Mobile app to analyse apk files based on yara rule

muhammad izham bin norhamadi

b032020039

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

# INTRODUCTION

## Introduction

Android Operating System is one of the most popular and widely used open-source mobile platforms and has the highest mobile market share until this day, making it the most widely used operating system in the world. This fact makes Android users the biggest target group for malware developers as trend analyses show large increase in mobile malware targeting the Android platform which leads to privacy thefts of Android users. The security and privacy of Android apps are very critical, especially that over 6000 apps are added to the Google Play Store every day. Thus, various mobile malware detection systems are proposed in the recent years to address this issue. The objective of this project is to develop a mobile application that can analyse APK files by utilizing YARA Rule. By the end of this project, it is expected to produce a functional mobile app that can analyse malware from APK files using certain YARA Rules.

## Problem Statement

Android Operating System was found with increasing malware attacks in recent year. Often users are not aware of malware installed on their device which can came from the Google Play or other unknown third-party source.

|  |  |
| --- | --- |
| PS | **Problem Statement** |
| PS1 | Android devices are prime target for malware and often users are not aware of malicious applications that are going to be installed |

Figure ‎1.2.1 Summary of Problem Statement

## Project Question

Based on the problem statement above, a suitable mobile development framework and YARA Rules need to be developed for a functional mobile analysis tool. Further study on YARA Rule is needed to understand the tool and its usage.

|  |  |  |
| --- | --- | --- |
| PS | **PQ** | **Problem Question** |
| PS1 | PQ1 | How to create an effective malware analysis tool on Android platform? |

Figure ‎1.3.1 Project Question

## Project Objective

The project aims to investigate the application of YARA Rule on malware investigation and to develop a mobile app that utilizes YARA Rule using any suitable framework or tool available.

|  |  |  |  |
| --- | --- | --- | --- |
| PS | **PQ** | **PO** | **Project Objective** |
| PS1 | PQ1 | PO1 | To investigate YARA Rule and its application on malware investigation |
| PO2 | To develop a suitable YARA Rule and mobile app |
| PO3 | To assess developed mobile app using sample APKs |

Figure ‎1.4.1 Project Objective

## Project Scope

### Automatically generate YARA Rule using open-source tools

Writing YARA rules manually requires a highly specialized skill set in security, whereas using tools can help generate YARA rules automatically with relative ease. However, generated YARA rules are generally not optimized for operations and require post processing manually to reduce false positives and to increase its effectiveness. Therefore, an optimal YARA rule for mobile malware requires a generated YARA rule from a selected tool and manually processing the rule.

### Develop mobile app

To produce a malware analysis app on Android, it is important to choose one of the mobile development frameworks such as React Native, Flutter and Kotlin each with their own pros and cons. Once developed, the software then can be installed through APK file to any Android devices.

## Project Contribution

Using YARA tools and automation, the project will generate YARA Rule that will identify and classify malware families, in addition of producing a malware analysis tool for Android platform.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS | **PQ** | **PO** | **PC** | **Project Contribution** |
| PS1 | PQ1 | PO1 | PC1 | Generation of YARA Rule |
| PC2 | Classification of malware |
| PO2 | PC3 | Produces malware analysis tool on Android |
| PO3 |

## Report Organization

Chapter 1: Introduction

Introduction chapter discusses about the overall picture of the project. This chapter also explains about the scope and explains the gist of the whole project.

Chapter 2: Literature Review

Literature Review will discuss about the problem statement in more detail. Next, this chapter will also discuss the findings found in research papers that are related to this topic. Things that are required to be inserted here are such as citation of the research papers.

Chapter 3: Project Methodology

Project Methodology will discuss the method completing this project. It will follow the project milestone given to make sure that each chapter are completed in time.

Chapter 4: Design

Design chapter models how the application will work which include the user interface, the framework used, the programming language and how the application communicate data online.

Chapter 5: Implementation

Implementation chapter is the development phase to build the application. It details the tools and requirement in the development and the creation of prototype.

Chapter 6: Testing and Analysis

Testing and Analysis chapter will test the functionality of the prototype and improving parts of the application to meet the requirements.

Chapter 7: Conclusion

Conclusion chapter concludes the result of the whole project. Starting from the design until testing and analysis chapter. This chapter will also conclude whether the project is a success or vice versa.

## Conclusion

The introduction explains the rough idea about the mobile analysis project which state the project’s problem statement, project question, project objective and project scope. It also shows the overview of the project report structure. The next chapter, literature review, will take an in-dept look on the success automatic YARA rule generation tools and its implementation on mobile platform.