Security Concerns within IoT

Elita Danilyuk
Dept. of Computer Science
Colorado State University
Fort Collins, United States
elita@colostate.edu

Zachary Lowe
Dept. of Computer Science
Colorado State University
Fort Collins, United States
zachary.lowe@colostate.edu

Tyson O'Leary
Dept. of Computer Science
Colorado State University
Fort Collins, United States
tyson.oleary@colostate.edu

***Abstract*—The consumer use of the internet of things has grown to such a large scale that most people interact with it daily. As the number of devices grows, so too does the volume of security issues and privacy concerns. It has spread from smart refrigerators, thermostats, phones, vehicles, sensors, and a vast amount of other consumer goods and products. Most devices within our grasp have been unified, which has led to a great deal of personal control as well as an abundant amount of individual and group data. With how closely these "things" are communicating with one another, it is important to understand the risks and rewards of how the data is being shared, whether it is public or private, and how secure it truly is. It is important to understand the state of the art of internet of things security in order to continue its improvement, as the security of the devices in a user's home should be taken seriously. This report will introduce the internet of things and explain why its security is important based on logic and ethics. Specific security issues that are relevant right now will be explained to give context of the current state of the art. Then, real attacks on these flaws will be described, using Amazon Alexa and smart TVs for example. After analyzing the flaws, we will present some possible solutions and security improvements, as well as give some predictions for the future of the security of the internet of things.**

Keywords—IoT, Internet of Things, Security, Data, Malware, Privacy, Embedded Software, Surveillance, Smart Devices, RFID

I. Introduction

The IoT is the general term for how the internet has, and is, connecting various "things," both object-to-object and person-to-object communications. It can more broadly be defined as the interconnected network of various physical objects which are enabled to send and receive data. The initial popularization of IoT began in the late 1990s and early 2000s. It was popularized by the idea of connecting home appliances to the internet. The term itself was first popularized by Kevin Aston. In 1999, Aston was the executive director of the Auto-ID center at Procter and Gamble [1]. Aston made the term the title of a presentation that linked the idea of Radio Frequency Identification (RFID) devices within P&G's supply chain. In the same year, Neil Gershenfield spoke about the principles of the IoT in his book When Things Start to Think [2]. The following year, 2000, LG announced the plans for the first Internet refrigerator. For the next few years, several more devices with RFID chips began development. The development of these devices quickly expanded to everyday consumers.

The consumer use of the IoT has grown to such a large scale that most people interact with it daily. It has spread from smart refrigerators, thermostats, phones, vehicles, sensors, and a vast amount of other consumer goods and products [3].

"Fig. 1", The IoT has transformed how people interact, live, and communicate with various devices. It has unified almost all devices within our grasp, which has led to a great deal of personal control, as well as an abundant amount of individual and group data. There were over 10 billion active devices in the IoT in 2021 and it is estimated that, "there will be 152,200 IoT devices connecting to the internet per minute," by 2025 [4]. With the increased number of devices connecting to the internet, by 2025, the data generated is expected to reach 73.1 zettabytes [4].

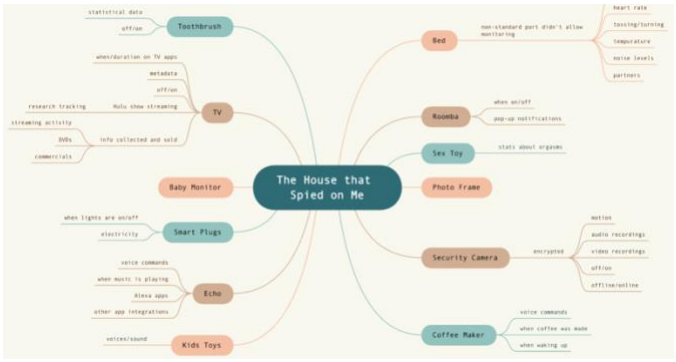

Fig. 1. This image is an example of the complex web of connectivity that the Internet of Things creates.

As the IoT continues to grow at such a large scale, a concern for security and surveillance has erupted. Another significant concern of the integration and exponential growth of the IoT is that the data that is being collected may be closely related to people as well as their daily activities and the increased relationships between the 'digital' and 'real' worlds [5]. The vast amount of data that is being generated and shared between devices create ethical concerns regarding the collection and use of data. Thus, new legal and development policies and challenges continue to appear.

