AI and Intrusion Detection

Victor Jehuziel CERVANTES IBARRA, Mingzhi HE, Assem MARATOVA, Alvaro Alejandro RODRIGUEZ GONZALEZ

Introduction

The Internet of Things (IoT) is one of the current fastest growing technologies. When we talk about IoT we refer to systems that interconnect through the internet by each providing an IP address. This technology comes with several advantages by allowing users to interact with the IoT-capable devices through the internet, and sometimes even the devices interacting amongst themselves. The IoT concept has become an integral part of our daily lives, providing users with unique capabilities ranging from home automation solutions to medical devices. Ultrafast wireless networks and advanced electronics allow IoT devices to efficiently and seamlessly collect, process and transmit large amounts of data. Advances in microelectronics coupled with low power consumption have made IoT devices even more feasible in remote locations requiring minimal physical surveillance and maintenance. This allows for the creation of networks that facilitate daily activities and can potentially improve the efficiency of our lifestyles. The full potential of IoT is yet to be uncovered since technology progresses rapidly, and there are more and more IoT devices being developed. However, there are disadvantages from a technology that relies on building networks through accessible sources. Although IoT devices seem harmless, they are not without security and privacy concerns, as there are many threats and vulnerabilities in today's IoT framework. Because these systems are connected from one to another, malicious access to one could jeopardize the entire network and exposure of user private data. There are multiple techniques that are used in attacks nowadays, and we will discuss a selection of them: DoS, Mirai, Scan and Spoofing. IoT security vulnerabilities lead to countless threats and attacks that can potentially compromise critical infrastructure and even national security, cause physical and financial damage and more. McAfee's quarterly Information Security Threats Report reports that 176 new cyber threats emerge every minute.

Denial of Service (DoS)

These kinds of attacks are one of the most common against IoT systems. Their main goal is to disrupt the expected behavior of systems, and there are different approaches to achieve this. For example, *jamming* happens at the physical layer, and this is the intermittent or continuous interruption of a signal. Furthermore, there are collision attacks at the data link layer which involves interfering with communication protocols to create said collisions. Doing so will require a retransmission of the packet, resulting in the waste of resources. Also, there are misdirection attacks on this layer where a jeopardized device will stop sending messages and disconnect a part of the network. Moreover, on the transport layer there are flooding attacks that consist of several connection requests to a device or server, and this will result in the exhaustion of resources for those requests, disabling such devices or servers. Another attack that depletes a device’s resources on this layer is de-synchronization. It forces the system into synchronization protocols until it stops working. Finally, the application layer falls prey to path-based attacks in which an attacker inserts packets over and over into a network. These attacks deteriorate the network of effective data transmissions, as well as consuming energy and bandwidth in the process.

Mirai

The Mirai botnet is a type of DoS attack that once it infects one IoT device, it scans the network for another vulnerable connection using a SYN scanner searching for Telnet or SSH ports. Once it finds another target, it self replicates and propagates by brute-forcing an attack on it. Its goal is to infect as many devices as possible. As a botnet, Mirai infects other devices that are then controlled via C&C servers, or command and control. Once a brute-force attack succeeds, it will send this server the address and credentials of the IoT device. These servers determine the next target. With that in mind, we can say that Mirai has two main components: a replicant module and an attack module. The replicant module is in charge of developing the botnet infection by multiplying it. It scans the network, looking for vulnerable devices, then it reports everything back to the C&C server. Finally, this server will inject the compromised device with a new Mirai botnet. This method of self-replication has resulted in the compromise of 380,000 devices just by Telnet attacks. The attack module is in charge of performing distributed denial of service attacks on the devices the C&C targets. It is capable of performing attacks on the network, transport and application layers. In the network layer, Mirai will perform a GRE IP or Ethernet flooding, and send several GRE packets to the DNS server to consume its resources. In the transport layer, it will perform a DNS water torture. By doing so, it will trick the ISP's DNS to attack the target's main DNS server. Once the server it's flooded, it becomes unresponsive. Furthermore, it will perform TCP STOMP, TCP SYN, TCP ACK, UDP, and UDP VSE query floods with the same goal. Finally, in the application layer, it will perform HTTP floods and CFNull attacks by exploiting valid GET and POST requests, as well as sending large amounts of junk information to the device until it's disabled. A Mirai-botnet-based DDoS attack on low-cost Internet of Things devices has infected more than 2.5 million devices in four months.

