Security in IoT for Smart Home Environment: Challenges and Approaches

Duy Thuc Pham (101767225)

Faculty of Science, Engineering, and Technology, Swinburne University

Hawthorn, Australia

101767225@student.swin.edu.au

I. INTRODUCTION

The application of the Internet of Things (IoT) has been widely used in the smart home environment recently. The term Smart home systems (SHSs) consists of multiple applications such as lighting control, entertainment, climate control and safety system, which communicates with each other via a home network (Lee et al. 2014, p. 67). The emergence of SHSs not only supports householders control the energy consumption, but it also brings more comfort and security.

However, the rapid advancement of SHSs has caused the increment of many security vulnerabilities including privacy, access control and secure communication (Conti et al. 2017, p. 544). Furthermore, due to lack of consideration of security in SHSs, many SHSs become the target for malicious actors (Song et al. 2017, p. 1844). More importantly, the intrusion may cause several severe cases such as leakages of user data, economic losses and a risk of human life (Han et al. 2015, p. 1116). Therefore, the purpose of this paper is to offer some insight into the security challenges and security solutions of SHSs by reviewing academic journals from the past.

The following review of literature starts by briefly discussing an overview of security in existing SHSs. Thereby, it addresses the need for security and privacy in SHSs. Then, the current security challenges of SHSs are reviewed to highlight barriers in integrating security to SHSs. Last but not least, the review presents two security approaches using security architectures and risk analysis methods to improve the security in existing SHSs and increase the awareness of security for IoT manufactures.

II. REVIEW METHOD

The reviewed articles in this review have been found on the database Scopus and IEEE. In the Scopus database, search term was “security in IOT smart home systems” and the subject area was “computer science” and publication from 2014 to present. Then, the result list was sorted based on the highest cited. After filtering the literature, 11 articles were selected to evaluate. The selection procedure was similar to IEEE databases, and consequently 2 journal articles and 2 conferences article were chosen.

After evaluating 15 articles, there were 6 relevant articles selected to review and 2 articles used as consultant references. In this review, 6 selected articles were grouped in to 3 groups: security challenges, security architectures and risk analysis methods. The journal article of Lin

& Bergmann (2016) mentioned both security challenges and security architectures, so it was used in two sections. Thereby, 2 articles were used to discuss the security challenges, 3 articles were used for security architectures, and 2 other articles were used for risk analysis methods.

III. REVIEW OF RELATED WORKS

A. Domain Overview

The cybersecurity and privacy requirements for SHSs are incredibly significant, due to the private user information that they contain (Song et al. 2017, p.1846). Even though the data tends to be harmless like the information of the smart heater, they could be used to check the availability of householders, and thus thefts can enter the house for burglary (Lin & Bergmann 2016, p. 44). Furthermore, the interaction over the insecure household network makes SHSs vulnerable to be attacked by malicious actors. Therefore, there is a need to deeply understand security challenges and also identify security approaches to help mitigate impacts and protect users.

Security challenges are some vulnerabilities and difficulties that currently exist in SHSs. For example, in smart home environment users are typically inexperienced in monitoring the network, and hence the intruders can access the home appliances such as cameras, doors, lights to retrieve the information of users.

Security approaches are some countermeasures or solutions that could help prevent potential intrusions or improve the security for SHSs. This paper provides two security approaches: security architectures, risk analysis methods. Security architectures are some recent architectures including encryption protocol, symmetric key and security model that have been used to improve the security for SHSs. Whereas, the risk analysis methods are those methodologies, which are used to evaluate possible risks in current SHSs so as to increase the awareness of security while developing IoT devices.

B. Security Challenges

The SHSs are different from other IoT environments, due to the heterogeneity of devices, manufactures and also an insecure of network infrastructure. Lee et al. (2014) address the necessity of identifying security challenges so that they establish the main security requirements for smart home devices. Their investigation is to conduct a test on some of the current SHSs including the Nest Learning Thermostat, Nest Smoke Detector, Samsung Smart TV, etc. As the result, based on their analyses, five main challenges: resource constraints, heterogeneous communication protocols, unreliable communication, energy constraints, physical access are identified. They conclude that the limitation of resources and energy is the main challenge of SHSs, and thus existing sensors and detectors are not able to implement the security algorithm (e.g. RSA; ECC). Although the authors provide the specification of the analyzed sensor, the evidence is not sufficient. Since the testing was conducted in 2004, and thus this sensor is apparently outdated.

The finding of Lin & Bergmann (2016) in 2016 was not similar to what Lee et al. (2014) found in last 12 years. They agree with Lee et al. (2014) that system resources and energy constraints are two of the main challenges of SHSs. However, they assert there are plenty of challenges that the last work did not indicate such as networked system accessibility, system physical accessibility, system heterogeneity, fixed firmware and slow uptake of standards. Noticeably, Lin and Bergmann identify the greatest challenge a human factor, since there are no security professionals to operate the smart home network, and thus householders cannot afford to control their home network. A good merit of this paper is to provide a practical vulnerability example regarding how home surveillance cameras may be attacked by using Shodan – an IoT search engine, and thus the authors want to alert householders not to trust on SHSs.

