REPLAY ATTACK ON BLUETOOTH COMMUNICATION WITH SOFTWARE DEFINED RADIO IN THE IOT BASED SMART HOME

AHMAD FUDHAIL IYAD BIN MOHD ZAINUDIN

MASTER OF SCIENCE
(COMPUTER SCIENCE)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2022

REPLAY ATTACK ON BLUETOOTH COMMUNICATION WITH SOFTWARE DEFINED RADIO IN THE IOT BASED SMART HOME

AHMAD FUDHAIL IYAD BIN MOHD ZAINUDIN

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Master of Science (Computer Science)

2022

ABSTRACT

- IoT smart home devices make it easier for people to monitor their home just by checking on their smartphones. Rather than physical risk, connecting smart home devices to the internet results in new security and privacy problems, such as confidentiality, integrity and authenticity of data exchange by the devices. Smart home devices are highly vulnerable to different security attacks that make a smart home unsecure to live. Therefore, it is necessary to evaluate the security risks to judge the situation of smart home devices. As homes are increasingly computerized and smart home devices being widely used, potential security attacks and their impact need to be investigated. The methodologies used in this report are implemented and design from OWASP Firmware Testing Methodology and OCTAVE aimed at two stages of replay attack which are Preliminary attack and Revamp attack of the chosen smart home devices: Hampton Bay Smart Doorbell and Wi-Fi August Smart Lock and conducting security analysis based on proposed penetration testing guideline. The research finds that the Hampton Smart Doorbell is vulnerable towards both preliminary and revamp stage while the Wi-Fi August Smart Lock is secured towards both attacks conducted. The findings in this thesis will assist in detecting vulnerabilities in smart home devices system when it comes to the specification of security criteria.

Keywords: Internet of Things (IoT), Smart Home Device, Smart Doorbell, Smart Lock, Detecting Vulnerabilities, Penetration Testing Guideline, Replay Attack.

ABSTRAK

- Peranti rumah pintar IoT memudahkan orang ramai memantau rumah mereka hanya dengan menyemak telefon pintar mereka. Daripada risiko fizikal, menyambungkan peranti rumah pintar ke Internet mengakibatkan masalah keselamatan dan privasi baharu, seperti kerahsiaan, integriti dan ketulenan pertukaran data oleh peranti tersebut. Peranti rumah pintar sangat terdedah kepada serangan keselamatan yang berbeza yang menjadikan rumah pintar tidak selamat untuk didiami. Oleh itu, adalah perlu untuk menilai risiko keselamatan untuk menilai keadaan peranti rumah pintar. Memandangkan rumah semakin berkomputer dan peranti rumah pintar digunakan secara meluas, potensi serangan keselamatan dan kesannya perlu disiasat. Metodologi yang digunakan dalam laporan ini dilaksanakan dan reka bentuk daripada Metodologi Pengujian Perisian Tegar OWASP dan OCTAVE bertujuan untuk dua peringkat serangan ulangan iaitu serangan awal dan serangan Ubahsuai peranti rumah pintar yang dipilih: Loceng Pintu Pintar Hampton Bay dan Wi-Fi August Smart Lock dan menjalankan analisis keselamatan berdasarkan garis panduan ujian penembusan yang dicadangkan. Penyelidikan mendapati bahawa Loceng Pintu Pintar Hampton terdedah kepada kedua-dua peringkat awal dan perombakan manakala Wi-Fi August Smart Lock dilindungi terhadap kedua-dua serangan yang dijalankan. Penemuan dalam tesis ini akan membantu dalam mengesan kelemahan dalam sistem peranti rumah pintar apabila ia datang kepada spesifikasi kriteria keselamatan.

ACKNOWLEDGEMENTS

First and foremost is to praise to ALLAH S.W.T for this golden opportunity and the strength to complete this thesis.

I would like to thank the Ministry of Higher Education, Malaysia for supporting this research under the Fundamental Research Grant Scheme (FRGS) RACER with code number RACER/1/2019/ICT04/UPNM/2. This research is also supported by National Defense University Malaysia (NDUM).

My sincere special thanks are extended to my supervisor and co supervisor, Dr Nor Fatimah Binti Awang and Dr Syahaneim Binti Marzukhi. For the guidance to finish this research.

A very special appreciation and thanks to my beloved parents, Mohd Zainudin Bin Ahmad and Nordalelah Binti Daud, and my dearest family for their never-ending support.

APPROVAL

The Examination Committee has met on **27 May 2022** to conduct the final examination of **Ahmad Fudhail Iyad Bin Mohd Zainudin** on his degree thesis entitled **'Replay Attack on Bluetooth Communication with Software Defined Radio in the IOT Based Smart Home.**

The committee recommends that the student be awarded the of Name of Degree (Specialisation).

