Anita Chidera Duanne Eluwa

22nd April 2022

EG 6335 – Wireless Security

Glenn Howard – Academic Research Essay

Academic Research Essay: IoT Security Challenges and Countermeasures

ABSTRACT

The Internet of Things (IoT) has rapidly evolved with time and is embedded in our everyday life. However, due to the challenges and security issues that wireless networks face daily, IoT devices are also facing the same security and privacy issues. Some of the challenges that these smart devices face include user unawareness, improper security controls, lack of device updates and patches, lack of monitoring, and a whole lot more. This research paper gives a little insight into IoT and its purpose in modern technology. Some of the different types of attacks that IoT devices are susceptible to are also explained. Countermeasures are also provided on how to mitigate the highlighted attacks. This is then followed by future work of this research paper and conclusion.

Keywords: Internet of Things; active and passive attacks; security; privacy

1. INTRODUCTION

Internet of Things (IoT) in layman's terms is any device that can connect to the internet. They include the refrigerator, microwave, washing machines, dishwashers, etc. They are often referred to as smart devices. There are smart home devices, industrial sensors, industrial robots, healthcare devices, connected cars, and even recently smart cities. These devices are embedded with processing ability, sensors, and software that enables the exchange of data and communication over the internet. Technology has grown and advanced over the years. IoT has also expanded with time. It has gone beyond the regular devices to being used for transportation, education, business development and a lot more. The expansion of IoT has solved a lot of problems in terms of convenience and made technology a lot easier. However, it has also brought about a lot of security and privacy issues. These have always been the major problem with technology and the fact that the users are unaware of these issues is also a challenge.

These modern technologies and IoT devices are introduced and given to the public with huge advertisements and marketing strategies, but no security awareness is made to the public. This makes it easier for attackers to penetrate and get into the system without being noticed. The unconscious use, not changing passwords, and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems' sensitive data and such inappropriate security practices increase the chances of a data breach and other threats (Tawalbeh, Muheidat, Tawalbeh, & Quwaider, 2020). Most of the attacks on these smart devices are classified as active and passive attacks. Active attacks are attacks where the adversary or unauthorized user attempts to modify the content of the messages. In passive attacks, the attacker listens to the data and decides to store them for a later malicious purpose. This is often known as an eavesdropping attack or sniffing attack. This is one of the most dangerous attacks because an attacker can be listening without the consent of the users, and it won't be noticeable. The next paragraph highlights some of the attacks that IoT devices are susceptible to.

2. IoT SECURITY VULNERABILITIES AND ATTACKS

The first attack that an IoT device is prone to is the eavesdropping attack. As I mentioned earlier, this is a passive attack that occurs on a network. For example, a smart vacuum cleaner that communicates over a network is susceptible to a hacker intercepting the network to steal data between the vacuum cleaner and the server. This type of attack can have an adverse effect on the user because it can go unnoticed.

The second attack is the jamming attack. This is one of the most common attacks that happen in the physical layer of the wireless network. Jamming attack occurs when radio frequencies interfere with the data communication and operations of the wireless network. This can be done intentionally or unintentionally. When it is done unintentionally, a cordless phone might be placed close to a microwave or a router and the signal transmitted will interfere with the wireless network and cause a jam. An intentional jam occurs when the attacker analyzes the wireless network spectrum and transmits a signal that interferes with the communication on the discovered frequencies. Then leads to a denial of service of the device and the network.

The third attack is a spoofing attack. This attack happens on the network layer or data link layer of the network. Spoofing occurs when an attacker pretends to be a legitimate or authorized user to gain access to sensitive information. In an IoT device, an attacker can use a legitimate user’s IP (internet protocol) address or MAC (media access control) address to gain access to the IoT device without the knowledge of the authorized user. Spoofing can also occur in voice user interfaces (VUIs). This can be either a replay attack, a hidden command attack or an inaudible command attack. In a replay attack, an adversary tries to fool the VUI by using the pre-recorded voice of a legitimate user while in hidden command attacks, attackers use a falsified speech signal as the system input. (Meng, Zhang, Zhu, & Shen, 2018). Attackers inject inaudible voice commands that humans might not hear or understand but will be understood by the VUI. These attacks are types of spoofing attacks that adversaries use in voice over interfaces.

The fourth attack found in IoT devices is privilege escalation. This is done when an attacker attempts to find bugs or weaknesses in the software to gain escalated access to a system. Privilege escalation can either be horizontal or vertical. Horizontal privilege escalation occurs when an unauthorized user tries to gain the privilege of another user and misuses the privileges granted. In this case, two users A and B have the same privilege access to a particular system or file, but user A tries to get user B's privilege access to use it for a malicious purpose or frame user B for engaging in illegal transactions. Vertical privilege escalation is when an attacker or unauthorized user hacks into a system and attempts to gain higher privilege access or more permissions than what he or she already has. For example, user A hacks into a system and has access to just the read files in the system, then user A tries to gain more access to the admin or root directory. This usually poses a greater threat to the system than the horizontal privilege escalation.

The fifth attack is the brute-force attack. Brute-force occurs when hackers try to guess a password or login information using a trial-and-error method until they exhaust all possible combinations and get access to the system. This is very common among IoT devices where an unauthorized user attempts to get into a device e.g., a safe box. The attacker then tries multiple combinations of passwords until the correct one is guessed and grants him access to the safe box. This is a very common attack as it does not necessarily require any special technical skill. Recently, some algorithms and tools make it easier to break into more complex systems in seconds and minutes.