A great example of ethical and security concerns around the growth of the IoT can be seen through what happened with Edward Snowden. Snowden worked for the Central Intelligence Agency (CIA) for three years before going to the National Security Agency (NSA) as an intelligence contractor. While working at the NSA, Snowden began to collect information on a secret surveillance program that the NSA was conducting. Snowden would eventually take a medical leave of absence,

leave the US, then whistle blow on the surveillance that the NSA was conducting. Snowden released information that the government agency was collecting mass information through telephone records. This information was gathered through of the ease and accessibility of records and information through the IoT. The government's decision and action to mass surveillance its citizens shows a lack of privacy, security, and legislation surrounding the ever growing IoT. This is just one well publicized event that shows the importance of how mass surveillance, rights, and privacy are a challenge through the IoT.

As these challenges continue to emerge, it is clear that the IoT has become a complex and intertwined web of network connections. With regards to how closely these "things" are communicating with one another, it is important to understand the risks and rewards of how the data is being shared, whether it is public or private, and how secure it truly is. Some key topics and information this paper will discuss will be related to current issues such as surveillance, malware, IoT attack surfaces, and universal standards. This paper will also go into detail about various devices security concerns and potential improvements that could be made to make the IoT more private and secure.

II. Current Issues and Approach Limitations

In relation to other technologies, the Internet of Things is still in its infancy. Because it is a new and emerging technology, under constant development and growth, there are several areas that present potential security risks that have not yet been resolved. Internet of Things technology is currently being used in a wide range of places, from our homes and vehicles to city infrastructure, healthcare, and within manufacturing. All of these different areas of application carry with them their own set of security needs. However, there is some common thread between them regarding certain areas of security. Backdoor vulnerabilities, shadow devices, malware, and the absence of a widely adopted security standard are all examples of current areas of issue. Given the large potential attack surface that IoT presents, these are all areas that will need significant improvement.

A. Surveillance/Backdoor

Many IoT devices used within industry today exist in the form of sensors, actuators, and cameras. These do not traditionally contain user facing operating systems and are very simple in terms of their design. Their security and communications can be equally simple, which presents a major security vulnerability. On the other hand, within the consumer sector we see IoT driven doorbells, fire and alarm systems, ovens, and other appliances. These types of devices operate over more common communication channels such as Bluetooth and Wi-Fi, however brand compatibility becomes the limiting factor with regard to how compatible these devices are to one another. Many of these such devices have manufacturer backdoors that are not typically accessible to the end user. Because they are generally tethered and controlled through a smartphone or computer they are only as secure as the device which has access to them [6]. For example, someone with malicious intent could potentially gain access to a user's home camera through remote access to their phone or computer. The manufacturers themselves are also able to perform data collection on use habits to improve and market their products. Whether this is ethical or not is a separate discussion, but the backdoor itself is a major security risk as things currently stand.

B. Malware

Not unlike more traditional internet connected devices such as our computers and smartphones, IoT devices can also fall prey to malicious software and viruses. Unlike more traditional devices, collections of IoT devices typically have much less diversity between devices, and virus removal can be extremely difficult. This, as well as the simplicity of the devices themselves, makes them a desirable target for those with malicious intent. As the IoT landscape continues to develop and grow it becomes a much larger target for potential attack and exploitation from those seeking to cause harm, particularly in cases where networks of IoT devices are not properly secured in the first place. As their use continues to increase, the development of rigorous security standards and anti-virus protections also needs to match or exceed in terms of innovation. In a comprehensive survey of world of IoT malware prevalence, researchers at University of Jyva¨skyla¨ concluded that although the variety of current threats is fairly small in comparison to more general computing devices, that the security community needs to adopt a more agile and proactive approach to developing countermeasures to these emerging attacks [7]. As the IoT continues to expand and impact more and more of our daily lives, we believe that the responsiveness towards targeted IoT malware will improve as well. If these improvements do not scale, malware may present a major inhibitory factor to the adoption of internet of things devices across the world at large.

C. Large Attack Surface

First, all of these previous areas of security concern are compounded by the fact that the current deployment of IoT devices is expansive. Current projections assert that there are over 14 billion IoT devices currently in deployment as of this year [8]. This number is only growing and has already outnumbered the population of people on Earth. This also means that without rigorous security standards in place there is an overabundance of potentially susceptible devices out in the wild. An entity with malicious intent has an extremely large pool of opportunity to dredge for possible hacking and unauthorized access. "Fig. 2", underlines the importance of IoT security as well as helps to explain why there is not yet a more universal security standard. There are just too many devices in place already to unify them now [9].

