Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2019 Proceedings

Southern (SAIS)

3-22-2019

Botnets: Smart Home User Vulnerabilities and Prevention

Ashley Newsome
University of Tampa, ashleynewsome37@gmail.com

Botnets: Smart Home User Vulnerabilities and Prevention

Ashley Newsome
University of Tampa
Ashleynewsome37@gmail.com

ABSTRACT

Internet of things (IoT) devices are emerging technology and everyday devices used worldwide that puts convenience at our fingertips through the collection and analyzation of our physical environment via the use of sensors and internet-connected devices. But that convenience came with the cost of IoT attacks tripling in number within the first half of 2018 compared to the number of IoT attacks in 2017 (Kaspersky Lab, 2018). In terms of home user devices, there are smart and fitness watches, refrigerators, and home assistants like the Google Home Assistant and the Amazon Echo Dot, and more. Although these devices aide in making life easier, IoT devices are prone to the threats, vulnerabilities, and risks that come with being connected to the Internet. Yet, at the same time, these devices are used to create smart homes. Research by OWASP and Lopez et al. (2018) has shown that there are several security threats to IoT that demonstrate the need to create stronger security practices. This project investigates ongoing research of IoT exploitation, particularly by botnets, to produce simple implementation recommendations and secure practices for home users. The aim of this research is to provide homes users with preventative methods to protect their smart homes and devices, so they do not fall victim to botnets.

Keywords

Botnet, Internet of Things, Smart Home

INTRODUCTION

It is estimated that there are around 23.14 billion Internet of Things (IoT) devices connected worldwide as of 2018 (IHS). That means there are approximately 3 devices per person based on the current worldwide population consensus, which is about 7.5 billion, according to the United States Census Bureau (U.S. Bureau). IoT is a developing technology that uses sensors and devices to improve communication and collect, process, and analyze user data with the concept of IoT being able to allow users to uniquely and ubiquitously identify, access, and control things (Awad and Ali, 2018). This technology exists as virtual assistants, kitchen appliances, security systems, and watches to name a few. They also expand the functionality of the Internet by "increasing the ability to connect multiple devices." (Awad and Ali, 2018) The ability to connect multiple devices benefits users with autonomy and convenience, particularly when they are used to create smart homes. Smart homes are homes that connect multiple internet-connected devices and sensors to achieve remote monitoring, access, and control (remote and local) of a user's residence via a phone or computer (Awad and Ali, 2018; Oxford). The devices promote comfort, convenience, security, and entertainment for a better user experience (Solaimani, Keijzer-Broers, Bouwman, 2013)

IoT devices, like any internet-connected device, present security challenges; and like personal computers, tablets, and smart phones they collect, process, and analyze personal and sensitive information. Unlike devices such as computers, tablets and smart phones, IoT nodes[1] have a resource-constraint nature that does not allow traditional defense practices to be directly enforced (Lopez, Uribe, Cely, Torres, Guataquira, Castro, Marmol, Nespoli, 2018). The lack of traditional defense practices in IoT devices can increase attack surface, which can be used to violate the C.I.A. triad. Attack surface is an element of defense-in-depth that comprises of all the different points an attacker can use to gain access to a system. These points are the reachable and exploitable vulnerabilities (Lopez et al., 2018; Northcutt, 2011). The C.I.A. triad is a measure of security level and represents the principles of confidentiality, integrity, and availability within information security. The goal of the triad is to keep data and information safe from unauthorized users and unauthorized alterations, all the while remaining available to authorized user. The triad can be violated through the exploitation of IoT vulnerabilities, which in turn increases the IoT attack surface.

[1] Node: A member of a network of a point where one or more functional units interconnect transmission lines.

According to Kaspersky Lab IoT report, "in the first half of 2018, IoT devices were attacked with more than 120,000 modifications of malware. That's more than triple the amount of IoT malware seen in the whole of 2017." (Kaspersky Lab, 2018) The significant increase in malware for IoT devices was sparked in 2016 with the Mirai botnet outbreak. A botnet is a network of computers infected with malicious software and controlled as a group without the owners' knowledge, typically used to send spam, perform distributed denial of service attacks, etc. (Oxford) Essentially, the infected device becomes a zombie awaiting orders from the master computer. For example, the Mirai botnet's purpose was to join infected computers together to form a large botnet to launch distributed denial of service (DDOS) attacks. DDOS is a form of denial of service in which a web server or other computer system is maliciously overwhelmed by spurious requests from many computers in different locations on the Internet, in order to make it inaccessible or unusable (Oxford). The devices infected were Linux or Unix-based. The infected devices – routers, IP cameras, DVRs, etc) – took orders using a command and control (C2) server to prevent being monitored. It either awaited commands to launch a DDOS attack or a brute force attack to infect other devices (NJCCIC, 2016; Margolis, Oh, Jadhav, Jeong, Kim, Kim, 2017). IoT technology is growing and, as mentioned earlier, there is a need to strengthen its security. As vulnerabilities remain outstanding for IoT devices, the attack surface will only grow with the development of IoT technology. Other botnets were created after Mirai using similar methods such as Imeij and TheMoon.