Members of the Examination Committee were as follows.

Prof. Ts. Dr. Omar Bin Zakaria
Faculty Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Prof. Dr. Mohd Nazri Bin Ismail
Faculty Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Prof. Dr. Azizah Abdul Manaf
Faculty of Science and Technology
Universiti Tunku Abdul Rahman
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Master of Science (Computer Science)**. The members of the Supervisory Committee were as follows.

NOR FATIMAH BINTI AWANG
FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

SYAHANEIM BINTI MARZUKHI
FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name : AHMAD FUDHAIL IYAD BIN MOHD ZAINUDIN
Date of birth : 4TH OCTOBER 1997
Title : REPLAY ATTACK ON BLUETOOTH COMMUNICATION WITH SOFTWARE DEFINED RADIO IN THE IOT BASED SMART HOME
Academic session : 2020-2022

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☐ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

Signature	**Signature of Supervisor/Dean of CGS/ Chief Librarian
Click here to enter text.	Click here to enter text.
IC/Passport No.	**Name of Supervisor/Dean of CGS/ Chief Librarian
Date:	Date:

*If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.

** Witness

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	-	Artificial Intelligence
DDoS	-	Distributed Denial of Service
EPC	-	Electronic Product Code
GHz	-	Megahertz
HCI	-	Host Controller Interface
ICT	-	Information and Communication Technology
ID	-	Identification
IEEE	-	The Institute of Electrical and Electronics Engineers
IoT	-	Internet of Things
IP	-	Internet Protocol
ISM	-	Industrial, Scientific and Medical
L2CAP	-	Logical Link Control Adaptation Protocol
LoRa	-	Long Range Radio
M	-	Meter
MAC	-	Medium Access Control
MHz	-	Gigahertz
MIC	-	Message Integrity Code
MOL	-	Methods and Objective Library
mW	-	Milliwatt
NFC	-	Near Field Communication
OCTAVE	-	Operational Critical Threat Asset and Vulnerability Evaluation
OWASP	-	Open Web Application Security Project
PC	-	Personal Computer
PIN	-	Personal Identification Number
PLC	-	Programmable Logic Controller
PoC	-	Proof of Concept

RFCOMM	-	Radio Frequency Communication
RFID	-	Radio Frequency Identification
SDP	-	Service Discovery Protocol
SDR	-	Software Defined Radio
SSID	-	Service Set Identifier
TAL	-	Threat Agent Library
TARA	-	Threat Analysis and Risk Assessment
UPNM	-	Universiti Pertahanan Nasional Malaysia
UWB	-	Ultra-wideband
VM	-	Virtual Machine
WI-FI	-	Wireless Fidelity
WIRED	-	Workshop on Internet Routing Evolution and Design
WIT	-	Wessex Institute of Technology
WLAN	-	Wireless Local Area Network
WSN	-	Wireless Sensor Networks

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Internet of Things (IoT) lacks a standard definition. The phrase has been used by a variety of persons throughout the years, but its first use has been credited to a digital innovation specialist named Kevin Ashton in 2009. According to all definitions, the original version of the Internet consisted of data generated by humans, whereas the second version consisted of data created by "Things", hence the name "Internet of Things".

The introduction of IoT technology into our homes creates modern safety issues, thus IoT-based smart homes require high-scale standards for security. Steinberg (2014) stated that since IoT-enabled smart homes are particularly vulnerable to internet attacks, the attacker has the ability to breach the users' privacy, steal their personal information, and watch them in their homes (Steinberg, 2014). Thus, suitable measures must be implemented to prevent this from happening. According to Evans (2011), there were 12.5 billion internet-connected devices in 2010 with 50 billion

interconnected devices projected by 2020, thereby increasing the number of security issues to deal with.

As the rate of smart homes devices increases, so does the complexity. A study by Mennicken, Vermeulen, and Huang (2014) reported that wireless networks and increasing amount of interaction between devices has increased the complexity of maintenance and security. The researchers showed that consumers use smart home to provide 'peace of mind'. Meanwhile, in terms of social challenges faced when implementing smart homes, one concern for customers was to keep their system secure (Brush et al., 2013). For instance, most households that use home automation in their everyday life believed remote access was a good idea (Brush et al., 2011). However, 7 out of 14 households raised concerns regarding the security of remote access, especially about remote access of door locks and cameras (Brush et al., 2011). Data leaks or breaches in smart homes raises concerns regarding privacy and security.