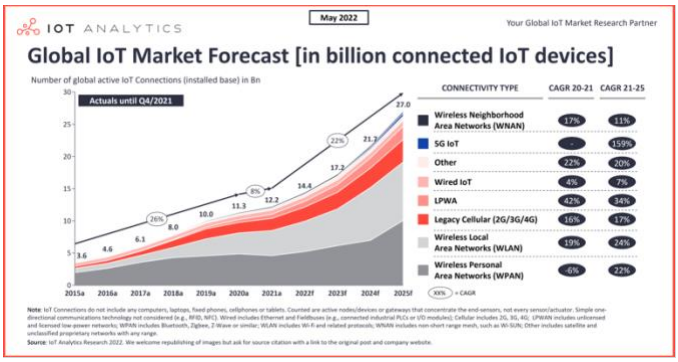

Fig. 2. This image shows the global market forcast of the Internet of Things.

D. Lack of Universal Standards

Any breach of security runs the risk of exposing more personal information than ever before, and as we become more and more attached to these devices, we also become more and more vulnerable. In its current form, IoT devices communicate through various existing protocols. NFC, RFID, Bluetooth, and Wi-Fi for example are all commonly used for IoT interconnectivity [10]. Although the adoption of smart home technology and other IoT appliances is growing, with nearly twice as many IoT devices as people on earth, there are still major improvements that can be made to their security [11]. Each of these comes with their own security standards, and currently there is no common communication standard that can be shared between all IoT devices regardless of their communication medium. This presents one of the most immediate issues facing security with the IoT. The current state of the art for Internet of Things security is that while these systems have preexisting security standards on an individual basis, there is not yet a standard that unites them all. The creation and adoption of such a standard would allow IoT to progress in new and exciting ways, furthering its usefulness to our relationship with technology.

One reason that has prevented such a standard from being developed is the sheer amount of diversity seen within the current Internet of Things landscape. That being said, some specific sectors within IoT have begun to see more homogenized standards and development. The Wi-SUN Alliance for example has been working to develop an IoT connectivity framework based on IEEE 802.15.4g standard based interoperability [12]. Their primary focus though is more centered around large -scale outdoor IoT wireless communication networks that would be used by service providers, municipalities, and governments to operate more infrastructure based IoT devices. Although they are finding success in building a unifying standard for those types of devices, it does not do much for more personal IoT devices such as smart appliances found within the home. The variation between types of IoT devices and their applications creates a difficult challenge for those who would seek to unify them. This is not to say that a universal security standard is not possible in the future, just that the focus now is more centered around unifying similar sectors.

III. Security Concerns Around Various Devices

This section will discuss specific descriptions of possible attacks on IoT devices that target the vulnerabilities that were previously described.

A. Amazon Alexa

The Amazon Alexa is a prime example of security concerns in an IoT device. It is a smart home device that listens for questions or commands from those nearby and responds accordingly. The response can be purely auditory or they could perform an action. The action would usually make use of a connection to other smart IoT devices in the user's home, such as their lights or entertainment system. The Amazon Alexa comes with the ability to recognize a myriad of such commands and has a way to expand the list with Alexa's downloadable skills, which can perform custom actions. They can be created by third party developers, which allows for a lot of creativity and innovation. For a skill to become available for download to Alexa, it must first pass Amazon's vetting process, which should ensure compliance to Amazon's security standards. It is necessary for the vetting process to be comprehensive because of the personal setting that Alexa functions within— the user's home.

However, according to a study completed by researchers from Ruhr-Universität Bochum in Germany, North Carolina State University, and Google, the vetting process is not good enough. The first issue is that developers can create skills under any name they wish. The vetting process does not do anything to confirm that a developer is associated with the name given, so if someone were to create a skill under the name "Samsung", there is nothing stopping them [13]. A reputable name can cause the user to trust the skill more easily and download it onto their Alexa, whether the skill was actually trustworthy or not. The vetting process also does not check the skill's activation command well enough. The developer can make a command from anything, including common words or phrases [13]. If they want to trick a user into running an action, it would not be difficult to get their trick past Amazon.

