UNIVERSITI TEKNOLOGI MARA

ADVANCEMENT OF HOME DIGITAL VOICE ASSISTANTS: ARCHITECTURE ENHANCEMENT AND HARDWARE BASED SECURITY

TS. RIZZO MUNGKA ANAK RECHIE

Thesis submitted in fulfilment
of the requirements for the degree of
Master of Science
(Electrical Engineering)

College of Engineering

March 2024

ABSTRACT

Voice assistants have become increasingly common in today's digital world because they are efficient and convenient. This technical development, however, also prompts worries about the susceptibility of personal information to security lapses. Users are growing increasingly concerned about potential risks such as identity theft and financial damages that may arise from data breaches. Voice assistants are vulnerable to a range of security weaknesses because to their extensive usage, which puts them at risk of unauthorised entry and data breaches. Safeguarding these devices against potential security threats has become an urgent priority, requiring actions to guarantee the privacy and protection of user data. This research project's main goal is to find out how well voice assistant security can be strengthened by installing a Hardware Security Module (HSM) and evaluate its efficiency. The main goal of this study is to show how HSM like the Zymbit Zymkey 4i can make speech assistants safer, lower security risks, and protect private and sensitive data like personal information. The study centres on employing the Zymbit Zymkey 4i HSM in a voice assistant system constructed on Raspberry Pi. The evaluation assesses the effectiveness of the HSM in delivering cryptographic key management and secure key storage to safeguard vital data from unauthorised access. The research thoroughly examines the characteristics of the HSM, with a particular focus on its energy efficiency and little memory usage. This study evaluates the practicality of incorporating HSM into voice assistant systems for extensive utilisation. This study shows that the inclusion of HSM greatly improves the security of voice assistant systems, based on thorough analysis and experimentation. The research findings suggest that the effective utilisation of HSM can verify the authenticity of voice assistant devices and prohibit system boot-up in the event of corruption. Moreover, the study emphasises the impressive energy efficiency and low memory usage of the Zymbit Zymkey 4i HSM, confirming its suitability for widespread use in voice assistant systems globally. To summarise, the usage of HSMs offers a practical and efficient method to enhance the security of voice assistant technology. This ensures that users data is safeguarded against unauthorised access and security breaches, while still benefiting from the convenience provided by these devices.

ACKNOWLEDGEMENT

First, I wish to thank God for giving me the opportunity to embark on my MSc and for completing this long and challenging journey successfully. My gratitude and thanks go to my supervisor Assoc Prof Ir Dr Yusnani Yussoff, Dr Lucyantie Mazalan, Mr. Saufy Rohmad and Mr. Suhairi Mohd Jawi for their endless guidance.

My appreciation goes to the Mr. Suhairi of the Cybersecurity Malaysia who provided the facilities insights, technology information and assistance during the development. Special thanks to all of my lab mates and friends for helping me with this research.

Finally, this thesis is dedicated to my family for their endless support and encouragement to make their dream come true to see their child on having a Master's Degree. This piece of victory is dedicated to all of you.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 Background Study

In the not-too-distant future, smart homes have become the norm, and digital voice assistants are a ubiquitous presence in households worldwide. These devices have revolutionized the way people interact with their homes, providing convenient voice-activated control over everything from lighting and temperature to entertainment systems and security cameras. But with this convenience comes a new threat: the risk of cybersecurity breaches that can compromise personal information, spy on individuals, and even control their homes. A perfect example of a household, whose digital voice assistant becomes compromised, leading to a terrifying and dangerous situation. Home Digital Voice Assistant (HDVA) is a home assistant software that runs or performs task based on the user voice command. HDVA function is to provide information or to run tasks such as telling the music title, tell the weather forecast for today, set an alarm, check if the user has any meeting at work today, or to check the user for any new email. By that, the location, contact details and the microphone service of the HDVA device are always activated to enable the HDVA service running smoothly.

The voice assistant varies in platform, it can run on smartphone, smart TV and HDVA device, such as Amazon Echo Dot or Google Home. The HDVA is connected to our home wireless router for it to work seamlessly. It is able to control smart home lights, smart TV and smart air conditioner. All of the smart home devices that are able to be controlled by the HDVA, must be configured by the HDVA dedicated applications itself for it to work flawlessly. The HDVA may provide usefulness in everyday life for its target user, but such device possesses a vulnerability that is not visible to the eye of consumer. From fake orders, active listening and device tampering for spying may cause privacy issues for its user.

The present study focusses towards the HDVA device security issues in terms of the device physical security state, boot signature integrity, and its feasibility for commercial use after the security enhancement. The HDVA common security issue comes from the audio input which is the dedicated microphone attached to the device.