International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

GENERATING SUMMARY RISK SCORES FOR MOBILE APPLICATIONS

Dr.M.Newlin Rajkumar,
Assistant Professor,
Department of Computer Science,
Anna University Regional Campus, Coimbatore, India

S.Mohan Kumar,
PG Scholar,
Department of Computer Science,
Anna University Regional Campus, Coimbatore, India

V.Dhurka,
PG Scholar,
Department of Computer Science,
Anna University Regional Campus, Coimbatore, India

Abstract: In Android's mobile application main effective defence mechanisms is how to against malicious apps is a risk score communication system which, before a user installs an app, while user installing any apps in their mobile phone to be get the permissions for app requires, so here we have to make the right decisions to follow the based on the risk instructions. in this point of to be ineffective as it presents the risk information. Every app is should be specified the risk in your mobile phone while we install the apps. In this connection apps will requires lot of technical concept and time to control the risk score information. We have to discuss the desired properties of risk signals, all the risk should be find out and showing in a one apps. it is relative risk scores for Android apps are implementing to the user and users can utilize when choosing apps. We present rate of apps we developed to install and user will make them to understand the concept. In this way we have some of the techniques to generate risk signals how we have to avoid the range of all the risk while, before install the apps. Here to be follow the important techniques are implemented to control the risks. This is very effectively identify the android malware attack, it is simple to understand, and very easy to use.

Keywords: Android, Application, Communication, Malicious, Malware attack, Risk.

I. INTRODUCTION

Android apps are built as, an individual activity provides to be activate and a service independently performs a risk score analysis patterns. We should be work on the background. From one component you can follow the component using intent. in entry points for a single app and allows any app to behave the application an action. in other apps may invoke. The Android provides a rich application framework that allows you to build a complete problem solving app. To solve Android application is developed to implement and access the Android app framework. Android is a mobile operating system (os). The Main information of this application the handheld devices are becoming and they provide the mobile devices have different mobile apps for installing new applications. Therefore, the main problem of defence mechanism to be against the malicious applications for most of the user will make the right decisions which is common fact must depend to a large degree on decisions made by the users. The main important part of malware defence on mobile devices is to communicate the risk of installing an app to users. The user enables and compares the risk situations and appears to clear the user to make the problems informed to take the right decisions. In order to consider about the user enrolment of service provider. So have to produce the output choose and install specific apps. One of Android's risk communication mechanisms will make the right decision.

II. EXISTING SYSTEM

In this Android's maindefence mechanisms against malicious apps is a risk communication connection is which apps on user programs are developed. Androidapps permissions are requires before the app is installed by the user, it is normal form mode we have to trusting that the user will make the right decision. The specific point of the project of in this approach used it is used to integrated. The Android apps has been shown as a risk signals. The android multiple permissions we have supported to maintain the user. When a user will install the apps from their mobile phone some progressive report to be make a effective programs.

A. Disadvantages of Existing System

- ✓ Risk warnings we cannot find out again.
- ✓ It is very difficult to check the risk.
- ✓ Analysis is not a simple
- ✓ Once install the apps we do not find the risk where will find.

III. PROPOSED SYSTEM

Android is an open source and Linux-based operating system. Android offers are unified approach to application development for using an android phone. In this paper, we investigating and permission-based risk score signals that used to develop critical permissions are found and check the user requirements. In this connection, we have to follow all user implementation. Initially reported in permissions that have significant security or privacy, a critical permission requested by apps in the same category as the app, the app is labelled as risky signals. It is used to perform a well-organized and security to the user secured risk score analysis. in this project main important part of knowing the information is independent people using mobile phone was some time we getting message suspense. in this type of message should be how to avoid in a critical problems. User applicable for the apps representation of similar database developed android applications, in each apps we will get the risk score in at the same time.