The most dangerous security flaw with skills comes in after vetting is complete. A developer could create a harmless skill that makes it through the vetting process and is thoroughly enjoyed by users, but still be malicious. Once a skill has been approved, the developer can change the backend code to whatever they want, which could completely change the effect of the skill's action [13]. The Alexa will have an abundance of personal data and information about its users, and a lot of this data can be used by skills. If the backend is redone to steal this data, the results could be very dangerous. This could also mean the developer could have access to other IoT devices the Alexa is connected to, making it an attack vector for other devices as well.

B. Smart TV's: Personalized Advertising

Similar to the Amazon Alexa, smart televisions are another type of IoT device that exists in most homes. The aspects of a TV that make it "smart" can vary because every manufacturer will put their own special features on each model to make it smarter than the rest. Most commonly, a smart TV is just a TV

that can connect to the internet. They also usually have preinstalled applications and an integrated way of installing new ones. The current TV market shows that anyone who buys a new TV now is almost certainly buying a smart TV. This means they abide in most households and are connected to the internet of things.

For a device to become smarter, it needs more data. So smart devices will have a plethora of different pieces of data about a person. For a smart TV, this can include microphone input, viewing and watch history, app analytics, and other more identifying information about the user [14]. This data is certainly used for benign purposes. It could be used to recommend new TV shows to watch or to optimize a user's viewing experience. However, the existence of the data leaves the possibility of unsolicited usage or full misuse. One concern is exposing the data directly to the developers who create software for the televisions. It is also concerning that many TVs are already using their collected data for targeted advertising. This is not an inherently bad thing, but the user usually is not given a choice as to how their information will be used, aside from a privacy policy [14].

IV. Potential Improvements

As with any growing technology there is always room for improvement and the IoT is no exception. As the IoT leaves its infancy, the world can expect to see major changes and improvements that fundamentally change our understanding of the technology.

A. Universal Standards

Out of these changes, one of the most impactful would be the adoption of universal security standards. Although it would be unfeasible to design a one-shoe-fits-all solution that encapsulates the entirety of the IoT, many industry leaders envision individual sectors embracing shared security standards in order to promote better cross-platform compatibility between products.

Particularly at the consumer level, a shared framework that allows users to experience the same rigorous security standards no matter the platform would be beneficial for all involved. Relating to this, further improvements could be made towards researching and preventing malware specifically designed to attack IoT devices and networks. Although compared to personal computers and smartphones the IoT is relatively safe, as the adoption of IoT devices grows the industry will need to be ready and able to respond to threats. Keeping abreast of the development of IoT-specific malware will be critical in ensuring the safety of users and entities that use these devices and remaining agile and able to react to potential threats as they emerge will soon become common practice within the IoT industry.

It can also foresee the advent of IoT related legislation that is specifically targeted at protected consumer privacy. As people live more and more of their lives online, privacy becomes more important as well. As users at all levels engage with the IoT in increasing numbers, privacy will need to be legally protected in a way that applies to this changing landscape. Improved legislation designed to protect privacy could further prevent surveillance or the prevalence of backdoors in our IoT networks.

B. Legislation

Bruce Schneider of Harvard University suggests a less technical approach to improving the security if the internet of things, in the form of legislation. The IoT Cybersecurity Improvement Act has already been drafted and introduced in the senate as of 2017. The act would create a minimum-security standard for any IoT device bought by the government [15]. His stance is that the field's priorities should not be set on developing new security measures when the bigger issue is that no one is implementing the defenses that are already available. Companies need an incentive to make their products secure. The bill would not force any companies to do anything or create any direct regulation on the market. Through creating a standard for the devices used by the big-spending government, companies are incentivized to at least meet the minimum.

Even this minimum standard, if spread wide enough, would be a massive improvement to the overall security of the internet of things. As discussed, one of the biggest problems with IoT security is the lack of standards. Obviously, having any standards in place is better than none. This would also create a foundation for further standardization, as it is much easier to add to a standard than it is to create one from scratch. The bill, if accepted, would create the head start we need. In his article, Schneider says, "The odds of this becoming law are zero," so he was undoubtedly excited when it was passed into public law in December 2020 [15].

C. Networking

A substantial portion of the security vulnerabilities in the IoT stem from network security and the large attack surface. Improvements should aim to shrink the attack surface as well as mitigate any networking threats. These threats should be similar or identical to known threats in existing networks, so the solutions are already known [16]. It seems that the best way to shrink the attack surface is to separate the networks. The FBI recommends that users keep their IoT devices on a separate Wi-Fi network than the rest of their devices. Specifically, they said, "your fridge and your laptop should not be on the same network" [17]. Having a separate network for IoT devices is not a realistic solution for the average person, but it does show the merits of having a separate IoT network in general. The Helium blockchain is one approach Helium is taking to implement this solution. They are working on creating a decentralized wireless network specifically for IoT devices. This approach is not a perfect solution, so more work is needed to create anything useful with a separate network.

