Mobile app to analyse apk files based on yara rule

muhammad izham bin norhamadi

b032020039

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

# Literature review

## Introduction

This chapter will discuss the literature review of the project. The framework of this literature review is as follow:



## Related Work/Previous Work

Due to how flexible and customizable nature YARA rules for malware analysis, there are several YARA rules generator tools that were created to automate the time-intensive process of generating the rules manually such as *yarGen*, *yaraGenerator*, and *yarbin* (Naik, 2020). *yarGen* is a Python-based tool utilized to generate YARA rules using intelligent techniques such as fuzzy regular expression, Naïve Bayes classifier and Gibberish Detector (Roth, 2017). *yaraGenerator* is a Python-based tool used for the generation of YARA rules with completely different signature for different types of files such as EXEs, PDFs and Emails utilizing string prioritization logic and code refactoring (Clark, 2013). *yarbin* is another Python-based tool that generates YARA rule by finding rare functions in a certain malware samples or families by checking function prologues which define the start of functions (Chrisdoman, 2016).

## Critical review of current problem and justification

Despite YARA being widely accepted technique for malware analysis, few tools exist and relatively little work has been done to automate the generation of YARA rules for specific malware families (Raff, 2020), many of the automatic generation tools were barely maintained and written with outdated Python libraries. Thus they were deemed unfit to be implanted to the current project. Besides that, APKs are zip archives, it is not ideal to build rules using APK information such as manifest and certificate as decompressing zip and extracting the information into a single module would add a lot of unnecessary complexity and dependencies. Most analysts resort to building YARA rules for the dex file only without external help. *Koodous* platform provides an API to parse the APK file into a JSON report to be used with *androguard-yara* but the usage limit for analysis report for free user is 5/day which is not ideal.

## Proposed Solution/Further project

In order to develop the project, Flutter was chosen as a suitable android development framework due to its compatibility with Android OS and extensiveness of Flutter library that allows rapid development of application. This project will make full use of VirusTotal API to parse APK file and to extract YARA rules from VirusTotal’s crowdsourced YARA rules that matches sample APKs. Next, the project will make use of Koodous to extract APK information into JSON report, then use Androguard module for YARA to integrate static APK analysis with custom YARA rules.

## Conclusion

In conclusion, this project will develop a static analysis app based on YARA rules using Flutter framework. The next chapter will discuss on the methodologies that will be done throughout this project.