Abdullah, Hamad, Abdulrahman, Moala & Elkhediri (2014) compiled the statistics from main academic sources to investigate the variety of possible research in the area of cybersecurity in IoT. Figure 1.1 shows the number of studies cited in the research related to IoT security threats from 1998 to 2020 (Rani et al., 2021). The field of IoT security has gained exceptional interest and importance in the last decade.

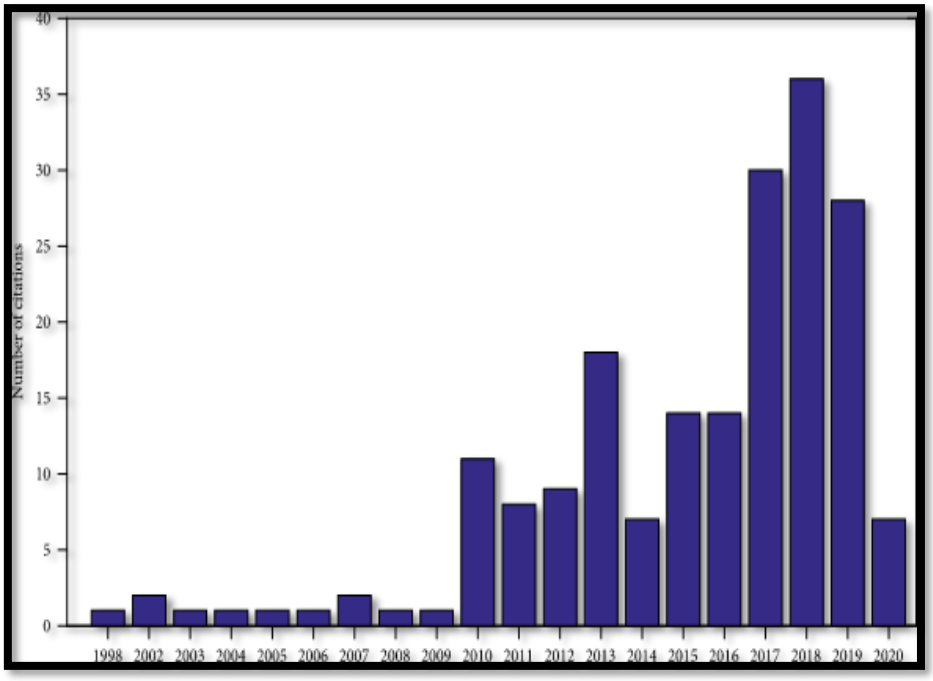

Figure 1.1 IoT security threats research analytics. (Rani et al., 2021).

This proposed research focuses on security assessment for detecting vulnerabilities for Bluetooth communication with software defined radio in two IoT-based smart home devices: Hampton Wireless Doorbell and Wi-Fi August Smart Door lock. In previous security assessment by Viderberg (2019), the author investigated attack vectors related to the technologies available over the internet. The research by Viderberg (2019) was further extended by Borg and Francke (2020) where their study covered a security assessment on Glue Smart Lock, focusing on the firmware of the embedded devices of the system as the main assets. Given that these latter authors focused only on the security of the Glue Smart Lock firmware, Viderberg (2019) suggested that future research should investigate the vector radio aspect, which is the Bluetooth communication of smart home device. Thus, this study addresses this gap of assessment in detecting vulnerabilities in IoT based smart home devices with

Bluetooth communication as its vector. This is in line with the method purposed by Gupta (2019) in his book by using Software Defined Radio (SDR) to analyse the communication and further exploit the vulnerabilities of smart home devices.

Internet of things devices are becoming increasingly employed, especially for smart door lock and smart doorbell as these two devices are mounted on the door, acting as the first line of defence for every room, house, and office. A smart door lock is a tool to execute the operation of locking and unlocking mechanism on a door through commands from an authorised device. This is accomplished through the use of a wireless protocol and a cryptographic key. The smart door lock also collects data related to the device's condition and as monitors to access the door and sends the live information to one or many devices connected to it.

A smart doorbell is designed to notify a smartphone or other home electronical appliances whenever a person arrives at the doorbell via internet or Bluetooth connections. Therefore, it will be automatically activated whenever a person presses the button on the doorbell or alternatively whenever it senses a person using its built-in motion sensors. Hence, this study addresses Smart Home Door Lock and Smart Doorbell high security management and the need for these devices to go hand in hand with the high demand among people.

1.2 Problem Statement

Stories about IoT-based Smart Homes and the associated significant security issues have raised public attention and sparked worries among users (Ali, W. et al 2017). A conventional primary defensive priority at home includes the entrance, doors, as well as their locking mechanism while protecting residents from unforeseen danger from intruders. Nevertheless, one of the possible threats of connecting a house via the internet is the possibility of a hacker intruding the house (Jordan, T. & Taylor, P. 1998). Specifically, the hacker uses an internet connection to gain the right to control the house regardless of place and time.