The contribution of this paper is as follows:

a) Review existing IoT vulnerabilities.
b) Detailed review about how botnets affect IoT devices and smart homes.
c) Propose simple implementation recommendations and secure practices for home users.
d) Application of proposed implementation recommendations and secure practices for home users.

The remainder of this paper is organized as follows: Literature review discusses smart homes, IoT networks, IoT threats and weaponization, and IoT exploitation. Results discuss in detail the recommendation and secure practices. Methodology describes how the proposal of implementation recommendations and secure practices for home users is created. Conclusion presents relevant conclusions found during research and future works. Finally, appendix shows illustrations found during research that may further some understandings.

LITERATURE REVIEW

Smart home networks are connected through more than just the wireless fidelity (Wi-Fi). Devices can also connect using radio frequency identification (RFID), Bluetooth, near field communication (NFC), internet pool (IP), electronic product code (EPC), and wireless sensor networks (WSN) (Awad and Ali, 2018). Regardless of the connection type, it is important for smart home users to protect their home from within and from outside. An attack from within the home uses technology that already exists in the home using the wired and wireless connections to exploit the vulnerable technology connected to the network. Outside attacks use the gateway to gain access. The gateway is a hardware device such as a router or server, that allows traffic to flow in and out of the network and is connected to the outside service provider by the access network (Chaqfeh and Mohamed, 2015). For example, Chaqfeh mentions that a direct attack on a gateway through Web server or a CGI vulnerability can result in an attack on an entire household. This outside attack is possible because, as stated earlier, the gateway is what allows the flow of traffic in and out of a network. An in-home attack, Chaqfeh also mentioned is "an attacker disguising itself as the internal user through the interactive DTV, IP set top box or home pad or accesses it illegally through other means to control the home appliances (Chaqfeh and Mohamed, 2015)."

Smart homes can be infiltrated in numerous ways. The following list few attacks based on connection used in smart homes (Ali and Awad, 2018; Oxford; Boreli, Gharakheili, Mehani, Sivaraman, Vishwanath, 2015; Breitfuß, Haselsteiner, 2006; Madakam, Ramaswamy, Tripathi, 2015)

Connection	Attacks
Wi-Fi • Any standard for high-speed wireless transmission of data over a relatively short distance	• DoS • Eavesdropping • ICMP flood • Impersonation • Man-in-the-middle
RFID • A form of wireless communication that uses electromagnetic coupling to uniquely authenticate users.	• Cloning • Counterfeiting • Data manipulation • DoS • Eavesdropping • Man-in-the-middle • Physical attacks • Replay • Spoofing
Bluetooth • A radio technology that allows devices such as computers, smartphone, and peripherals to communicate wirelessly over a short range.	• Eavesdropping • Man-in-the-middle • Relay
NFC • A wireless communication interface that allows devices to communicate within a range of about 10cm when either device creates a RF field for the other to receive.	• Data corruption • Data modification • Eavesdropping • Man-in-the-middle
WSN • A wireless network consisting of devices that use sensors to monitor surrounding physical or environmental situations.	• DoS • HELLO flood • Impersonation • Misdirection • Replay • Selective forwarding • Sinkhole • Sybil • Wormhole

Table 1. Types of IoT connections and attacks

The unsecure connection of IoT devices provided to attackers can be weaponized against major organizations and smart home users. For example, in 2016, the Mirai botnet mentioned earlier, played a role in a DDoS and TCP attack against a company called Dyn that provides DNS services to other major companies such as Zillow, Hersey, CNBC, and Soundcloud. The attacks targeted managed DNS infrastructure with the destination port 53. DDoS attacks use DNS protocol, which can make it difficult to determine legitimate traffic from attack traffic. According to Dyn, "the impact of the attack generated a storm of legitimate retry activity as recursive servers attempted to refresh their caches, creating 10-20X normal traffic volume across a large number of IP address. When DNS traffic congestion occurs, legitimate retries can further contribute to traffic volume. We saw both attack and legitimate traffic coming from millions of IPs across all geographies (Hilton, 2016)." The result of successful DDoS attacks can be devastating to an organization. Apart from the interruption of services, successful DDoS attacks can also result in financial loss or negatively affected brands.

According to Ho, "smart homes have a larger and more complex attack surface than existing systems because of the broad range of heterogeneous home devices, the lack of a professional administrator to oversee and maintain these devices, a diverse set of variable and personalized security goals that each home resident might want, and potentially new attack scenarios enabled by cyber-physical, sensor-rich devices (Ho, Leung, Mishra, Hosseini, Song, Wagner, 2016)." Attackers can take advantage of the attack surface by exploiting the vulnerabilities in IoT devices to carry out attacks on the smart home or use the smart home to carry out attacks on a target.

