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

# INTRODUCTION

// 200 words

The advancement of IoT in smart home environment recently ask the

# REVIEW METHOD

// 100 words

# REVIEW OF RELATED WORKS

## Domain Overview

## Security Challenges

The heterogeneous devices and manufactures cause the vulnerabilities in smart home systems [], and thus it is crucial to identify security challenges for smart home systems to find some effective countermeasures for protecting users.

The authors claim that due to the significance of the private information containing in smart home systems, security requirements for them is essential. In order to identify the main challenges and threats in smart home systems, authors conduct a test to some of the smart home systems including Nest Learning Thermostat, Nest Smoke Detector, Samsung Smart TV, etc. Consequently, based on the analysis, they found out five main challenges in smart home systems: resource constraints, heterogeneous communication protocols, unreliable communications, energy constraints, physical access. They claim that the limitation of resource and energy are the main challenges for smart home systems. A strong merit of this article is to conduct an investigation of existing security threats in each OSI communication layer. Thereby, the authors asserted the need for further study to mitigate the attack from the malicious firmware.

Lin and Neil W.Bergmann2016 report that even though smart home systems are able to bring more comfort, security and ecological sustainability, there are plenty of challenges in smart home systems (SHS). They show that these challenges come from many factors such as networked system accessibility, system physical accessibility, system resources, system heterogeneity, fixed firmware and slow uptake of standards. Noticeably, they consider the most challenges to be 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. In addition, a practical vulnerability example regarding how home surveillance cameras may be attacked by using Shodan – an IoT search engine – is provided to alert householders not to trust on smart home systems. However, the lack of quality data for each vulnerable factor in this research article makes these arguments less persuadable.

## Security Architectures

The need for having an effective security architecture to help mitigate risks in smart home system has been increased recently due to the advance of IoT. Tianyi Song, Ruinian Li identify the current architecture and design in smart home systems may have some security and privacy issues, which can lead to the leakage of user’s privacy information containing in smart home systems. 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 cloud. Despite believing the new architecture is more secure than existing smart home systems, authors doubt that it can be intruded by some malicious software and firmware. Hence, they 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 smart home systems. However, in order to use the complex computational to generate chaos-based cryptographic, smart home systems should have an adequate hardware specification. Hence, their approaches are not sufficient with existing smart home systems (e.g. sensors; and detectors), due to the resource limitation.

A variety of security problems of cloud-based architecture have pointed out the need of rigorously analysis the security of this architecture. In the investigation of Zhen Ling and Junzhou Luo, they prove that despite using the cloud-based architecture with 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 successful 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 is stolen. So, the paper offers some defense strategies such as using 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 smart home systems as well as mitigate the vulnerabilities. However, the need for a new architecture is not indicated in the literature. Lin and Neil W. Bergmann 2016 believe that cloud-based architecture should be replaced by a new architecture. Because 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. Len and Neil suggest using gateway architectures for smart home systems. The IoT gateway is relatively the bridge between local IoT infrastructure and the cloud. Additionally, it requires the authentication of all smart home systems before transmitting data to the cloud as well as it defenses home appliances from intrusions by acting as a firewall. The most interesting part of this paper is to address the need of technical support in smart home system. Therefore, they require the IoT devices should have an auto-configuration and also the regular firmware updates, so as to patched security problems and mitigate potential security risks before it may harm the privacy information of users.

## Risk Analysis Methods

The heterogeneity of smart home systems has addressed the importance of identifying possibility risks that could harm householders. In the work of Andreas Jacobsson, Martin Boldt, the find out 32 risks that can occur in smart home systems. 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 the result, they identify the highest ranked risk is lack of access control configuration in the gateway device, which causes by human factor. Therefore, they focus on the need of applying Information Security Risk Analysis (IRSA) method in design and development phase to rigorously evaluate any potential impacts. The authors claim that IRSA not only help identify many risks and vulnerabilities of smart home systems 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 include 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 smart home systems, it does not provide any practical approaches to help mitigate these risks.

The emergence of new smart home devices leads lead to the rise of new security risks. In 2018 Bako Ali and Ali Ismail 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.

# CONCLUSIONS

// 250 words

# REferences reviewed

# references consulted