The Internet of Things: Safety Issues and Solutions

Olivia Criscione

University at Albany, SUNY

CINF100X

Professor Jeff Yates

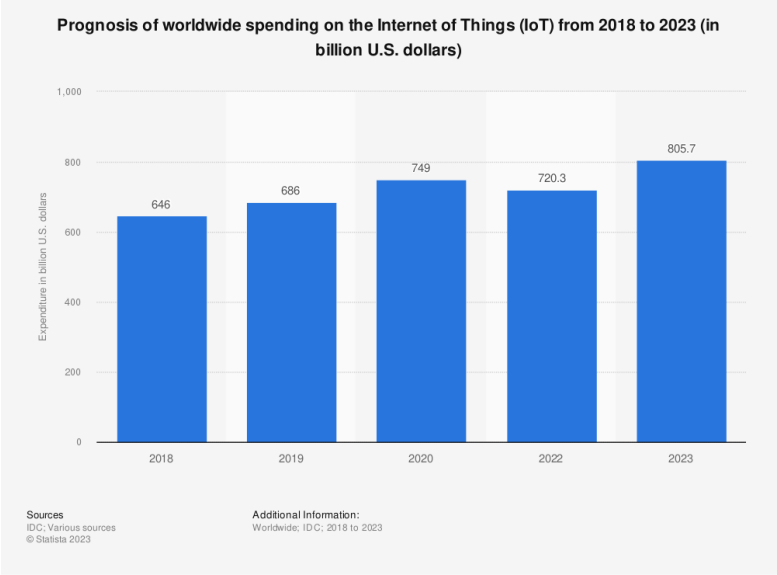
Internet of things (IoT) devices are becoming increasingly popular in homes across the world due to the convenience that they provide. However, these devices can leave you and your personal information at risk. Device owners are given little to no information about how these devices can impact their cyber-attack risk and are not given any solutions which would enable users to lower their risk. These devices also pose a major risk to many industries that rely on IoT technologies for communication, monitoring, sensing, and convenience.

IoT devices are any type of physical object, device, sensor, or node that connects with other devices via the internet. While IoT devices are becoming increasingly popular today, they have been around since the 1980s when the first IoT device ever was created, a soda machine (Watters, 2023). The creation of the IoT soda machine led to the creation of ATMs, another widely used IoT device today. Users can use IoT devices to add remote access and functionality to their home and life, and they are also used for monitoring and sensing in many different industries. Internet of things devices are used especially in the healthcare, agriculture, construction, energy, and industrial industries (Watters, 2023). In 2022, internet of things devices used in the healthcare industry were market valued at an astounding $291.2 billion and the industrial industry is expected to reach $106.1 billion on IoT devices by 2026 (Watters, 2023). According to CompTIA, there are approximately fifteen billion IoT devices in the world in 2023. The internet of things market is expected to have more than seventy-five billion devices worldwide by 2025 (Watters, 2023). According to Forbes, the average household in the United States has approximately 20.2 connected IoT devices (Koetsier, 2022). By 2025, it is predicted that each person will own approximately 25 personal IoT devices (Butun, Österberg, & Song, 2020). The graph below shows the IoT market over the past six years. According to the graph below, worldwide spending on Internet of Things devices continues to grow year over year and is expected to continue trending upward because of the convenience that they provide to

homeowners and the impacts that they have made on different industries, making monitoring, and recording easier and cheaper than ever before. Due to the coronavirus pandemic in 2020, the IoT market grew because people were unable to leave their homes for work and recreation and needed to add functionality for both work and leisure time to their homes via Internet of Things devices. In 2022, the market decreased slightly due to people returning to work in-person instead of virtually. So far in 2023, IoT device spending is at 805.7 billion dollars worldwide, showing how big the IoT market is currently (Vailshery, 2023).

Figure 1:

IoT Market Spending Worldwide in Billions: 2018 – 2023.



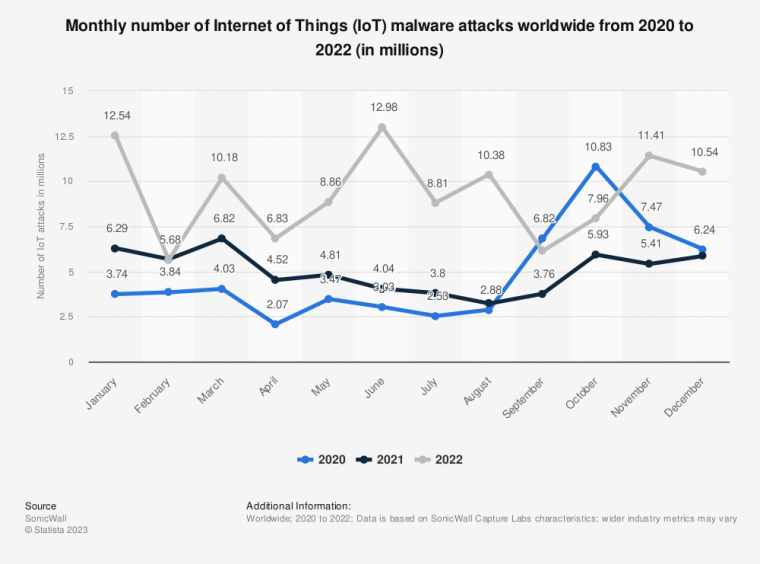
The increase in IoT devices in the world comes with a huge challenge for the technology industry, in both security vulnerabilities and threats. IoT devices are constantly communicating and sharing data with other devices via the internet with few security precautions in place to keep personal and corporate data safe. While the Internet of Things market is already worth billions on its own, the IoT security market was worth an estimated $3.35 billion dollars in 2022 and is expected to grow to $13.36 billion dollars by 2028, at over 25% a year (Watters, 2023).

