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

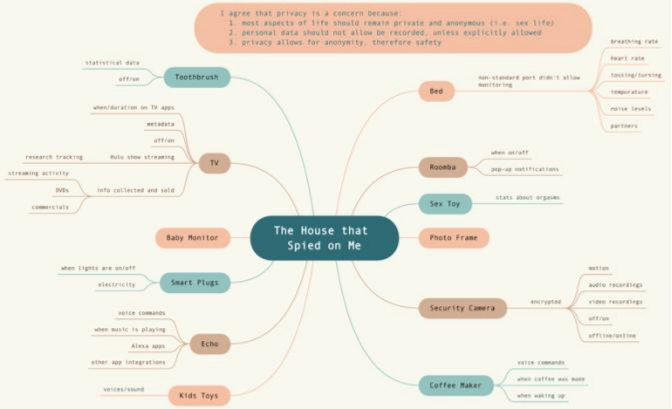
***Abstract*—The consumer use of the internet of things has grown to such a large scale that most people interact with it daily. As the number of devices grows, so too does the volume of security issues and privacy concerns. It has spread from smart refrigerators, thermostats, phones, vehicles, sensors, 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

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 RFIDs 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].



[Talk about article, update image above]

The IoT has transformed how people 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].

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. [ADD MORE ABOUT SNOWDEN]

As these challenges continue to emerge, it is clear that the IoT has become a complex and intertwined web of network connections. 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. [ADD KEY CONTRIBUTIONS]

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 haven’t 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 don’t 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

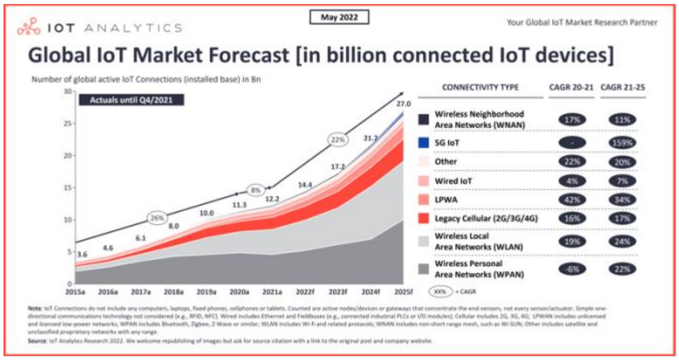
[ENTER]

C. Shadow/Rogue Devices

[ENTER]

D. Large Attack Surface

First All of these previous areas of security concern are compounded by the fact that the current deployment of Internet of Things devices is expansive. Current projections assert that there are over 14 billion IoT devices currently in deployment as of this year [7]. 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. This figure underlines the importance of IoT security, and also helps to explain why there isn’t yet a more universal security standard. There are just too many devices in place already to unify them now [8].



E. 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 [9]. 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 [10]. 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 [11]. 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 doesn't 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 isn't 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 described above.

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 [12]. 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 [12]. 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 [12], which could completely change the effect of the skill's action. 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

[WORK IN PROGRESS]

- F As devices become smarter, they store more data about a person
- This goes for TVs now too. Roku, Apple TV, etc.
- TVs themselves are taking data to make targeted advertising
- Privacy concern

IV. Potential Improvements

[ENTER]

V. Conclusion

[ENTER]

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 things apart," *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] M. Hasan, Global IoT Market Forecast [in billion connected IoT devices]. 2022.

[8] 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].

[9] 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.

[10] 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.

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

[12] 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.