V. Conclusion

Since the late 1990s, computer scientists have been working to create an Internet of Things that can be used by anyone. This is an appealing idea, because most people would like their devices to become smarter, more automated, easy to use, and interconnected with other devices. The unification of these devices has improved many parts of people's lives, such as making mundane tasks automated. However, unifying these

devices has come with a plethora of security and privacy challenges. Some examples of the challenges discussed in this paper was through the form of surveillance, company-inserted backdoors, and specialized malware. All of these issues can be further amplified with the lack of universal standards and the large attack surface created by a network of devices that everyone uses. Smart assistant devices are always listening and often have a large developer base, which is bound to include some malicious actors. Even televisions are beginning to track data about their users. Although the situation of IoT security may seem dire, there is still hope.

Today, standards are being developed on multiple fronts to attempt to unify the devices and their security. Legislation is being put in place to incentivize securing devices and ensuring privacy. Of course, research is always continuing in an effort to find better methods of securing IoT devices and the network that connects them. In the future, it is likely that the biggest improvements in IoT security will be in standardization. Going off of the development of standards in the past, it is not a trivial task to get everyone to agree, and it is even more difficult to get everyone to adopt the new standard. What the industry needs to accomplish this is time. There will be more legislation to help with this, because the government will want to ensure that any smart devices they use are at least minimally secure. The evolution of IoT specific malware will become a growing threat. This will require even more research and adaptability in the field to keep pace. In essence, despite the challenges on the horizon, the future is looking bright for a secured Internet of Things.

REFERENCES

[1] P. Corcoran, The Internet of Things: Why now, and what's next? *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 63-68, 2016.

[2] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications,* 2015.

[3] L. Chapin, S. Eldrige, K. Rose, The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. Geneva, Switzerland: Internet Society, 2015.

[4] B. Jovanovic, "Internet of things statistics for 2022 -taking thingsapart," DataProt. [Online]. Available: https://dataprot.net/statistics/iot-statistics/#:~:text=In%202021%2C%20there%20were%20more,in%20economic%20value%20by%202025. [Accessed: 10-Jun-2022].

[5] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical design in the internet of things -science and engineering ethics," SpringerLink, 21-Jan-2016. [Online]. Available: https://link.springer.com/article/10.1007/s11948-016-9754-5. [Accessed: 21-Jun-2022].

[6] T. Munk, "The internet-of-things: A surveillance wonderland," *Rethinking Cybercrime*, pp. 191–211, 2020.

[7] A. Costin and J. Zaddach, "IOT malware: Comprehensive survey, analysis framework and case studies," IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies. [Online]. Available: https://i.blackhat.com/us-18/Thu-August-9/us-18-Costin-Zaddach-IoT-Malware-Comprehensive-Survey-Analysis-Framework-and-Case-Studies-wp.pdf. [Accessed: 05-Jul-2022].

[8] M. Hasan, Global IoT Market Forecast [in billion connected IoT devices]. 2022.

[9] M. Hasan, "State of IOT 2022: Number of connected IOT devices growing 18% to 14.4 billion globally," *IoT Analytics*, 14-Jun-2022. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/. [Accessed: 20-Jun-2022].

[10] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in internet of things: State of the art and Challenges," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017.

[11] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IOT devices in the home: Security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[12] Wi-SUN for IoT, "Wi-SUN for IoT," *SUN Alliance*, 22-Apr-2022. [Online]. Available: https://wi-sun.org/.

[13] C. Lentzsch, S. J. Shah, B. Andow, M. Degeling, A. Das, and W. Enck, "Hey Alexa, is this skill safe?: Taking a closer look at the Alexa Skill Ecosystem," *Proceedings 2021 Network and Distributed System Security Symposium*, 2021.

[14] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, D. Y. Huang, N. Feamster, E. W. Felten, P. Mittal, and A. Narayanan, "Watching you watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices," *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019.

[15] B. Schneider, "IOT security: What's plan B?," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 96–96, 2017.

[16] F. A. Alaba, M. Othman, I. A. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, Jun. 2017.

[17] "Tech Tuesday: Internet of things (IOT)," *FBI*, 03-Dec-2019. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot.