be smart, cities will be smart, it is up to us as “white hat” citizens to be smarter.

References

State of Arkansas v. James A Bates (Circuit Courts of Benton County February 17, 2017).

X. Jia, Q. Feng, T. Fan and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 1282-1285, doi: 10.1109/CECNet.2012.6201508.

Li, Shancang, Song, Houbing, & Iqbal, Muddesar. (2019). Privacy and Security for Resource-Constrained IoT Devices and Networks: Research Challenges and Opportunities. Sensors (Basel, Switzerland), 19(8), 1935.

IoT device hacking risk exposed. (2014). Electronics Weekly, (2581), 7.

Køien, G. (2016). A privacy enhanced device access protocol for an IoT context. Security and Communication Networks, 9(5), 440-450.

Ali, I., Sabir, S., & Ullah, Z. (n.d.). Internet of Things Security, Device Authentication and Access Control: A Review. *International Journal of Computer Science and Information Security (IJCSIS),14*(8).

Branscombe, M. (2020, February 11). IoT security is bad. It's time to take a different approach. Retrieved from https://www.zdnet.com/article/iot-security-is-bad-its-time-to-take-a-different-approach/

Chiu, A. (2019, December 13). She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter. Retrieved from https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/

Gabbai, A. (2015, January 01). Kevin Ashton Describes "the Internet of Things". Retrieved from https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

George Khoury, E. (2019, March 21). IoT Kids' Toys Privacy Breach Case Settles. Retrieved from https://blogs.findlaw.com/technologist/2018/01/iot-kids-toys-privacy-breach-case-settles.html

Hauser, C. (2017, April 27). In Connecticut Murder Case, a Fitbit Is a Silent Witness. Retrieved from https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html

Johnson, K. (2017, October 08). Middletown man's electronic heart monitor leads to his arrest. Retrieved from https://www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942

Zatz, C. J., Aradi, L., & Mathis, P. (2017, July 10). Recent IoT Device Cases. Retrieved from https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/

Footnotes

Tables

Table 1

IoT Attacks and Impact

Attacks	**Impact**
Node Tampering	High
Fake node	High
Side channel attack	Medium
Physical damage	Medium
Malicious code injection	High
Protecting sensor data	Medium
Mass node authentication	High
Heterogeneity problem	High
Network congestion problems	Medium
RFIDs Interference	Low
Node jamming in WSN	Low
Eavesdropping attack	low
Denial of service	High
RFID spoofing	High
Routing attacks	High
Sybil Attack	High
Data Security	High
Interoperability and portability	Medium
Business continuity and disaster recovery	Medium
Cloud audit	Medium
Tenants security	High
Virtualization security	Medium
Data access and authentication	High
Phishing attacks	Medium
Malicious active X scripts	High
Malware attack	High

Note: Data for the IoT Attacks and Impact is from the International Journal of Computer Science and Information security (IJCSIS)