Smart Door Lock and Smart Doorbell are crucial Smart Home devices to be assessed for their security and reliability in this thesis. As mentioned earlier, both devices are common components that are mounted on the door. There have been reports by Hassija V. et al (2019) on the increased possibility of a security breach including the owner's cloud servers, which could also be a target for an attack to obtain key information. The communication between these smart devices and the owner's mobile device remains a high potential target by attackers. Bluetooth Low Energy (BLE) is a widely used protocol for transferring data between the IoT devices' components.

The IoT is redefining traditional hardware functions. It poses security risks, but it also opens up new possibilities. In order to identify malicious software or hardware assaults on key IoT devices, such as a Smart Home Door Lock and Smart Doorbell,

extensive monitoring and reporting are required to maintain software and hardware integrity.

The present research focused on evaluating the security of Bluetooth communication with Software Define Radio (SDR) that enables the analysis of radio communication technology in IoT devices, specifically the August Smart Door Lock and Hampton Bay Smart Doorbell. Both of these IoT devices implement BLE to communicate between the devices involved.

When testing radio penetration, it is necessary to search for the device's FCC ID and determine the frequency at which it communicates. However, there is one drawback to this: What if the gadget broadcasts at 436 MHz and the following device to be tested at 355 MHz? According to Gupta (2019), the ideal way to address this problem is to use SDR, which allows the adjustment of the listened radio frequency and decode the signal dependent on the evaluated device. As a result, individual hardware for different devices is no longer required, rather a mix of a single hardware and software utility that allows for adjustments based on requirements (p. 225).

Relevant attacks were conducted in this research, followed by testing the security vulnerabilities in Bluetooth communication in specific selected smart home devices. These procedures were undertaken so that users are informed about security risk issues that could be exploited by potential attackers due to their lack of awareness.

1.3 Research Question

(a) What are the common vulnerabilities in IoT-based Smart Home?

(b) How to perform penetration testing with Software Define Radio (SDR) on Smart Home Devices?

(c) How to capture the Bluetooth Low Energy (BLE) frequency signal of Smart Home Devices using Software Defined Radio?

1.4 Objectives

(a) To identify attacks and vulnerabilities that are common in Smart Home Devices.

(b) To perform penetration testing with Software Define Radio (SDR) on Smart Home Devices.

(c) To measure and analyse Smart Home Devices' Bluetooth Low Energy (BLE) frequency signal of Smart Home Devices using Software Define Radio.

1.5 Scope of Research

This thesis focuses on security penetration testing with SDR to investigate vulnerabilities in Bluetooth communication of the IoT devices Smart Home – Hampton Bay Smart Doorbell and August Smart Lock, utilising the framework described in Chapter 3 as the focus of this research. Four experiments that cover all the threats will be conducted, as well as the code and information on data captured will be presented to identify the flaws in August Smart lock and Hampton Bay Smart

Doorbell. Due to time constraint, other attack vectors and attacks or testing on other type of smart home devices will not be covered.

1.6 Research Contribution and Significance

It is prudent that the research findings will help to elucidate the security threat posed by chosen IoT-based smart home devices. Based on the experiment of using August Smart Lock and Hampton Bay Smart Doorbell, consumers will be educated about the possible dangers they face and the precautions they may take to make their Smart Homes safer, whether intended or unintended. Therefore, this finding directly contributes to other security experts working on IoT-based Smart Homes in IoT security research field.

Further, the findings will reveal whether there are any weaknesses in Bluetooth communication in August Smart Lock and Hampton Bay Smart Doorbell, as well as probable implications. Lessons learnt from the security assessment framework will assist future development of any IoT security research. Based on the findings in this thesis, IoT technology installations may be designed to be more secure for users and consumers as the usage of smart device is increasing in line with rapid pace of modernization.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, previous studies related to the IoT-based smart home which are the enabling technologies for IoT, smart home structure, and IoT component architecture are reviewed. Previous research on Bluetooth technology in enabling IoT and Bluetooth security threats are also discussed to understand how the Bluetooth communication works and to identify the associated security threats. The discussion also includes replay attack, software defined radio, and IoT security framework in order to propose a suitable penetration testing guideline that can be adapted and implemented in 'Replay Attack on Bluetooth with Software Defined Radio in The IoT Based Smart Home'.

2.2 Enabling Technologies for IoT

The Smart Home Concept has become a reality due to advancements in ICT, such as computer networks, embedded systems, and artificial intelligence. It is now feasible to create artificial intelligence in smart homes by adding new smart features