Security in IoT for Smart Home Environment: Challenges and Approaches

A Methodological Review

Duy Thuc Pham (101767225)

Faculty of Science, Engineering, and Technology, Swinburne University

Hawthorn, Australia

101767225@student.swin.edu.au

# INTRODUCTION

The increasing rapidly of the Internet of Things (IoT) recently leads to the development of IoT appliances in many areas including smart home systems (SHSs). SHSs are a group of IoT devices which are used to help householders in lighting control, climate control, entertainment and safety systems via a home network (Lee et al. 2014, p. 67). With the support of SHSs, the smart home is now more comfortable and secure for householders to live as well as control the energy consumption efficiently. Nevertheless, due to the heterogeneous hardware, software and the precious privacy user data, SHSs become a target to attack by many malicious actors (Song et al. 2017, p. 1844).

The purpose of this paper is to address some research methods that have been conducted in the security of SHSs. Thereby, it will identify the limitation of these methods so that the future researcher can apply the research method effectively.

# REVIEW OF RELATED WORKS

## Security Communication Protocols

One of the main challenges in the security for SHSs is heterogeneous communication protocols (Lee et al, 2014), which intruders may take advantage of this to retrieve privacy information. In the work of Ling et al (2017), they conduct a case study on a Edimax SP-2101W – a popular smart plug system - to investigate its communication protocol, and then four attacks: device scanning attack, brute force attack, spoofing attack; and firmware attack were simulated to test the security of the smart plug device. They propose the architecture of smart home plug system including three components: smart plugs, controllers; and remote cloud servers for the experiment. Also, in order to improve the security, the smart plug systems and controllers are authenticated with a cloud server on EC2 instance. The experiment was setup

## Risk Analysis

# REferences reviewed

1 Ali, B & Awad, A 2018, ‘Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes’, *Sensor*, vol. 18, no. 3, p. 817.

2 Jacobsson, A, Boldt, M & Carlsson, B 2016, ‘A risk analysis of a smart home automation system’, *Future Generation Computer Systems*, vol. 56, pp. 719-733.

3 Ling, Z, Luo, J, Xu, Y, Gao, C, Wu, K & Fu, X 2017, ‘Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System’, *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899-1909.

4 Song, T, Li, R, Mei, B, Yu, J, Xing, X & Cheng, X 2017, ‘A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes’, *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844-1852.

5 Halabu, D, Hamdan, S & Almajali, S 2018, Enhance the Security in Smart Home Applications based on IOT-CoAP protocol, *IEEE*, Beirut, Lebanon, pp. 81-85.

# references consulted

6 Conti, M, Dehghantanha, A, Franke, K & Watson, S 2018, Internet of Things security and forensics: Challenges and opportunities, *Future Generation Computer Systems*, vol. 78, pp. 544-546.

7 Han, J-H, Jeon, Y & Kim, J, ‘Security Considerations for Secure and Trustworthy Smart Home System in the IoT Environment’, *International Conference on ICT Convergence 2015,* ICTC 2015, pp. 1116-1118

// double check 8 Leedy, P & Ormrod, J 2015, ‘Practical Research: Planning and Design’*, Global Edition*, 11th ed, Pearson, Boston.

// 9 Zaidan, A, Zaidan, B, Qahtan, M, Albahri, O, Albahri, A, Alaa, M, Jumaah, F, Talal, M, Tan, K, Shir, W & Lim, C 2018, ‘A survey on communication components for IoT-based technologies in smart homes’, vol. 69, no. 1, pp. 1-25.

10 Lee, C, Zappaterra, L, Choi, K & Choi, H-A 2014, ‘Securing Smart Home: Technologies, Security Challenges, and Security Requirements’, *IEEE Conference on Communications and Network Security,* CNS 2014, pp. 67-72.