Techniques to Analyze, Identify and Verify the Risk of an Android Application

Pooja Gurunath Isame
Department of Master of Computer Applications
Institute of Management and Computer Studies

Abstract— Android is an open source mobile operating system contributed by Google. In general, Google Play is the most secure place to download the mobile applications for Android system. Products from this website are surely safe promised by Google Company. But there are many other third-party app stores around the world offering similar software. One incentive for them is that the security policy on different platforms varies a lot, and Android developers are free to distribute apps in any intended ways, which leads to a certain risk in the assorted stores such as malware. Therefore, it is crucial to know which application store can be trusted from the various app stores. To support our research, a tool named APK Safety Test is developed to compare the APK files from different application stores with the version on Google Play. In this study, nine stores around the world are chosen and 20 various applications from .them are checked in real-time by using the tool. From this research, people can learn the different risk how can be detected. Furthermore, this paper analyzes the result of risks how to affect the applications.

Key words: Android Application, Android Stores, APK Files, Risk

I. Introduction

Android is the most popular system for mobile devices and the corresponding applications are used a lot by users to serve their daily life. With the increasing numbers of Android applications and stores, the potential risks cannot be ignored as they may lead to the malicious invasion which will affect the whole system. In this research, these third-party stores compared to Google Play, which is the standard at this time, the content includes risks? Definition and analysis of Android applications and comparison process to get the trusted application stores.

II. An Overview of Android

A. Android System-

Android is an open source mobile operating system firstly contributed by Google Company. All source codes of the system are free so people can follow the agreement of GNU to use it freely. Google develops two parts for supporting Android system; they are Android Open Source Platform (AOSP) and Google Mobile Service (GMS). AOSP contains the kernel and parts of core user functions. As the Android kernel is developed by Linux, which is open source, code of AOSP is also public and used for free. The part of GMS packages all the basic functions and software from Google to serve the developers and users but it is not free. [15] The built-in features of Smartphone and tablets usually offer connections for users to access to Google services on their phones conveniently like search, Gmail, maps and other advanced services. Using these functions on the computer side is similar.

B. Android Applications-

It is a kind of software application developed to be used on devices that are associated with Google’s Android platform. Android applications can run on Android smartphones, tablets, and other devices. Some of them can be downloaded freely, and some need to be purchased. With the development of Android technology, users can get access to many functions with Android applications on corresponding devices like gaming, media editing.

C. Google Play VS Third-Party Stores-

Google Play is the official place to download the mobile applications for Android system. However, there are still lots of third party app stores around the world. Many reasons lead people to use the third-party stores. Some application stores have their applications? Availability limited in specific countries or themselves are not localized in some regions. And a good number of Android developers are doing a staged roll out which means that not all users can access to applications at the same time. Also, many app stores routinely offer applications free of charge or at a discounted price to attract more clients.

D. APK File-

The full name of APK is? Android application package? Which is the form of application in the Android system. It can be in the shape of identification and operation. An APK file, the kernel part of an Android application, contains an META-INF folder, res, AndroidManifest.xml, Classes. dex and Resource. arsc. As users intend to find the similarities between these applications from third-party stores and Google Play, each part in the APK file has to be checked. In this report, the APK files from Google Play are used as the standards to be compared with those from other Android Apps stores.

III. Problem Definition

This study will investigate the reasons to

Make the change of APK files and the risks of these changes. All the stores in this paper compare with Google Play, especially focus APK file of the same applications.

- Detection process will avoid time error, they can be tested together and compare with Google Play at the same time.
- To prevent manual testing and decrease the artificial error rate.
- Detect all the elements which will influence the deference and risks.
- It also shows detail information for each item.
- Thorough evaluation mechanism for difference detection.

A. Question

1) How to tell if there are any risks in an Android application?
2) Which part of an APK file (the core of an Android application) may be attacked?
3) Which Android third-party store can be trusted in this research?

IV. METHODS

This section will describe the methods used in our research.

A. Scientific Approach

The approaches include empirical and deductive research.

