Android Malware Analysis Using Resources

Pravin Rathod, Sunil Misal & Gaurav Sakhre

Abstract: Currently the intelligent terminal based on the Android has occupied most of the market, and the number of malware aiming at Android platform is also increasing. The problems of security threats and privacy disclosure caused by malicious behaviors are becoming more serious. How to make the security assessments and metrics effectively for the security of application has become a research hotspot in recent years. In this project we are going to design application which can analyze the application’s resources and through the result of analysis user can identify application is infected by malware or not.

1. Introduction

With the rapid development of the application software based on Android smartphones, the Android phone becomes more and more popular in people’s life in recent years. Android smartphone has brought great convenience to people’s life, at the same time, it causes problems of security. With the increase use of mobile devices, malware is also enjoying unprecedented growth at the expense of unsuspecting and naive users. Even though several mobile security solutions have been proposed, it is apparent that more effort is required to ensure the security of the data on these devices.

Android malware analysis using resources technique analysis the application’s resources and through the result of analysis user can identify that application is infected by malware or not. Now a days most of the people are using android phones but they don’t know how to secure the mobile phones. Mobile phones security problems are increasing day by day because various type of attacks on the mobile phones are also increasing. Malware is malicious code which gains the access of mobile device to perform the malicious activities such as damaging the device, stealing the secure information and irritating the users by doing some unwanted activities. Malware analysis is used to acquire the knowledge of the application behavior from which antivirus team can easily identify the malware affected application. In this project we are detect or analysis the malware using resources which are used by the application this malware can be detected by signature based algorithm.

2. Android and need for analysis

A. The Android Operating System

Google's Android OS is built on the ARM platform with a modified Linux kernel of version 2.6.x (versions older than 4.0) or 3.x (version 4.0+) and was released in 2008. Lower level system utilities are written in C while most user “applications” are written in Java, although it is possible to write applications using native code in a language such as C++. Google's custom Dalvik virtual machine is a replacement for the standard Java virtual machine used on other desktop and server platforms; the engine is optimized for limited resources typically available on mobile devices. Therefore, if a developer writes an Android application in Java, it will be compiled into dex bytecode (in a file called classes.dex), not standard Java bytecode that would run on Windows or UNIX platforms. A detailed presentation of Dalvik can be found in Dalvik author Dan Borstein's presentation.

B. Currently Available Security Measures

Google's Play Store has a security enforcement known as the "Bouncer" which verifies the applications being uploaded for any suspicious behavior. It works on a blacklisting based approach and instances have occurred where-in the malicious application survived several hours or even days before it was detected and taken off. However, this app still does not protect the users from installing malicious apps from sources other than the Play Store. 4.2 version (Jelly Bean) of Android has shipped with a security feature to counter this problem. A new feature allows the user to verify the third party application being installed on the phone. However, research published by Jiang suggests that the system has a malware detection rate of 15.32%. An anti-malware system must have an detection rate of at least 80% to be deemed acceptable.

C. Existent Security Issues

Applications in Android devices may be installed through either the Google Play Store (formerly called Android Market) or through a variety of third party application stores. Some of the third party stores are Opera Mobile app store, GetJar, SlideME, etc. The fact that Android permits application installation from third party vendors means that Google has no control over the quality or safety of the applications provided in these stores. Several cases were encountered where legitimate apps from the Google Play Store were modified to inject malicious code and the modified...
Apps were sold in these third party stores. It is difficult to determine whether the application is genuine or not. In these cases, the reliability of the application depends upon the security measures implemented by the application store. This makes it essential to provide a reliable means to verify the authenticity of the applications.

As in this heading, they should be Times 11-point boldface, initially capitalized, flush left, with one blank line before, and one after.

3. Block diagram of proposed system
In this architecture diagram the malicious data, malware app and malicious links are compared with the metadata of application and if we find metadata like permissions not matching then we will mark current app as malware.

![Architecture Design](image)

WORKING

After clicking on application, It will scan all possible keyword, all metadata and permissions. According to metadata and other keywords it decide which kind of app it is(eg. Messenger, social networking app, ecommerce app). With prebuilt database of possible app categories it compares the metadata of current app with present database. If we find metadata like permissions are not with the present database then we will mark current app as malware.

4. Acknowledgment

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who make it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to undertake this project report. We have a great pleasure in presenting the project report “Android Malware Analysis Using Resources” under the guidance of Prof. J.S.Patil. We are truly grateful to project guide Prof. J.S.Patil for her valuable guidance and encouragement. Her encouraging words went a long way in providing the patience and perseverance, which were needed to complete this project report successfully. I would like to express my gratitude to Dr. M.G. Jadhav, Principal of Jayawantrao Sawant College of Engineering and Prof. S.V. Todkari, Head of Department of Information Technology for their support and guidance. Finally we express my sincere thanks to our parents and all those who helped us directly or in directly in many ways in completion of this project report.

5. REFERENCES