International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

SECURITY ATTACKS AND PREVENTION IN IOT : A COMPREHENSIVE STUDY

L.Febin Rani

Assistant Professor,Deptof CSE, Bethlahem Institute of Engineering, Tamil Nadu

Abstract

The Internet of Things (IoT) industry is booming, offering data-backed insights that are providing value to numerous enterprises and industries. In agriculture, for instance, IoT devices are helping farmers monitor weather changes in the precise location of their crops to optimize labor, water usage and harvest health. In the supply chain, the IoT is being used to track the location and conditions of shipments, ensuring that transported goods make it to their destination safely and on time. DDoS attacks happen when devices are manipulated to send so many messages that the IoT network becomes overwhelmed and shuts down. Hackers use this method to take control of multiple compromised devices to create a "traffic jam," preventing necessary information from getting through to its destination.

Keywords: IoT, DDoS.

1. INTRODUCTION

Now, it is not only us with our computers, but there are also "things" that interact with the Internet without our intervention. These "things" are continually communicating with the Internet, a fridge sending an update of the food inside or our vehicle transmitting messages to the mechanic to inform its oil levels. IoT is wonderful in many ways. But unfortunately, technology has not matured yet, and it is not entirely safe. The entire IoT environment, from manufacturers to users, still have many security challenges of IoT to overcome, such as:

- Manufacturing standards
- Update management
- Physical hardening
- Users knowledge and awareness

2. CURRENT THREATS TO THE IOT

The following security issues with IoT can be classified as a cause or effect.

1) Lack Of IoT Manufacturers

New IoT devices come out almost daily, all with undiscovered vulnerabilities. The primary source of most IoT security issues is that manufacturers do not spend enough time and resources on security. For example, most fitness trackers with Bluetooth remain visible after the first pairing, a smart refrigerator can expose Gmail login credentials, and a smart fingerprint padlock can be accessed with a Bluetooth key that has the same MAC address as the padlock device.

This is precisely one of the biggest security issues with IoT. While there is a lack of universal IoT security standards, manufacturers will continue creating devices with poor security. Manufacturers that started to add Internet connection to their devices do not always have the "security" concept as the crucial element in their product design process.

The following are some security risks in IoT devices from manufacturers:

1. Weak, guessable, or hard-coded passwords
2. Hardware issues
3. Lack of a secure update mechanism
4. Old and unpatched embedded operating systems and software
5. Insecure data transfer and storage

2) Lack Of User Knowledge & Awareness.

Over the years, Internet users have learnt how to avoid spam or phishing emails, perform virus scans on their PCs, and secure their WiFi networks with strong passwords.

But IoT is a new technology, and people still do not know much about it. While most of the risks of IoT security issues are still on the manufacturing side, users and businesses processes can create bigger threats. One of the biggest IoT security risks and challenges is the user's ignorance and lack of awareness of the IoT functionality. As a result, everybody is put at risk.

Tricking a human is, most of the time, the easiest way to gain access to a network. A type of IoT security risk that is often overlooked is **social engineering attacks**. Instead of targeting devices, a hacker targets a human, using the IoT.

3) IoT Security Problems In Device Update Management

Another source of IoT security risks is insecure software or firmware. Although a manufacturer can sell a device with the latest software update, it is almost inevitable that new vulnerabilities will come out.

Updates are critical for maintaining security on IoT devices. They should be updated right after new vulnerabilities are discovered. Still, as compared with smartphones or computers that get automatic updates, some IoT devices continue being used without the necessary updates.

Another risk is that during an update, a device will send its backup out to the cloud and will suffer a short downtime. If the connection is unencrypted and the update files are unprotected, a hacker could steal sensitive information.

4) Lack Of Physical Hardening

The lack of physical hardening can also cause IoT security issues. Although some IoT devices should be able to operate autonomously without any intervention from a user, they need to be physically secured from outer threats.

Sometimes, these devices can be located in remote locations for long stretches of time, and they could be physically tampered with, for example using a USB flash drive with Malware.

Ensuring the physical security of an IoT device begins from the manufacturer. But building secure sensors and transmitters in the already low-cost devices is a challenging task for manufacturers nonetheless. Users are also responsible for keeping IoT devices physically secured. A smart motion sensor or a video camera that sits outside a house could be tampered with if not properly protected.

