2019.20

Android Malware Detection using Multilevel Classifier Fusion

Mahesh R. Gavale[1], Prashant M. Yawalkar[2]

[1]Student, M.E Computer Engineering, MET's institute of engineering, Nashik, India
[2]Professor, M.E Computer Engineering, MET's institute of engineering, Nashik, India

Abstract

Abstract— One of the important security factor for the smart phones is Malware detection. The techniques used presently are not sufficient enough to provide accurate detection in polymorphic viruses and zero-day attacks. So the need for malwares detection using machine learning arises rigorously. We propose a machine learning based approach for detecting malwares and benign of the apps installed on the smart phones. A Multilevel classification model that detects the malwares by using a trained model of the base classifiers machine learning algorithms at the lower level and a set of the ranking algorithms at higher level to enable fusion using pairwise combination of ranking algorithms and detect the better average accuracy of fusion.

Keywords: Malware classification, Android Malware detection, Classifier fusion, Machine learning, Mobile security, Static analysis

1. Introduction

The Internet is becoming an important part of everyone life as the online transaction and online net banking is being popular nowadays. The users of Internet including corporates faces security threats caused by malware. Malware is a program that affects a computers, laptops and mobile without the user's permission and with an intention to cause damages to the system or steal private information from the system. Trojans spyware and viruses are examples of malware that have minima security defenses. These malware apps infected on privacy and compromise security by allowing an unauthorized access to personal information.

Android Malware -The malicious software is a specifically build for attack on mobile device. The types of malware are exploits on OS (Operating System), mobile phone and software where mobile devices are increasingly common.

Types of malwares

1. **Ransom ware** - The ransomware is type of malware which is abstracts the information of infected mobile devices and asks for pay money and retrieves that files.

2. **Spyware-** The spyware is type malware that a continues monitor the sensible information and collect about the user like SMS, MMS and contact numbers. It may also keep calls of the Android and transfer the voice data to the remote server without knowledge of the user.

3. **Mobile Bot nets** - The Mobile Bot nets is type malware that is a network of affected mobile devices that are controlled and administered by remotely using botmasters. D - Dos attacks, Carry out Spam delivery on the host devices.

4. **Dynamically Downloaded code** - It is type of malware that is an installed application in mobile devices to download a malicious code and deploys on mobile device.