Lastly, there is also a vulnerability called zero-day vulnerability. This occurs when the software developers are not aware of the present vulnerability in the system. Hence, it remains quietly in the system and until it has been mitigated, hackers will continue to exploit it and cause harm to the system by compromising the data or the software of the system.

The above attacks explained are some of the major attacks that IoT devices are faced with every day. These attacks work in each other's favor because when one attack is successful, it makes the system more vulnerable and easier for the other vulnerabilities to be exploited. There are however countermeasures that are used to eliminate or reduce the possibilities of these attacks in the system.

3. COUNTERMEASURES AGAINST IoT ATTACKS

3.1 Eavesdropping Attack

To protect against eavesdropping, the most important security measure to implement is encryption. Encryption is a cryptographic method of converting plain text (the original data) to cipher text (unreadable data). It uses a secret key for this conversion and the key is only known to the sender and receiver. There are different algorithms used for encryption depending on the key size like RSA, SHA256, or hash chains are required to secure the user and environment data from being captured because this will help in gaining the trust of the individuals, government agencies and industries in IoT applications (Hassija, et al., 2019). When this is done, the attacker won't be able to read the data being transmitted because it will be written in garbage. Another way of preventing eavesdropping attack is to use a virtual private network (VPN). A VPN allows users to share information across a public network without making the content of the data public. This is highly recommended when using a public Wi-Fi network. The VPN will provide online privacy and prevent eavesdropping.

3.2 Jamming Attack

Jamming attacks as explained earlier are very common among IoT devices and often lead to a denial of service of the device and the network. To protect against jamming attacks, intrusion detection systems are recommended because they detect the jamming attacks instantly. Frequency-Hopping Spread Spectrum (FHSS) minimizes unauthorized interception and jamming of radio transmission by switching a carrier among frequency channels using a shared algorithm that is known to the transmitter and the receiver. Direct Sequence Spread Spectrum (DSSS) multiplies the data that is transmitted, and a Pseudo-Noise (PN) digital signal and the processing makes it difficult for an attacker to descramble the transmitted data to recover the original signal.

3.3 Spoofing Attack

The best way to prevent IP and MAC spoofing is to use a packet filter. Packet filtering analyzes and blocks packets that contain conflicting source information. Hence, the packet filter eliminates the malicious packets coming from the hacker into the network to prevent them from being spoofed. To mitigate the voice user interface (VUI) from being spoofed, a two-factor based voice authentication is proposed. This helps to generate a unique voice of each user using an accelerator and cannot be replicated. This will prevent the attacker from spoofing a voice and deceiving the device that it is the legitimate voice being used.

3.4 Privilege Escalation

The principle of least privilege is the most common method used to prevent privilege escalation. This is the principle that allows users to have only the necessary privileges and access to specific data and programs. This is a very important security measure and is recommended by the NIST framework (NIST 2P 800-179) as a security policy that must be obeyed to protect the confidentiality, integrity, and availability of data. With this principle implemented, it prevents unauthorized users from trying to escalate their privileges to gain access to sensitive data. It enhances access control of the device and the data. Another security measure is enforcing strong password policies for each user. The users should weave unique passwords and must meet the requirements of password complexity and length for each device or system. There are also some privilege escalation attack prevention tools that can be used to detect the attempt of a privilege being escalated. Some of the tools are, Cynet 360, Exabeam, JumpCloud and a lot more.

3.4 Brute-force Attack

The first and most important way to protect against brute force attacks is end-user training. The user of the device needs to know that there are requirements and policies for passwords. The mistake users usually make is keeping the default passwords of the devices as their passwords. This is one of the weakest passwords that any device can have and makes it super easy for an attacker to guess the password. The users should be aware that passwords must be complex and have a required length. The higher the complexity of the passwords, the harder it is to successfully launch a brute force attack. Adding another layer of security like a two-factor or multi-factor authentication reduces the possibility of a brute-force attack. There are also password management tools that can help generate complex passwords that meet the password requirements.

3.5 Zero-day Vulnerability

One way to eliminate a zero-day vulnerability is to enforce constant system updates and patch management. This helps to reduce the vulnerabilities that are hidden and unknown to the developers before giving the attackers an opportunity to exploit. The most effective way to prevent a zero-day vulnerability is to implement a web application firewall (WAF). The WAF filters all incoming traffic and eliminates malicious traffic that could target the vulnerabilities in the system.

IoT PRIVACY ISSUES

Having looked at some of the security vulnerabilities of IoT devices, it undergoes some privacy issues as well. Consumers are sending in their data without even realizing the depth of it and what the data is used for. Some of the smart devices like Amazon Alexa and Google Assistant can listen to conversations and capture your location. Some of these data are sold to third party companies that might be used for constant advertisements which serve as a disturbance and possibly sold to spies or illegal users. This can lead to stalking, breach of confidentiality, and a lot more. Checking the privacy settings of the device to turn off certain features, updating the device regularly and using strong passwords can help protect your privacy to an extent but not fully. It is advisable to be well round aware of the privacy issues associated with these devices before purchasing them.

CONCLUSION

IoT technology has evolved since its inception and has brought convenience to consumers and modern-day technology. It however continues to pose a security and privacy threat to its users. There can only be methods to remediate these threats but not eradicate them completely. There are new developments each day and constant security research is required to discover new ways to protect the CIA and the privacy of the IoT devices.

REFERENCES

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, 4102.

Meng, Y., Zhang, W., Zhu, H., & Shen, X. (2018). Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures. *EEE Wireless Communications*, 53-59.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, 82721-82743.