Security in IoT for Smart Home Environment

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, the pros and cons of these methods will be analyzed so that the future researcher can learn from it to select the sufficient research method for their research.

# REVIEW OF RELATED WORKS

This review method paper will evaluate five articles related to two security solutions for SHSs – which are secure communication protocols and risk analysis methods. In the communication protocols section, with an aim to research the effective communication protocol, three research papers with two methods: a case study and experimental method will be reviewed. Besides, two risk methods applied focus group method to identify security threats and vulnerabilities in SHSs will be reviewed in the risk methods section.

## Communication Protocols

One of the main challenges in the security for SHSs is heterogeneous communication protocols (Lee et al, 2014), by which intruders may take advantage of this to retrieve private information. In the work of Ling et al (2017), they focus on a case study of an Edimax SP-2101W – a popular smart plug system. The authors conducted two experiments in this case study. While the purpose of the first one is to exploit the communication protocol of the smart plug system, the other is to test the security of this communication protocol when being attacked in real-world.

The authors conduct the first exploratory experiment in three phases: the smart plug registration phase, the authentication phase; and communication phase with three components: smart plugs, smartphones; and cloud servers. They observe and record the data rigorously and then interpret the data as a narrative so that researchers are able to gain insight into how this communication protocol actually works in reality. The next experiment is to evaluate the security of the smart plug system by simulating four attacks: device scanning attack, brute force attack, device spoofing attack; and firmware attack. They conduct this experiment on five Edimax plugs deploying overseas and connecting them to the Internet. The authors respectively walk through each attack and observe how these smart plugs response. Consequently, from their analysis, the data is narratively presented to explain their experiment in detail.

The strong merit of this case study is to show how the communication protocol of the smart plug system works in detail. Also, the result of four simulated attacks addresses some existing limitation of the communication protocol in the smart plug system. Although the case study of a smart plug system provides in-depth knowledge about the security of the smart plug system, the major drawback of this method is that the findings of a single case cannot be used in other cases (Leedy & Ormrod 2015). Therefore, it is obvious that the smart plug system cannot portray for all SHSs, and hence the communication protocol of smart plug system cannot work for other SHSs e.g. smart lights, smart TVs, etc.

While variables are hardly controllable in the case study method, they can be controlled by the researcher in experimental method (Leedy & Ormrod 2015). In addition, the results of the experiment can be generalized to larger populations. In an effort to enhance the security in SHSs, Halabu, Hamdan and Almajali (2018) performed a one-shot experiment on three types of hash function: SHA-1, SHA224; and SHA256 based on CoAP protocol. The purpose of this experiment is to identify the hash function that best suited to CoAP protocol in term of execution time and energy consumption. The authors apply three hash functions to 6 simulated sensors and connect to one controller over the CoAP protocol. Thereafter, they use a software Contiki os to evaluate the enhanced protocol and collect the data with regards to power consumption and execution time. Based on data analysis, they conclude SHA224 is the most appropriate hash algorithm in the CoAP protocol.

However, this experiment has some issues with the dependent variables and thus it impacts results as well. Leedy and Ormod (2015) assert that one shot experiment’s results are meaningless due to low internal validity. To illustrate in the paper of Halabu, Hamdan and Almajali (2018), though the authors aim to enhance security in SHSs, instead of choosing the security of these hash functions as a primary dependent variable, the authors select energy consumption and execution time. Therefore, the result cannot illustrate whether the SHA224 can improve the security of SHSs better than two other hash functions or not.

The experiment of Song et al (2017), however, is considered to be more sufficient than the research of Halabu, Hamdan and Almajali (2018). In an attempt to propose a new communication scheme for SHSs, the authors conduct an experiment on two privacy preserving schemes: hash function-based and chaos-based to evaluate the security and performance. Firstly, the authors set up the testing environment including an appliance group, a monitor group and central controller. In other words, the appliance group is smart home appliances such as smart TV, thermostat, etc. Meanwhile, the monitor group is sensors and detectors; and the central controller is the server. Thereafter, they propose in detail two privacy preserving schemes inclusive with algorithms to implement them in both client and server side. On the one hand, in order to test the security strength of two privacy preserving schemes with regards to confidentiality, data integrity and availability, the authors simulate an eavesdropping attack. Based on their security analysis, two privacy-preservation ensure the communication protocol of SHSs is highly protected. On the other hand, the performance evaluation is analyzed with respect to computational complexity and communication overhead. Consequently, according to the analysis data, they conclude that the chaos-based scheme is more efficient than a hash-function to use as a privacy-preservation scheme in communication protocols in SHSs.