According to CompTIA, there were over twelve million cyber-attacks via IoT devices in 2022. Malware attacks also increased by over 77% in just the first half of 2022, highlighting the lack of security protocols in IoT devices. One example of a common security vulnerability in IoT devices is cloud integration issues (Butun, Österberg, & Song, 2020). Insecure hardware with little to no built-in security controls or functions allow for easy access for hackers (Pratt, 2023). Difficulty with software updates adds to security vulnerabilities in these devices with little to no security patches being developed for these devices, especially if it is an older model, making it easy for hackers to exploit these IoT devices.

According to the graph below, over 10.5 million Internet of Things devices were victimized by cyber malware attacks just in December of 2022 (Petrosyan, 2023). The previous year in December, 5.85 million IoT devices were victimized, showing a dramatic increase between 2021 and 2022. The highest month for malware attacks on IoT devices was June 2022, with almost 13 million devices victimized (Petrosyan, 2023). This graph does an excellent job of showing not only how many cyber-attacks are occurring for users, but also showing how fast cyber-attacks are growing on these devices. Each device attacked by malware has users' personal information and data. Businesses that use IoT devices could have also had their valuable data stolen or lose functionality over their businesses, potentially costing them financially as well as impacting their credibility. Cyber-attacks also greatly impact the target businesses credibility for current and future customers, leading to an impact in sales and users. Security measures need to be implemented to reduce the number of attacks and the negative impacts that they have on users, businesses, and customers.

Figure 2:

Number of IoT Malware Attacks in Millions Worldwide: 2020-2022.



The lack of security protocols poses a huge threat to the industries that utilize Internet of Things devices, especially the healthcare industry. In the healthcare industry, IoT devices are used for monitoring and communication (Watters, 2023). An attack on a hospital would leave the hospital with little communication and devices which would become extremely dangerous and potentially deadly to patients. The healthcare industry also utilizes wearable IoT devices for patients, allowing the patient to see medical information while also sending the data directly to the provider's network. Because "It is often hard for these resource-constrained devices to execute computation-heavy security protocols for device authentication, public-key encryption, and rule out information leakage" hackers often exploit these wearable devices (Burg, Chattopadhyay, & Lam, 2018). These devices are often victimized by denial-of-service (DoS) attacks through a man in the middle operation, due to lack of encryption and other security vulnerabilities. Security vulnerabilities can lead to theft of confidential patient medical history (Burg, Chattopadhyay, & Lam, 2018). IoT devices are also used within the military for communication and for military operations / missions. A security vulnerability within the IoT devices used by the military could lead to casualties on the battlefield (Burg, Chattopadhyay, &

Lam, 2018). The widespread use of IoT devices across different industries and the great impacts that attacks can have on these industries, is another reason to invest into IoT security.

Wireless sensor networks used in IoT devices are vulnerable to a variety of cyber-attacks. These attacks are broken down into two distinct categories: passive attacks, and active attacks. Passive cyber-attacks are categorized as hidden attackers who damage network function or collect information and data. Examples of passive attacks include: eavesdropping, traffic analysis, and node outages / destruction. Active cyber-attacks are categorized as an attacker who impacts a targeted network by damaging the function and operations of the network. Denial of Service (DoS), jamming, blackholes, wormholes, and sinkholes are all examples of active cyber-attacks on Internet of Things devices (Butun, Österberg, & Song, 2020). Another type of IoT attack is IoT botnets, where an attacker "infects an IoT device with malware through an unprotected port or phishing scam and co-opts it into an IoT botnet used to initiate massive cyber-attacks" (Pratt, 2023). This type of attack is used for distributed denial of service attacks (DDoS) to overwhelm and disarm the targeted network traffic. Botnet attackers utilize IoT devices for attacks due to "weak security configurations and the quantity of devices that can be consigned to a botnet" for attacks (Pratt, 2023). Ransomware attacks are another common type of IoT attack used by hackers. Attackers "infect devices with malware to turn them into botnets that probe access points" to enter the target network, who then can steal company or personal data that they can threaten to keep, sell, delete, or release to the public. The only way to get the stolen data back is for the company or person to pay the ransom that the attacker requested. Sometimes, even if the company pays the ransom, the attacker will still delete the stolen data (Pratt, 2023). The reason that victims often decide to pay the ransom is because it would be too difficult for them to try to recover their data back through alternative means. It is hard to regain information because attacks are often so "difficult to decrypt that sometimes it becomes necessary to pay" the