A. Comparision Of Android Applications

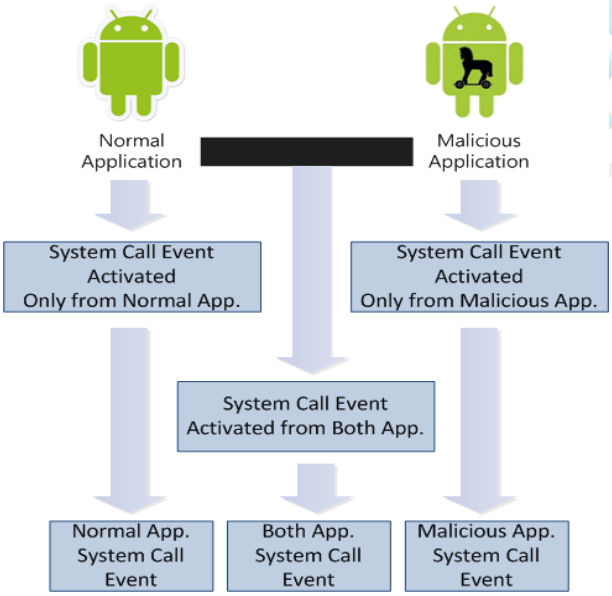

Figure1. Comparison of Android application

B. Advantages Of Proposed System

- ✓ idea of risk score functions to improve risk communication for Android apps,
- ✓ We can use all android mobiles.
- ✓ Installation is very simple
- ✓ Easy to found the risk which we have done.

IV. MODULES

The proposed system has four modules

- ✓ Feature extraction
- ✓ Training the classifier
- ✓ Contribution
- ✓ Risk score based classification

A. Feature extraction:

In mobile learning and android mobile application is a common risk factor avoiding and feature enhancement. The feature extraction set of measured the risk scores analysis and also covered by generating a risk signals. In this way we are following some information to be secured and transferring the data will be secured. User before checking malicious mechanism is declared to base on the risk factor so we have to design the application to the user. It is reducing the risk factor for while using the android mobiles from the user.

B. Training the classifier:

The classifier is a set of API that allows you to define the risk score problems. The user refers the classes of clarification, that time user will waiting to get the message from the traditional output. We have to following some of the standard training application to be contributed to all apps which we have developed among the malicious apps.dalvic virtual machine access to find the risks. The risk scale idendifications.in that mainly represented to compile the user.

C. Contribution

The android mobile application we have developing and avoid the unnecessary problems, which is defined to implement an user request given by user installing an apps required, and also to check the priority to how the risks are available while installing the apps. in this application should be useful to get the all information are required to control the risks. They have help you to found the all high risk problems were we can start to finding the problems, while developing the one apps .it is very simple to use and easy to install.

D. Risk score based classification:

Risk score based classification is better to identify an risk levels it low level, or medium level, or high level, all the level of the risks should be clarified in single apps. We should analysis and install the apps before using the user. The security of risk score based application is configured representation of defence mechanism .they have any application has been applicable to the user environmental score based risk should be followed by defence mechanism. it can be security to manipulate the unique user representations.

The risk score check with the android mobile apps representation of software orientations which will get the output of some information to the standard risk signals.

V. CONCLUSION

This paper extends our previous work on smartphone risk assessment by describing a privacy impact assessment (PIA) for android apps.The importance of effectively communicating the risk of an application to users, and propose several methods to range this risk. One of the effectivemethods is we are using RSS method which has several advantages. It performs a well an identifying most current malware apps as high risk. In this method allows to how to find or highly critical permissions and less-critical permissions to affect the overall score in an easy to understand.

VI. REFERENCE

[1]"Android tops 81 percent of smartphone market share in Q3". Retrieved November 4, 2013.

[2]Android OS: A robust, free, open-source operating system for mobile devices‖ , pdf by, Paul Michael Kilgo.

[3] Sankaranarayanan, S. ; Comput. & Inf. Syst., Inst. Teknol. Brunei, Negara, Brunei ; Wan, A.T., Clean Energy and Technology (CEAT), 2013.

[4] K. Akhila, a Novel Approach of Mobile Based Student Attendance Tracking System Using Android Application, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April - 2013 ISSN: 2278-0181.

[5] W. Enck, D. Octeau, P. McDaniel and S. Chaudhuri, "A Study of Android Application Security," Proceedings of the 20th USENIX Security Symposium, **(2011)**.

[6] Y.-J. Ham, W.-B. Choi, H.-W. Lee, J. D. Lim and J. N. Kim, "Vulnerability monitoring mechanism in Android based smartphone with correlation analysis on event-driven activities", 2012 2nd International Conference on Computer Science and Network Technology, **(2012)**.

[7] Z. Mednieks, L. Dornin, G. Blake Meike and M. Nakamura, "Programming Android", O'Reilly, Sebastopol, CA, USA, **(2012)**.

[8]D. James, "Android Game Programming For Dummies", John Wiley & Sons, Inc., Hoboken, New Jersey, USA, **(2013)**.

[9] M. Nauman, S. Khan and X. Zhang, "Apex: Extending Android Permission Model and Enforcement with User-Defined Runtime Constraints", Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, **(2010)**.