Smarthome increased reliance on the internet of things: issues in security

Introduction

The Internet of Things (IoT) plays a significant role among many Smarthome consumers today. It is no secret that Smarthome technology affords many households the ease and convenience of interaction through the process of automation. Many household consumers make use of the technology to assist with everyday functions such as enabling alarm sensors, appliances and security cameras to name a few. Unfortunately, Smarthome environments are increasingly on the radar of hackers as a growing number of consumers embrace these devices in their homes (Yoon, Park & Yoo, 2015). From the consumers vantage point looking out this may appear to be advantageous; however, from a threats perspective looking in, this is a potential goldmine as multiple access point inside a home area network (HAN) may be available. Malicious actors can exploit the consumer's benefits from using this technology by unlocking a diversity of potential security challenges and issues. The evolving reliance and interconnectivity of the IoT leaves open security and safety vulnerabilities where each attached device to include access to a HAN is susceptible to an attack or misuse (Lin & Bergmann, 2016).

Problem Statement

Over the last decade, there has been an exponential growth concerning the dependency on the Internet of Things. Today, by some estimates, there is in excess of 18 billion connected devices related to the IoT (Wei, Yan, Anni & Yuqing, 2019). This approximation is composed of both enterprise clients and consumers, which accounts for roughly 80 percent of this usage. This is an

increase of more than 20 percent over last three plus years (Wei, Yan, Anni & Yuqing, 2019). These numbers will expectantly increase as more and more households are transitioning to Smarthome enabled technologies. As a result, the security implications surrounding the growing dependency on the IoT will increase proportionally.

Since advancements within the IoT will continue to flourish and continuously attract more clients and consumers, the security implications will only manifest even further as threats continue to explore new opportunities to exploit the vulnerabilities. Perhaps, the only methods to adequately address the growing security concerns are for clients and consumers to sufficiently manage the number of connected devices by removing nonessential assets, ensure the latest and most up-to-date security solutions are in practice, or lastly, an-all-out flat disconnect from the IoT. In either case, it is imperative for Smarthome consumers to evaluate the risk from utilizing the IoT in order to make informed decisions.

Purpose Statement

The purpose of this paper is to explore and highlight the growing and overarching security concerns, issues and challenges that exist due to the increased dependency on the IoT in Smarthome environments. It will examine the need for next generation tools, techniques and practices to minimize the effects of nefarious actors and threats. While the Internet of Things provides efficiency and convenience for Smarthome environments through automation and interoperability, the adverse security implications have escalated due to the growing dependency on the Internet of Things.

Research Questions

This study looks to answer the following research questions:

1. What are the current security concerns and challenges that can affect smart home clients and consumers within the Internet of Things?
2. How can clients and consumers increased dependency on the Internet of Things heighten current security concerns and threats in smart home environments?
3. How can current security threats benefit from exploiting clients and consumers increased dependency on the Internet of Things in smart home environments?

Significance of study

The study will examine and give credence to the security implications regarding Smarthome clients and consumers deep reliance on the IoT. It is imperative to understand the risk and vulnerabilities that accompany the steady increase of interconnecting multiple devices in a Smarthome environment. By doing so, this potentially gives threats a collective number of avenues into an active network; subsequently, these threats are able to access and expose sensitive and private information. The study will bring this understanding to the most novice of IoT consumers and clients; provide fundamental knowledge and awareness of current security concerns, threats and best approaches to minimize exposure. This study will also exhibit the need for future research and development efforts and methods to strengthen smart device protocol standards and advance the quality of device security measures.

Definition of Terms

- CONSUMER/CLIENT: Persons who uses the IoT for services.
- ESP: Encapsulating Security Payloads provides confidentiality, integrity & authenticity.
- HAN: Home Area Network, network or networks within a consumer's household.
- HTTPS: Hyper-Text Transport Protocol Secure provides secure C2C communications.
- IoT: Internet of Things, provides interconnection of computing devices.
- IPS: Internet Protocol Security authenticates and data packets sent over the web.

References

- Conti, M., Dehghantanha, A., Franke, K. & Watson, S. (2017). Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems Journal* , *78* (2), 544-546. doi: 10. 1016/j. future. 2017. 07. 060
- Kumar, S. K., Vealey, T. & Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Direction: *49th Hawaii International Conference on System Sciences (HICSS).* Koloa, HI. IEEE.
- Lin, H. & Bergmann, N. W. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *School of Information Technology and Electrical Engineering, 7* (3), 1-15. doi: 10. 3390/info7030044
- Wagay, A. P. & Mohiuddin, K. (2017). Internet of Things: Security Challenges. *International Journal of Engineering Research in Computer*

Science and Engineering, 4 (12), 283-290. doi: 01. 1617/vol4/iss12/pid71605

- Wei, Z., Yan, J., Anni, P. & Yuqing, Z. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal, 6* (2), 1606-1616. doi: 10. 1109/JIOT. 2018. 2847733
- Yoon, S., Park, H. & Yoo, H. S. (2015). Security Issues on Smarthome in Internet of Things Environment. *Computer Sciences and its Applications* . (pp. 691-696). doi: 10. 1007/978-3-662-45402-2_97