Overall, the lack of attempt to study the similarity of the hash-function scheme and the chaos-based scheme is the major limitation in the static group comparison experiment of Song et al (2017). Firstly, there is a question on whether they are similar before the test Leedy and Ormod (2015). Secondly, the possibility of generalization this experiment in different cases could be a challenge for future researchers. Nevertheless, compare to the method of Halabu, Hamdan and Almajali (2018), the results are more valid and reliable. The testing environment was introduced rigorously; independent variables and dependent variables were sufficient with the purpose of the experiment, and thus the results ensured the validity of the research method.

## Risk Analysis Methods

Risk analysis method is one of the security enhancement for SHSs since it helps identify potential security vulnerabilities, and thus IoT manufacturers can find countermeasures to mitigate the problems. With the aim is to estimate the probability of threats in SHSs, Jacobsson et al. (2016) conduct a focus group questionnaire including security experts, domain experts and system developers of SHSs. The procedure starts by separating the gateway architecture into six components: connected sensors, in-house gateway, API, mobile devices; and mobile device app. They analyze each component of the architecture with hardware, software, information, communication and human respectively to find out related threats. Thereafter, they set up two collaborative workshop sessions and invite nine persons in each workshop. After that, these participants need to rate the probability of these identified threats from unlikely/negligible to likely/disastrous in a five-level scale. After gathering exploratory data from the open questionnaire, the authors derive three intensity classes: low, medium and high. As the result, 32 risks are found, in which 4 risks are classified as high, 9 as low and 19 as the medium.

In recent research, Ali and Awad (2018) propose a new risk analysis for SHSs which applies the OCTAVE Allegro method. The research method is almost the same as the method of Jacobsson et al. (2016), but instead of collecting data from the technical group (security experts, developers, etc.), it creates an analysis team including the multidisciplinary people throughout the organization (Caralli et al 2007). Moreover, the procedure to collect data is slightly different from Jacobsson et al. (2016). In the OCTAVE Allegro method, the analysis team not only answer the open-ended questionnaire but also, they have to identify information assets and threats scenarios in worksheets. Finally, based on 10 critical information assets identified from the analysis team and risk analysis process, the authors find out 15 security risks in SHSs and also propose appropriate mitigation solutions.

Overall, the focus group questionnaire method in two research methods helps researchers thoroughly investigate the risks that exist in SHSs, since Hesse-Biber and Leavy (2011) assert that focus group is helpful for researchers to explore issues surrounding the topic, especially when the knowledge about the topic is little. Another advantage of the focus group is that it collects empirical data simultaneously from multiple participants. Furthermore, they can help each other to understand questions, and thus the accuracy of data may be slightly improved. Nevertheless, it is apparent that the cost is high in two research papers due to the fee for workshops, participants and preparing the questionnaire. The method of Jacobsson et al. (2016) is not only better than the work of Ali and Awad (2018) in terms of cost and time but also the number of risks that they identified is higher. It is because Jacobsson et al. (2016) apply the focus group method more sufficient than method of Ali and Awad (2018). First, they select a minority group having some common characteristics (security expert, system developer and domain expert) which is suitable with the fundamental of the focus group (Hesse-Biber & Leavy 2011). Second, the technician group can identify significant risks efficiently.

# Conclusion

In this method review paper, five papers have been reviewed with regards to the security solutions for SHSs. Three papers conduct a qualitative research method to collect data like a case study and focus group, while two papers conduct an experiment to gather quantitative data. Although each of them has some pros and cons, depends on the aim and research context, the researchers can apply it appropriately to answer critical questions. A recommendation of Chowdhury (2015) is that the combination of the qualitative and quantitative method can improve the quality of the research method. As Chowdhury (2015) state the weakness of qualitative method can be compensated by the strength of the quantitative method and vice versa. However, regardless of research methods that researchers apply, the validity and reliability of results must be ensured in order to help further research.

# 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.

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.

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.

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.

# references consulted

Caralli, R.A, Stevens, J.F, Young, L.R. & Wilson, W.R, ‘Introducing Octave Allegro: Improving the Information Security Risk Assessment Process’, *Technical Report CMU/SEI-2007-TR-012*, Software Engineering Institute: Pittsburgh, PA, USA, 2007.

Chowdhury, M 2015, Coding, sorting and sifting of qualitative data analysis: debates and discussion. *Quality & Quantity*, vol. 49. no 3, pp.1135-1143.

Hesse-Biber, S & Leavy, P 2011, *The practice of qualitative research*, 2nd ed, SAGE Publications, Los Angeles, pp. 163-191.

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.

Leedy, P & Ormrod, J 2015, *Practical Research: Planning and Design,* Global Edition, 11th ed, Pearson, Boston.