Universiti Teknologi MARA

Analysis of Android apps based on their behaviour during runtime by Frida

Rosamira binti Amaran

Thesis submitted in fulfilment of the requirements for Bachelor of Computer Science (Hons.) Data Communication And Networking

July 2020

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, praise and thanks to Allah SWT, for all the graces and blessings and also Selawat and Salam to the Prophet Rasulullah SAW, hopefully His syafa‟at will be abundant in days later.

First, I would like to express my highest gratitude to my supervisor, En Hamid bin Othman for her guidance, advice and support in order to complete this final year project. I appreciate every single “walk” she taught me. I would also like to thank Dr Siti Arpah Binti Ahmad as the lecturer for CS245 for his guidance and encouragement during the preparation of this project.

Thanks also to all the lecturers in the course of Bachelor of Science (Hons) Networking & Data Communications at UiTM Shah Alam for their patience and kind advice during the process of completing the project.

Lastly, thanks you so much to all those who supporting me in any way during the completions of this proposal report by discussing, sharing or exchanging ideas and everyone who are directly or indirectly in making this project successful.

ABSTRACT

Android is the most commonly used mobile device operating system. Due to the biggest mobile market, attract many hackers to develop malware to exploit users. Regarding to overcome this problem, developing a trustworthy and fast malware analysis method is necessary. In addition, there are limited resources for mobile devices to test applications. Frida , which is free and open source dynamic code instrumentation toolkit that works by injecting a JavaScript engine (Duktape and V8) into the target projects. Besides, Frida lets us execute snippets of JavaScript into native apps on multiple platforms such as Android and iOS. In this project, we can use frida by implements code injection which is writing code directly into process memory. Then, JS gets executed with full access to memory, hooking functions and even calling native functions inside the process.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Mobile devices, especially smartphones, make a major contribution to the fast and massive sharing of information environment (Hunjae Kang, 2015). We use it for communication, business transactions, entertainment and many other activities (Waqar Rashid, 2018). But, at the same time, the increasing of using mobile devices caused some problems. In 2018, 5,321,142 million malicious installation packages, 151,359 new mobile banking Trojans and 60,176 new mobile ransomware trojans were detected by Kaspersky Lab product and technologies. These cybercriminal cases were recorded as the highest cases in this state. Both new mobile devices infection technique like DNS hijacking and step-up in the use tried-and-tested distribution schemes like SMS spam were also observed during this year. Virus attackers focused on Droppers (Trojan-Dropper) to bypass detection. In addition, mobile devices also attack back accounts. Usually mobile devices are bypassed by apps or adware apps. Mobile malware mainly targets Android platform due to the fastest growing mobile operating systems, which account for about 87.8 percent of the market share. These malware applications, also known as malware, can slow down devices processing and internet speed (Taniya Bhatia, 2017). They can also strain your devices batteries by continuously displaying aggressive adware (Rishabh Kaushal, 2017).

According to data available on the worldwide market share of mobile operating systems, the android platform runs on 76.24% of smartphones and all about 23.76% of all phones (https://gs.statcountser.com/os-market-share/mobile/worldwide). A major contributor to Android's popularity is the fact that it is used as an operating system for their devices by many more smartphones and device manufacturers. By comparison, iOS is limited to iPhones and iPads made by Apple only. IOS is better than android. It's because when developers upload some applications to the apple store, it's going to be reviewed and verified by apple, so apple doesn't enable us to use random apps, and