C. *Security Architectures*

The need for having an effective security architecture to help mitigate risks in SHSs has been increased recently due to the advance of IoT. Song et al. (2015) identify the current architecture and design in SHSs may have some security and privacy issues, which can lead to the leakage of user's privacy information containing in smart home devices. Therefore, the authors offer a new security architecture for smart home appliances with four groups: appliance group, monitor group, central controller group and user interfaces. This paradigm is an IoT cloud-based architecture, in which the central group is the server deploying in the cloud. Despite believing the new architecture is more secure than existing SHSs, authors doubt that it can be intruded by some malicious software and firmware. Hence, Song et al. (2015) recommend using a chaos-based cryptographic scheme along with message authentication codes (MAC) while transmitting data between OSI layers so as to reduce security threats. The main contribution of the paper is to provide a privacy-preserving communication protocol algorithm in order to ensure the confidentiality, availability and integrity as well as reduce the possibility of leaking user information in the SHSs. However, in order to use the complex computational to generate chaos-based cryptographic, these devices should have an adequate hardware specification. Hence, their approaches are not sufficient with existing SHSs (e.g. sensors; and detectors), due to the resource limitation.

A variety of security problems of cloud-based architecture have pointed out the need for rigorous analysis of the security of this architecture. In the investigation of Ling et al. (2017), they prove that despite using the cloud-based architecture with the MD5 hashing algorithm, attackers can obtain the credential including the user account and password by using spoofing attack. The test was conducted with Edimax SP-2101W - the common smart plug device and a remote authentication server deploying in Amazon Web Services. Based on their analysis, they assert that the success rate increases with the speed of the transmission. In other words, if 1010 spoofed packets are sent in 3 minutes, there is higher than 90% that the user account and password are stolen. So, the paper offers some defence strategies such as using the secure communication protocol, mutual authentication between devices and server, intrusion detection system, anti-bot mechanism and data-integrity to improve the improve the security of SHSs as well as mitigate the vulnerabilities. However, Ling et al. (2017) do not provide an effective architecture to improve the current security architecture for SHSs. Therefore, Lin & Bergmann (2016) suggest replacing cloud-based architecture with the gateway architecture for SHSs. Since they assert the Internet for home appliances is not able to guarantee a high-speed, low-latency and availability, and thus intruders can use denial of service attacks to disrupt the system. The IoT gateway is relatively the bridge between local IoT infrastructure and the cloud. It defences home appliances from intrusions by acting as a firewall. Additionally, it requires the authentication of all SHSs before transmitting data to the cloud, and thus it ensures there are no suspicious devices in the network. This paper also addresses the need for technical support in the SHSs. Thus, they require the IoT devices should have web-services to support auto-configuration and automatic firmware updates, so as to patch security problems and mitigate potential security risks before it may harm the privacy information of users.

D. Risk Analysis Methods

The heterogeneity of SHSs has addressed the importance of identifying possible risks that could harm householders. In the work of Jacobsson et al. (2016) they find out 32 risks that can occur in home appliances. Their research method is to examine 6 groups within the gateway architecture: 1) connected sensors, 2) in-house gateway, 3) cloud server, 4) API, 5) mobile devices and 6) mobile applications with five factors: software, hardware, information, communication protocols and human actors in smart home devices. As a result, they identify the highest ranked risk to be lack of access control configuration in the gateway device, which is caused by human factor. Therefore, Jacobsson et al. (2016) focus on the need of applying Information Security Risk Analysis (IRSA) method in the design and development phase to rigorously evaluate any potential impacts. The authors claim that IRSA not only helps identify many risks and vulnerabilities of SHSs in development but also help prevent and mitigate the identified risks. The strong point of the paper is to propose a model of security, which includes developers and security experts along with IRSA, to highlight the level of awareness of privacy of the IoT community as well as manufactures. Although the literature indicates many risks that likely occur in SHSs, it does not provide any practical approaches to help mitigate these risks. Furthermore, the involvement of security experts in development phase apparently increases the cost of developing SHSs.

The emergence of new smart home devices leads to the growth of new security risks. In 2018 Ali & Awad (2018) offer a new risk analysis method known as OCTAVE Allegro (OCTAVE) to improve the existing method and also provide new solutions to prevent the potential risks. The method includes four major phases: establishing drivers phase, profiling assets phase, identifying threats phase, risk-mitigating phase. The first two phases initiate the list of risk measurement criteria and boundaries for logical, technical, physical and people assets. The last two phases are to find the threats based on these identified criteria and decide the mitigation strategies. Ali & Awad (2018) pointed out 15 security risks based on 10 critical cyber from real-world examples. Thereby, they propose some countermeasures such as applying biometrics or multi-factor to improve the level of authentication, using an intrusion detection system and setting up virtual private networks. Although the article rigorously analyzes the security risks in existing SHSs, authors address the necessity of further study to develop a framework to identify and analyze security risks for household appliances.

IV. CONCLUSIONS

The IoT devices in smart home environment are containing many security vulnerabilities and threats. The review has identified some of the main challenges as well as pointed out that the human factor is the biggest challenge in SHSs. Therefore, the need for improving the awareness of householders, developers and manufacturers in term of security is important.

To improve the security and prevent potential threats from malicious malware and software, the review has found out the comprise of the gateway architecture and web services for auto-configuration and automatic firmware updates. The gateway architecture cannot ensure the security of SHSs if the firmware of devices is not updated to patch and fix issues regularly.

In addition to the gateway architecture, the risk analysis method should be applied to find out appropriate countermeasures for mitigating the security risks. The OCTAVE method is best suited to be chosen as the risk analysis method, as it is more effective than IRSA in terms of cost and risk measurement criteria. Although the review has pointed out some existing security challenges and security approaches, further research is needed to address new unseen security challenges and to develop effective security solutions for protecting SHSs in the future.

Word Count: 2161

V. REFERENCES REVIEWED

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

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.

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.

Lin, H & Bergmann, N 2016, ‘IoT Privacy and Security Challenges for Smart Home Environments’, *Information*, vol. 7, no. 3, p. 44.

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.

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.

VI. REFERENCES CONSULTED

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.

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