Enhanced Risk Deduction on Installed Android Applications

Hari Rajai[1], Sachin Bojewar[2]

[1]*P.G. Scholar, Department of Computer Engineering, ARMIET, Maharashtra, India*
[2]*Associate Professor, Department of Information Technology, VIT, Maharashtra, India*

Abstract - *Popularity of mobile phones has made them target for intrusive and malicious applications. For building an effective security mechanism for Smartphone there is a need to understand user's attitude towards the security of the information in their Smartphone and the ways adopted by users to perform various tasks on their Smartphone. This understanding will prove to be helpful in building security mechanisms for Smartphone. In current security mechanism the android users have only one android permission display screen which appears after the user have selected an application for download. This permission display screen shows full information describing what permission user is granting to that particular application while installing. The current security mechanism in android lets users to take the decision by understanding the permissions that the application requests before installation. Previous research has shown that the reliance on user for making installation decision is ineffective as users have very less understanding of the technical knowledge about these application permissions. The current risk information mechanism where user is shown the list of permissions proves to be ineffective as it requires technical knowledge and time to understand the permissions. The proposed system provides risk information to the user in a very friendly manner and also suggests the percentage of risk each application carry along with the amount of risk in categories. Also it shows list of permissions taken by installed applications and their risk percentage along with other risk indicators.*

Key Words: **Smartphone, Risk Communication, usability, mobile security, privacy, applications, permissions.**

1. INTRODUCTION

1.1 Overview

In recent years Smartphone have become pervasive. They complement traditional computing devices such as laptops and desktops. There is a significant growth in number of applications in android market place. In recent years, android and iOS, the two most popular Smartphone operating systems have changed the phones from calling devices to pocket computers. This has been achieved through Smartphone applications that user can install on their phone from software markets. According to Google, more than 500,000 devices running android operating system are being activated every day. Android devices are being used widespread for personal and commercial purpose. From novices to experts, there is varied user base for Smartphone devices. New privacy and security threats have been posed by ubiquitous usage of these devices. Our digital devices contain all our information such as contacts, E-mails, passwords and access to locally stored files and files on cloud. There is a risk to access to this personal information by unauthorized parties such as developers of applications being installed on android devices. Also there is another risk which comes from sensors that these devices support. Smartphone support a number of different types of sensors. An access to these sensors through installed applications possess a serious security risk for example user's location can be accessed traced by GPS whereas user's audio can be recorded from microphone and images can be taken from camera without user's consent. Also Smartphone devices are often connected to monetary accounts through messages or phone calls or there is an existence of digital wallet information in mobile. This means any mobile application that has an access to this information through permission can access and log this information. There is a very thin line between benign applications and malicious applications where many applications can be overly invasive but not malicious. For computers, user installs very few applications that too from well renowned developers but in case of mobile devices a person downloads many applications from different unknown vendors on trial basis.

1.2 Installing Android Application

In Google play store, users are shown permission only after they have decided to install the application. Researchers have shown that users are most likely to avoid the permissions displayed as they have already decided to install the application. Also when users pay attention to the permissions, they hardly understand the permissions as these permissions require technical knowledge for understanding which resources these permissions are requesting. In Android, an application must request a permission from the user to access a particular resource. Android shows the warning to the user about the permissions that the application is requesting for accessing the resources. In current situation, the android expects the user to take an informed decision. Here the effectiveness depends upon the choices made by the user. The consideration of an application as too invasive or not depends upon users privacy preference. The risk of installing an application is not conveyed to the user so that the user can make effective decision about installation of an application. Android's current risk communication mechanism is of limited effectiveness. Studies have also demonstrated that users tend to ignore the permissions while installation of an application [3] [4]. Some recent work has been done by modifying the permission category headers, reducing the number of permissions, emphasizing risks, incorporating user reviews and rethinking of timing when and how permission are granted to the application before installation. The proposed system considers an alternative approach which aims to help user to make installation decision with better understanding of security and privacy information.

1.3 Objectives

- To provide a risk score to each installed application in form of risk percentage, color, graph and Low/Mid/High format.
- To provide a way to uninstall an application when the user finds it to be inappropriate or malicious

2. LITERATURE SURVEY

2.1 A Conundrum of Permissions: Installing Applications on an Android Smart Phone

Every time user installs an application, a list of permissions required by that application is displayed. By looking at that application, user can decide whether to trust that application will not damage their phone, share information with untrusted source or not. People from different cities who used Smartphone were interviewed. The aim of this interview was to know whether people understand the permissions, whether they understand risk associated with all permissions. It was found that people view these permissions generally and they do not understand them. People are also unaware of the risk associated with all permissions asked by an application. In short, it can be said that users are not well informed about the security risks associated with applications. [3]

2.2 Android Permission: User Attention, Comprehension and Behavior

Android permission system shows list of permissions required by Android before installation of the application. It is accepted from the user to view and understand all the permissions and decide whether to install the application or not. Survey was done to check whether people read, understand the permissions displayed before installation. It was found that only 17% of the people surveyed actually read the permissions, others blindly accepted. Only 3% of the total people surveyed could tell what those permissions meant. [4]