5) Botnet Attacks

A single IoT device infected with malware does not pose any real threat; it is a collection of them that can bring down anything. To perform a botnet attack, a hacker creates an army of bots by infecting them with malware and directs them to send thousands of requests per second to bring down the target.

Much of the uproar about IoT security began after the Mirai bot attack in 2016. Multiple DDoS (Distributed Denial of Service) attacks using hundreds of thousands of IP cameras, NAS, and home routers were infected and directed to bring down the DNS that provided services to platforms like GitHub, Twitter, Reddit, Netflix, and Airbnb. The problem is that IoT devices are highly vulnerable to Malware attacks. They do not have the regular software security updates that a computer has. So they are quickly turned into infected zombies and used as weapons to send incredibly vast amounts of traffic.

6) Industrial Espionage & Eavesdropping

If hackers take over surveillance in at location by infecting IoT devices, spying might not be the only option They can also perform such attacks to demand ransom money.Thus, invading privacy is another prominent IoT security issue. Spying and intruding through IoT devices is a real problem, as a lot different sensitive data may be compromised and used against its owner.

On a basic level, a hacker might want to take over a camera and use it for spying. Still, one should not forget that many IoT devices record user information, whether it is health equipment, smart toys, wearables, etc. On an industrial level, a company's big data that can be collected by hackers to expose sensitive business information.

3. DETECTION MECHANISM

IIoT infrastructure should be protected by a comprehensive set of security solutions that do not disrupt operations, service reliability or profitability. A practical and simple, yet secure solution that can be easily and widely adopted by IIoT device makers and their customers is more effective than a 'super solution' that fails to gain serious traction. Security solutions should include the following capabilities.

3.1 Firmware integrity and secure boot

Secure boot utilizes cryptographic code signing techniques, ensuring that a device only executes code generated by the device OEM or another trusted party. Use of secure boot technology prevents hackers from replacing firmware with malicious instruction sets, thereby preventing attacks. Unfortunately, not all IIoT chipsets are equipped with secure boot capabilities. In such a scenario, it is important to ensure that IIoT devices can only communicate with authorized services to avoid the risk of replacing firmware with malicious instruction sets.

3.2 Mutual authentication

Every time a smart actuator in the manufacturing floor connects to the network it should be authenticated prior to receiving or transmitting data. This ensures that the data originates from a legitimate device and not a fraudulent source. Secure, mutual authentication—where two entities (device and service) must prove their identity to each other—helps protect against malicious attacks. Cryptographic algorithms involving symmetric keys or asymmetric keys can be utilized for two-way authentication. For example, the Secure Hash Algorithm (SHA-x) along with hash-based message authenticated code (HMAC) can be used for symmetric keys and Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys.

3.3 Secure communication (end-to-end encryption)

Secure communication capabilities protect data in transit between a device and its service infrastructure (the cloud). Encryption ensures that only those with a secret decryption key can access transmitted data. For example, a smart actuator that sends usage data to the SCADA must be able to protect information from digital eavesdropping.

3.4 Security monitoring and analysis

Security monitoring captures data on the overall state of an industrial system, including endpoint devices and connectivity traffic. Data is then analyzed to detect possible security violations or potential system threats. Once detected, a broad range of actions formulated in the context of an overall system security policy should be executed, such as revoking device credentials or quarantining an IoT device based on anomalous behavior. This automatic monitor-analyze-act cycle may execute in real time or at a later date to identify usage patterns and detect potential attack scenarios. It is critical to ensure that endpoints devices are secured from possible tampering and data manipulation, which could result in the incorrect reporting of events.

3.5 Security lifecycle management

The lifecycle management feature allows service providers and OEMs to control the security aspects of IoT devices when in operation. Rapid

over the air (OTA) device key(s) replacement during cyber disaster recovery ensures minimal service disruption. In addition, secure device decommissioning ensures that scrapped devices will not be repurposed and exploited to connect to a service without authorization.

4. CONCLUSION

The main emphasis of this paper was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. In this survey, twelve different types of attacks are categorized as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks along with their nature/behavior as well as suggested solutions to encounter these attacks are discussed. Considering the importance of security in IoT applications, it is really important to install security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and network.

REFERENES

[1] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.
[2] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.
[3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014. [4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.
[5] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.
[6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
[7] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
[8] A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
[9] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in iot environment," in Computer Science and its Applications. Springer, 2015, pp. 691–696. [10] R. H. Weber, "Internet of things–new security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.