Scan

The main focus of a scan attack is to find vulnerabilities in a network. IoT devices tend to lack security and are easily targeted. As an example, there is the nmap scan, which is used to perform scans on local and remote networks. It can be used to find open ports, network protocols and to identify the operating system a remote machine is operating on. There is also masscan, a TCP port scanner that asynchronously sends SYN packets. It's very similar to nmap, but its flexibility allows for a wider range of settings in regards to ports and addresses. There are multiple other types of scanning tools, but they generally want to meet the same purpose as the previously mentioned ones. Scanning attacks are usually the first step towards building up into a different, more aggressive attack on a network.

Spoofing

Spoofing attacks are used to manipulate an identity by appearing as a trusted identity and infiltrate a network. This is extremely dangerous because personal and sensitive data could potentially be accessed through this attack, as well as leaving the network vulnerable to further attacks. Spoofing takes advantage of trusted relationships and the low security of IoT systems. For instance, spoofing can be achieved by faking an IP or MAC address when communicating with IoT devices due to the wireless nature of their communication. After an attacker successfully pretends to be another trusted device, the network will be prone to a more serious attack such as DoS attacks, or even becoming targeted and vulnerable to future attacks. ARP Spoofing sends malicious messages in a local network by using a valid IP address and connecting it to the MAC address. Once this is done, the attacker can access and modify data that only the owner could've accessed. By providing their own MAC address, attackers could even pretend to be a host and receive the messages being transmitted, and be able to steal a token to fully access applications in the network. Similarly, there are DNS Spoofing attacks where domain names are resolved to IP addresses by pushing corrupted DNS cache information to a host and becoming an impostor with the host's domain name.

Conclusion

The volume of attacks using various security vulnerabilities is expected to grow even higher. By the end of 2020, most of the 26 billion IoT devices do not offer adequate security measures to protect against the ever-growing pool of cyberattacks and threats. In addition, the simplicity of most Web interfaces used in IoT devices makes them quite vulnerable to remote attacks. Although effective security enhancement methods have been proposed for network devices, most of them are not suitable due to the modest computing power of the latter. Moreover, most of these solutions use software that has its own set of problems and vulnerabilities. Consequently, it is critical to explore and, if possible, use hardware support in conjunction with IoT device security software to prevent unanticipated threats. In addition to that, it's very important to educate users about the threats that are available out there so that they can become conscious about the information they share online. Even though the security is the responsibility of the providers and not the users, it's still important to help people understand the importance of their own exposure. It's also important to change the default passwords, and to use very strong passwords. That being said, continuous updating and patching of the devices should be integrated, especially because of user negligence. IoT devices should also be separated in the network into a part with firewalls or other security protocols that protect them. All in all, technology will continue to advance, and as the problem continues to grow, so will the solutions to them.

References

Addeo, E. J. (2021, December 7). *Get to know the internet of things: Definition, applications and more*. devry.edu. Retrieved January 21, 2022, from https://www.devry.edu/blog/internet-of-things-definition-and-more.html

Bajrami, V. (2020, March 31). *Running a quick nmap scan to inventory my network*. Enable Sysadmin. Retrieved January 21, 2022, from https://www.redhat.com/sysadmin/quick-nmap-inventory

Biggs, J. (2016, October 10). *Hackers release source code for a powerful ddos app called mirai*. TechCrunch. Retrieved January 21, 2022, from https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/

Blog: The Mirai botnet - tips to defend your organization. CIS. (2021, July 30). Retrieved January 21, 2022, from https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/

Bursztein, E. (2021, September 20). *Inside the infamous Mirai IOT Botnet: A retrospective analysis*. The Cloudflare Blog. Retrieved January 21, 2022, from https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#toc-2

In *McAfee Labs Threats Report*. Retrieved from https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2017.pdf.

Masscan: Kali linux tools. Kali Linux. (2021, September 10). Retrieved January 21, 2022, from https://www.kali.org/tools/masscan/#:~:text=MASSCAN%20is%20TCP%20port%20scanner,arbitrary%20address%20and%20port%20ranges.

Tsiatsis, V. (n.d.). *Denial-of-service attack*. Denial-of-Service Attack - an overview | ScienceDirect Topics. Retrieved January 21, 2022, from https://www.sciencedirect.com/topics/engineering/denial-of-service-attack

Unicornscan: Kali linux tools. Kali Linux. (2021, September 10). Retrieved January 21, 2022, from https://www.kali.org/tools/unicornscan/#:~:text=Unicornscan%20is%20an%20attempt%20at,IP%20enabled%20device%20or%20network.

What is a spoofing attack? detection & prevention. Rapid7. (n.d.). Retrieved January 21, 2022, from https://www.rapid7.com/fundamentals/spoofing-attacks/