Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 407 – 417

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

A Novel Approach to Detect Android Malware

Shaikh Bushra Almin[a], Madhumita Chatterjee[b]

[a]*Department of Information Technology, Pillai's Institute of Information Technology, Navi Mumbai, India*
skbushra78691@gmail.com
[b]*Department of Computer Engineering, Pillai's Institute of Information Technology, Navi Mumbai, India*
mchatterjeee@mes.ac.in

Abstract

Android is the world's most popular and the largest installed base of any mobile platform. It has gained huge popularity among Smartphones and is growing very fast because it gives its users a world class platform for creating apps and games and allows them to be distributed instantly. Secondly, it also offers ample free third party applications to be downloaded and installed from Google Play, the premier marketplace for selling and distributing Android apps. Android openness has made it a favourite for users and developers alike. Many apps are getting downloaded by the user from play store every month. However due to this, the number of harmful apps in the form of malwares getting downloaded are also increasing. These malwares performs the various activities behind the scene, such as stealing various sensitive information of the users and signing up victims to subscription services. As a result of this, users are getting affected and their privacy gets compromised. As developers are also free to develop and publish their own creation in a play store without undergoing any scrutiny of their apps, they tend to take the advantage of user's inability to analyze the risk of such apps.

This paper proposes a system which would help the users in analysing and removing such harmful apps and thereby protecting their security and privacy. This is achieved by analysing the various permissions used by an application that it has requested during installation. The overall process of analysing apps is done using clustering and classification techniques. The major objective of the proposed system is to detect and remove the malwares that are present in the user's Android device.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: Android; Malware; Permissions; App/s; Cluster; Malicious; Benign.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.170

1. Introduction

Android is built on open Linux Kernel. Since it is an open source, it gives the opportunity to the developers to come up with their own technological advancements. Android has online market for software store. It allows Android users to select and download third party applications provided by the developers on the market. Android has security features built into its operating system called as permission model. Android permissions are nothing but the rights given to the applications to allow them to do certain tasks like send/receive SMS, take pictures, use the GPS or make phone calls, etc. This permission model tries to restrict an access to the systems or user's information but it nevertheless provides a way to use only certain allowed permission according to user. A user while installing any application in Android phone is first presented with the list of all permissions required by it, after which a user either has to grant all the permissions or reject it. If a user doesn't grant these permissions, it will result in stopping the installation. Thus in order to install and use an application, user has to grant all the permissions that an application needs and then the installed application runs under the granted permissions.

A user who wishes to install and use any application doesn't understand the significance and meaning of the permissions requested by an application, and thereby simply grants all the permissions as a result of which harmful applications also get installed and perform their malicious activity behind the scene. The user's inability of analyzing the risk of any application results in compromised security and privacy.

In this work we propose a system to protect Android user's from malicious applications. The proposed system first applies a k-means clustering algorithm on the permissions of installed applications to categorize them into one of those malicious applications and then a naïve Bayesian classification algorithm is used to accurately classify whether an application is benign or a malicious one. The system reduces the user's burden of analyzing the risk of applications and also assists them in making the decision of removing an application that is harmful.

The rest of this paper is organized as follows: Section 2 provides some related work; Section 3 describes the proposed system in detail; Section 4 discusses in brief about the implementation. In Sections 5 and 6 we discuss the results of our implementation and also give a comparative study of our proposed system with existing anti-virus systems. We conclude in Section 7 with future scope.

2. Related work

Takayuki et al. have proposed a system that assesses and presents the risk level of an Android application to the user at the time of installing the application [1]. The risk assessment involves the following two parameter: (1) the number of downloads and user rating or review from the Android market; (2) the analyses of combinations of permissions for malicious applications. Initially a rule set is made to decide whether the combination of permissions are malicious. The system then reads the permission's combinations of the applications upon its installation and then it searches those permission's combinations in the predefined rule set to distinguish the malwares from benign applications. In order to calculate risk, the system retrieves the number of downloads and user rating from the Android market. The system assigns a base value from 3-5 to permission's combinations and weights to the user ratings and downloads. The weights are assigned depending upon the number of user ratings and downloads to calculate the risk level. The system then presents the risk information of the applications to the user using various colors as risk indicators and finally the user decides whether to delete it or not based on the presented risk's information.

Suleiman Y. et al. have presented an effective approach to alleviate the problem of detecting malicious app based on Bayesian classification models obtained from static code analysis [2]. The models are built from a collection of code and app characteristics that provide indicators of potential malicious activities. In this work, the detection strategy leverages the applications' reliance on the platform APIs and their structured packaging to extract certain properties that could serve as indicators of suspicious activity, such as intent to filtrate sensitive information, launch a malicious payload at runtime, or presence of embedded secondary payload in the external folders etc. These properties then form the basis for Bayesian classifier, which is used to determine whether a given Android app is harmless or suspicious. In order to obtain the feature sets for building the Bayesian model, a Java-based Android package profiling tool for automated reverse engineering of the APK files is implemented. After reverse engineering