ransom (Humayun, Jhanjhi, Alsayat, & Ponnusamy, 2020). The United States is the number one country for ransomware attacks, making up 29% of the attacks worldwide (Humayun, Jhanjhi, Alsayat, & Ponnusamy, 2020). With so many different attacks on IoT devices, it will be especially important to make the necessary security changes to reduce the number of attacks worldwide and to reduce the impacts of these attacks on the victims.

While the IoT market continues to grow rapidly, we will need to invest heavily into the IoT security market to combat IoT based cyber-attacks. One of the easiest ways to improve security vulnerabilities is to make sure that you always update your devices to the latest software update if available. IoT manufacturers need to be more vigilant in creating new software updates and security patches to improve security of their devices (Pratt, 2023). Businesses need to know their IoT assets and ensure that all assets are updated and accounted for (Pratt, 2023). They should also create security protocols and strategies. Accountability and updating will greatly improve security for businesses and personal owners because many businesses do not know how many assets they own, which can lead to a security leak via a missing device on their network that provides easy access to their network and data. Adding encryption into the link-layer would reduce passive attacks on WSNs such as eavesdropping (Butun, Österberg, & Song, 2020). Camouflaging nodes from attackers and increasing the number of nodes would provide greater protection against node destruction / outage attacks (Butun, Österberg, & Song, 2020). The figure below also shows great ways to improve IoT security such as strengthening the most vulnerable points where attacks are most likely to occur (Pratt, 2023). Reviewing assets and management policies is also an effective way of improving security because it adds accountability of assets and ensures updating of out-of-date security policies that do not provide adequate coverage for the company (Pratt, 2023). It is also a promising idea to hire ethical hackers or penetration testers to evaluate the security of your company and to provide insight

into where you can improve your digital security (Pratt, 2023). Ethical hackers can point you to weak links in your security network that can be easily exploited by attackers.

Figure 3:

Steps to Improve IoT Security and Reduce Attacks.

While having IoT devices can be convenient for the home, in healthcare, and other industries, it is important to take the necessary steps to protect your personal and consumer information by implementing security practices such as changing default passwords to long, hard to guess passwords, updating to the newest software / security update, creating more security patches, and knowing your assets. In a fast-growing market of Internet of Things devices, it is important to start to heavily invest in the IoT security market to add functionality to the devices which would allow security measures to be implemented.

Work Cited:

Burg, A., Chattopadhyay, A., & Lam, K.-Y. (2018, January). Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. Proceedings of the IEEE, 106(1), 38-60. doi: 10.1109/JPROC.2017.2780172. https://ieeexplore-ieee-org.libproxy.albany.edu/document/8232533

Butun, I., Österberg, P., & Song, H. (2020, First quarter). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644. doi: 10.1109/COMST.2019.2953364. https://ieeexplore-ieee-org.libproxy.albany.edu/document/8897627

Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2020, May 28). Internet of Things and Ransomware: Evolution, Mitigation and Prevention. Egyptian Informatics Journal. Retrieved from https://www.sciencedirect.com/science/article/pii/S1110866520301304.

Koetsier, J. (2022, September 6). Smart home: Apple is the fastest-growing connected device company. Forbes. Retrieved from https://www.forbes.com/sites/johnkoetsier/2022/08/31/smart-home-apple-is-the-fastest-growing-connected-device-company/?sh=a4ec0f07dd48.

Figure 2:

Petrosyan, A. (2023, April 6). Monthly number of Internet of Things (IoT) malware attacks worldwide from 2020 to 2022. Statista. Retrieved from https://www-statista-com.libproxy.albany.edu/statistics/1322216/worldwide-internet-of-things-attacks/.

Figure 3:

Pratt, M. K. (2023, June 27). Top 12 IoT security threats and risks to prioritize. TechTarget. IoT Agenda. Retrieved from https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize.

Figure 1:

Vailshery, L. (2023, July 26). Prognosis of worldwide spending on the Internet of Things (IoT) from 2018 to 2023. Statista. Retrieved from https://www-statista-com.libproxy.albany.edu/statistics/668996/worldwide-expenditures-for-the-internet-of-things/.

Watters, A. (2023, July 18). Top 30+ IoT statistics and facts you should know for 2023. Default. Retrieved from https://connect.comptia.org/blog/top-internet-of-things-stats-facts#:~:text=There%20are%20approximately%2015.14%20billion,IoT%20is%20remote%20asset%20monitoring.