The Mirai botnet was able to spread using a Command and Control (C2) server. When Mirai was able to connect to the server via the infected device, the infected device would scan for other vulnerable devices. Once a victim has been identified, Mirai

would try logging in using brute-force[2] over an SSH and telnet connection. If the device was able to login, it would send the information to another server and the Trojan would be downloaded onto the new device. When this process is complete, Mirai will attempt to conceal itself by deleting binary and "obfuscating its process name in a pseudorandom alphanumeric string (Margolis et al., 2017; Antonakakis, April, Bailey, Berhard, Bursztein, Cochran, Durumeric, Halderman, Invernizzi, Kallitsis, Kumar, Lever, Ma, Mason, Menscher, Seaman, Sullivan, Thomas, Zhou, 2017)." The Mirai botnet were able to spread to hundreds of thousands of IoT devices and attacked other companies such as OVH, Krebs on Security, and Liberia's Lonestar Cell within the span of 4 months (Antonakakis, et al., 2017). Other IoT botnets such as TheMoon and Imeij were created and deployed after the Mirai outbreak.

There is no perfect security solution to completely eradicate attacks like Mirai. However, the spread of Mirai could have been mitigated. Regarding IoT devices, the responsibility lies with both the manufacturer and home users. For instance, remote access is part of the luxury of smart homes. The user can monitor the home while at work or on vacation. But, when home users implement weak passwords or use default passwords, or when manufactures create devices with insecure network services, poor encryption and authentication methods, then remote access can leave a user's devices vulnerable to attack, increasing the spread of malware and the IoT ecosystem's attack surface.

RESULTS

The vulnerabilities found can be grouped into seven security groups: authentication, cryptography, education and training, network security, patch and update, physical security, and user interface (web, cloud, and mobile interface). Each group contains home user defense methods that list ways to defend against its respective vulnerability. The botnet-specific IoT vulnerabilities is comprised similarly. These lists will be further appended and analyzed to create a proposed list of simple implementation recommendations and secure practices for home users. The preposition will then be applied in a controlled home environment. In the process of curating the vulnerabilities of IoT devices and smart homes, methods of securing the devices for IoT manufactures became apparent.

METHODOLOGY

Using current research and literature from databases such as Science Direct and ACM digital Library, a list of known IoT vulnerabilities will be created and botnet-specific IoT vulnerabilities will be created. The methods of exploitation of the vulnerabilities will also be collected. Based on this information, a proposed list of simple implementation recommendations and secure practices will be created. Application of the proposed list will be tested through a simulation of using the proposed list to secure the devices and creating a botnet that will attempt DDoS attacks and possible propagation in a controlled environment. The implementation recommendations and secure practices should be simple enough for any home users to understand and implement, while retaining effectiveness. This will also be tested during the application process of this research.

CONCLUSION

Although there is no perfect security solution, there is still a need for manufactures to improve the security of IoT devices. Smart home security has become the responsibility of both home users and manufactures. Using the proposed implementation recommendations and security practices, smart home users can improve the security of their homes locally and remotely.

REFERENCES

Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors,18*(3), 817.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Zhou, Y. (2017). Understanding the Mirai Botnet. *26th USENIX Security Symposium,*1093-1110.

Chaqfeh, M. A., & Mohamed, N. (2012). Challenges in middleware solutions for the internet of things. *2012 International Conference on Collaboration Technologies and Systems (CTS)*.

[2] Brute-force attack: a repetitive attack that uses combinations of usernames and passwords until access is granted into a site, server, or anything that requires a password.

Haselsteiner, E., & Breitfuß, K. (n.d.). Security in near field communication (NFC). Retrieved from academia.edu.

Hilton, S. (2016). Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog. Retrieved January 01, 2019, from

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart Locks: Lessons for securing commodity internet of things devices. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS 16*,461-472.

IHS. (n.d.). Internet of Things (Iot) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions) [Chart]. In *Statista - The Statistics Portal*. Statista.

Kasperky Lab. (n.d.). New IoT-malware grew three-fold in H1 2018.

López, D. D., Uribe, M. B., Cely, C. S., Torres, A. V., Guataquira, N. M., Castro, S. M., . . . Mármol, F. G. (2018). Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. *Wireless Communications and Mobile Computing,2018*, 1-18.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications,3*, 164-173. doi:10.4236/jcc.2015.35021

Margolis, J., Oh, T. (., Jadhav, S., Jeong, J. (., Kim, Y. H., & Kim, J. N. (2017). Analysis and Impact of IoT Malware. *Proceedings of the 18th Annual Conference on Information Technology Education - SIGITE 17*.

Meyers, M. (2015). *CompTIA network certification exam guide: Exam N10-006*. New York: Mcgraw Hill Education.

New Jersey Cybersecurity and Communications Integration Cell. (n.d.). Mirai. Retrieved September 07, 2018, from

Northcutt, S. (n.d.). The Attack Surface Problem.

Oxford University. (n.d.). ESEARCH.

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*.

Solaimani, S., Keijzer-Broers, W., & Bouwman, H. (2013). What we do – and don't – know about the Smart Home: An analysis of the Smart Home literature. *Indoor and Built Environment,24*(3), 370-383. doi:10.1177/1420326x13516350

U.S. and World Population Clock. (n.d.).