Android: S-Based Technique in Mobile Malware Detection

Rahiwan Nazar Romli¹, Mohamad Fadli Zolkipli¹, Al_Fahim Mubarak Ali¹, Muhammad Ramiza Ramli¹
¹Faculty of Computer System & Software Engineering, University of Malaysia Pahang, Gambang, Malaysia

Corresponding author Email: rahiwan@ump.edu.my
Received: 19 July 2017   Accepted: 27 September 2017

Mobile malware is a serious threat in mobile security. Malware detector is the primary tool and first defense to protect mobile device against mobile malware. The impact of malware is negative. It causes files to be corrupted and secret information being compromised. Nowadays malware writers try to avoid detection from malware detectors using several techniques such as polymorphism and metamorphism. In order to overcome malware, concern in mobile, we propose a new framework for malware detection which is signature based technique using pattern matching. This framework uses signature number and Secure Hash Algorithm (SHA) as signature in the detection process. Both features will be examined by sequence in order to detect leakage of information. As a result, a file that considered as suspicious or malware will be sent to cloud for analyzing and classification.

Keywords: Mobile Malware, Polymorphism, Metamorphism, Signature Based Technique

1. INTRODUCTION

The increasing use of mobile devices become dramatically. This phenomenon occurs due to capability mobile device compare to personal computer. The capability includes small size with powerful processor, higher memory capacity and portable contributing in increase of mobile user. In quarter 4 of 2016, a report by IDC showed that 428.5 million mobile devices were shipped by smartphone vendor and roughly 81.7% of user primarily target Android operating system¹.

The rise of mobile threat occurred since 2009 and the number of this threat has rapidly increased and mostly targeting android users. Attackers look for profit by stealing information through system vulnerabilities and mobile device is the easier way to get in. Malware can be filtered through anti-malware tool or anti-virus. However, according to Moutaz² due to limitation of mobile resources, anti-virus engine can’t work properly in mobile devices for malware detection.

The problem arises when mobile device is infected by malware before new malwares are identified and kept for future use. This problem happens because current antivirus can’t detect malware due to malware author using the evasion technique such as polymorphism and Metamorphism. Both of technique have ability to change their code. For example, polymorphism is used to evade detector by mutate the code in different form (morph) while keeping the original code. While, metamorphism is another technique that automatically recode itself when propagate but still have the same behavior.

In this paper, we propose a new framework for malware detection that using Signature Based Technique and Artificial Intelligent algorithm to solve the problem. The proposed framework consists of two part which is S-Based Detection and Pattern Matching Algorithm. We hope our finding as wake up call for malware researcher to improve the current approach in mobile malware detection.

The rest of the paper is organized as follow; Section II highlights state of the art of scope of study. Section III discusses about related work from previous study. Section...