1) Empirical Research - namely, is a method to summarize conclusions containing the general meanings and laws from a lot of experimental facts, and obtain the nature of items and the internal rules of development through scientific inferential ways.
2) Deductive Research - which means some unknown information deduced from the known part according to theories representing objective laws are worked out by the investigators.

This method of scientific thought contains the observation process, mode searching, and reaching a conclusion to explain the fact while the fact supports the conclusion conversely. The result is resolved based on the acquired data in terms of positivism. To obtain all the information required, the auxiliary tool is used to search each part of the APK file.

B. Package Verification Detection:

This detection is work for the old version of APK file or incorrect APK file. When the stores are updating the applications, the code and pictures will be changed more or less. It is easy to make an error for detection report. If the name of the package is not same as the standard, it is greatly influenced by the mistakenly downloading. So these situations will be divided into the unknown level. This tool will use the Apk Utile jar which is from third-party. It will use the jar to get the information retrieval of APK file, it includes the name and version of this package. During the detection process, it will check the encoding and decoding of package version. Because the version name of package file might do not show the real version, it just a character string of application version. On the other hand, the version code can be used to check the update or demotion of applications, use commons-codec to calculate the sha256 of APK file.

C. Package Distinction Detection:

The essential of the package is a kind of jar file and the default list will be stored in the directory of META-INF/MANIFEST.MF, this list will generate automatically. The list file stores all the files which packaged in an archive file (package files). Moreover, the difference detection of the package can be used to compare the Digital Signature of the package. Any change of signature shows the modification of file by the third-party. Comparing the sha1 of the same file, the sum of all the files, the redundant files or deleted files of MANIFEST.MF is the way used in this study. For CERT.RSA, it compares the sha256, because the code of sha256 will be changed if certificate changed.

V. OBJECTIVES

The main objective of this research is to give a proper guidance before getting trapped by fake android application to every person throughout the world and reduce the number of victims who fall in such trap.

VI. CONCLUSION

Answers to research questions-

1) "How to tell if there are any risks in an Android application" - APK code changed, it means the code of APK was de-complicated to a new APK file. If the code was changed, the signature and classes.dex of APK file would be different. Classes.dex is the place to store the code of APK file.
2) "Which part of an APK file (the core of an Android application) can be attacked"- The answer should be the resource.asrc and classes.dex. If the resource.asrc and classes.dex of an APK file are attacked, the APK file gets the unclear influence.
3) "Which Android third-party store is the most secure one in this research"- Combining all the results, it is evident that 1Mobile is on the top of the recommendation list. 1Mobile is the most similar store to Google Play, so this store can be trusted in this research. But there is a problem that 1Mobile does not have reliable stability as for Chinese users. So for the users in China, 360 is the safest store in this research and 360 shows the security information for each application when users search the application.

ACKNOWLEDGMENT

This research was supported/partially supported by Institute of Management and Computer Studies (IMCOST), Thane, India. We thank our Guide from IMCOST, Thane who provided guidance, insight and expertise that greatly assisted throughout the research, although they may not agree with all the conclusions or interpretations of this paper. We thank Research Guide, Professor, IMCOST, and Thane for comments that greatly improved the manuscript. We would also like to show our gratitude to the institution for sharing their pearls of wisdom with us during this research.

REFERENCES

[1] S. Hill, "Tired of Google Play? Check out these alternative Android app stores", Digital Trends, 2015. [Online]. Available: http://www.digitaltrends.com/mobile/android-app-stores/#:IVaEf0CR83NonA. [Accessed: 27- Feb- 2016].
[2] "Android Security Internals", Network Security, vol. 2015, no. 6, p. 4, 2015.
[3] "Android app ranking and market analysis.", Androidrank.org, 2016. [Online]. Available: http://www.androidrank.org/. [Accessed: 24- May- 2016].
[4] "Download APK free online downloader APKPure.com", Apkpure.com, 2016. [Online]. Available: https://apkpure.com/. [Accessed: 25- May- 2016].

