"Less Give More": Evaluate and zoning Android applications

Mohd Faizal Ab Razak, Nor Badrul Anuar, Rosli Salleh, Ahmad Firdaus, Muhammad Faiz, Hammoudeh S. Alamri

Abstract

The Android security mechanism is the first approach to protect data, system resource as well as reduce the impact of malware. Past malware studies tend to investigate the novel approaches of preventing, detecting and responding to malware threats but little attention has been given to the area of risk assessment. This paper aims to fill that gap by presenting a risk assessment approach that evaluate the risk zone for an application. The permission-based approach is presented for evaluating and zoning the Android applications (EZADroid), based on risk assessment. The EZADroid applies the Analytic Hierarchy Process (AHP) as a decision factor to calculate the risk value. A total of 5000 benign and 5000 malware applications were drawn from the AndroZoo and Drebin datasets for evaluation. Results showed that the EZADroid had achieved 89.82% accuracy rate in classifying the application into a different level of risk zones (i.e. very low, low, medium, and high). The Android security mechanism is the first approach to protect data, system resource as well as reduce the impact of malware. Past malware studies tend to investigate the novel approaches of preventing, detecting and responding to malware threats but little attention has been given to the area of risk assessment. This paper aims to fill that gap by presenting a risk assessment approach that evaluate the risk zone for an application. The permission-based approach is presented for evaluating and zoning the Android applications (EZADroid), based on risk assessment. The EZADroid applies the Analytic Hierarchy Process (AHP) as a decision factor to calculate the risk value. A total of 5000 benign and 5000 malware applications were drawn from the AndroZoo and Drebin datasets for evaluation. Results showed that the EZADroid had achieved 89.82% accuracy rate in classifying the application into a different level of risk zones (i.e. very low, low, medium, and high). Keywords: Risk assessment; Analytical hierarchy process (AHP); Mobile device; Android; EZADroid

1. Introduction

As technology grows with time, the mobile device landscape continues to evolve. The increasing speed, power, storage space and available application services such as online shopping and games have led mobile users into adopting this technology. As the number of mobile devices increase, malware attacks, especially on Android, also rise consecutively [1]. According to Trend Micro 2016 Security Prediction’s report, malware growth is expected to be 20 million by the end of 2016 while Android is labeled as a high-risk mobile application [2]. The trend shows that more sophisticated mobile malware with zero-days attack bypassing a modern security defenses. The attacks are difficult to identify or mitigate since the number of attacks is probably higher and unnoticed. An Android application known as GodLess, for example, has infected 850,000 mobile devices worldwide [3]. Out of the 96% surge in mobile device infections, Android was the hardest hit by 74% cases while the iOS device recorded only four (4) % of infection rate [4]. In 2014, Symantec discovered more than 317 million new malware while PandaLabs was able to neutralize 75 million malware [5]. These figures demonstrate that, on average, nearly one (1) million malware are released every day [6]. This explosive growth in Android malware causes serious infiltrations to the Android system [7]. In addition, the trends that will dominant in 2018 and influence malware attacks such as evasive techniques, malware vaccination, ransomware and Android malware [8,9]. These trends will continue to dominate in 2018 with continually-evolving threats [9]. To combat these problems, security researchers have designed various anti-virus, anti-malware software and risk analysis which used to detect and analyze the risk of malware applications [10]. This is done by analyzing the patterns of the malicious activities which is achieved by looking at their predefined signatures or by monitoring the application’s behavior.

In particular, the noticeable change of the malware behavior detected through existing approaches such as anti-virus, firewall and the Intrusion Detection Systems (IDSs) [11,12]. However, these approaches are inadequate to fully eliminate the attack since recent malware are capable of evading detection [13,14]. Google Play has introduced a detection approach known as Bouncer [15]; it provides automatic scanning and the removal of potentially malicious applications [13,16]. However, it is inefficient enough to examine applications from third party sources [13] which may lead to privacy violations [17]. Another approach provided by Google Play is a security mechanism which restricts Android applications from accessing private data by using a permission-based system [18]. Nonetheless, the mechanism is also unable to completely protect Android from malware attacks. Expanding on this, the APK Auditor and Stowaway is one mechanism that uses the permission analysis to classify the Android applications as benign or malware.