2.3 The Effectiveness of Applications Permissions

Traditional user-based permission system was such that it gave all privileges to all applications. But modern platforms have transformed into a new model. In modern application, each application has different set of permissions based on its functionality and requirements. Modern platform functionality has advantage over traditional one. But it works on one simple assumption that users take the permission list displayed seriously. It assumes that users read and understand all permissions then only accept to install the application. Surveys were performed on two platforms; those were Google Chrome extension system and Android OS. The permission requirements are collected from all Google Chrome extensions and Android applications. From this collected data, it is checked whether these permissions are effective in protecting users from the security risks. [6]

2.4 Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints

Android is an open source operating system in which developers can easily develop applications and users can easily install and use the applications. But allowing users to install third party application poses security risks. Existing security mechanism in Android displays a list of permissions which that application requires to the user. If user wishes to install that application he has to accept all the permission; otherwise he cannot install the application. There is no option of granting some application and rejecting other. There is also no mechanism of restricting the usage of few resources based on runtime constraints like location, time etc. Apex is a policy enforcement framework that allows users to grant permissions selectively and also impose runtime constraints. Users can set these constraints using simple user interface. Framework is implemented by doing minute change in the existing framework of Android. [8]

3. EXISTING SYSTEM

Smartphone have become very important part of everyday life. On one hand Smartphone has eased a man's life and on other hand it has increased security risks. The GPS unit in the mobile phone if kept ON can tell exactly where the user is, while the microphone can record audio, and the camera can record images. Through SMS messages, phone calls, and data plans, mobile phones are linked directly to some monetary risks. In such cases, there is an increase in user's monthly bill or confidential bank details may get leaked while the user may be using online payment facility. While installing Android application from Google Play Store, a list of permissions is displayed. This list gives details to the user of all the access which the application will require in mobile phone, for example, access to SD card, access to gallery, access to camera etc. Android relies on users to understand permissions and install the application only if acceptable. But researches and surveys have proved that user do not go through the permissions and directly install the application without being aware of the risks involved in that. Most users do not read permission as these permissions are in technical terms which are not understandable to ordinary user. An application is considered to be risky or not depends on user's privacy preference. Due to this, user end up downloading risky applications. [3]

3.1 Disadvantages of Existing System

- It presents permissions list in very technical way which is not understandable to the users.
- It allows users to install insecure applications which may cause damage to the system.

4. PROPOSED SYSTEM

In the proposed system, summary risk rating is displayed for each application. Comparison among the applications in terms of risk factor can be done using summary risk rating. Current permission information is ignored by the user as it is represented in stand-alone fashion. These permission list displayed in current system requires user to have technical knowledge. It is also time consuming, as user has to spend time in understanding each permission and compare with other application. In the proposed system, after installing an application, risk associated with that applications are displayed. User can choose whether to install the application or not. Risk rating is translated into categorical value such as high risk, medium risk and low risk. Also a numerical score is represented which is known as risk score. Using risk scoring function, percentile number denoting risk of the application is displayed. This risk score tells about the risk related to the application. This system provides comparative risk information. Risk information of each application can be compared. Percentile number is very easy to understand. A graph is represented showing the risk of application.

4.1 Advantages of Proposed System

- It represents permissions in simple way, so that user can ignore risky applications.
- Comparison between two applications can be done to find out which application is secure.
- It displays risk score in percentage, as well as categorizes application as high risk, medium risk and low risk applications.
- It displays graph to indication risk of application.

5. MODULE DESCRIPTION

5.1 Get Installed Applications

In this module it uses package manager to get the list of applications installed in the mobile. And when selecting the one in the list it gets the package name of the application and stores it in the variable and passes it to the next module through intent.

5.2 Permission List

In this module, the package name is got from the previous module. By using, the packageInfo built-in class available in android to get the permissions requested by that application. And then compares it with already inserted permissions and its associated risk and display the risk level.

5.3 UnInstall:

In this module, user can able uninstall the high risk application.

5.4 RiskDatabase:

In this module the database is created and the available permissions in android and its associated risk are stored. And the methods to insert, select, delete are made available so that other module use it by calling the method.

6. SURVEY AND RESULT ANALYSIS

Three experiments were conducted to know about users' knowledge about permissions and how participants understood risk score.

6.1 Demographics

A survey about risk communication was conducted on 50 participants. Out of the 50 participants, there were 29 male and 21 female. Out of 50, there were 25 in age group of 18-25 years, 15 between 26-40 and 10 were in age group 41 years and above. In 50, 56% of the participants have used an Android device for more than 1 year, 36% have used android device for less than 3 months and 6% of participants surveyed have never used android device. In 50, 36% of participants download Android application more than twice per month, 50% of participants download Android application, less than twice in a month and 14% of participants rarely download application.

Experiment 1:-

Android security system relies on the user to understand the list of permissions displayed while installing an application. The aim of this experiment was to know whether participants understood about the list of permissions which are displayed before installing any application. For this purpose, three pairs of similar applications from Google PlayStore were selected. One of the selected applications did not ask for any special permission and the other application asked for risky permission. In the first set of experiment, two similar game applications, Bubble Blast and Bubble Blast 2, are shown. Bubble Blast game ask for permission to access Photos/Media/File and Bubble Blast 2 does not require any special permissions. In the second set of experiment, two similar PDF Reader applications, PDF Reader – Scan, Edit & Share and PDF Reader, are shown. PDF Reader – Scan, Edit & Share asks permission of device & app history, Identity, Photos/Media/Files, Device ID and call information, Camera, Wi-Fi information. PDF Reader asks permission for Photos/Media/Files. In the third set, two similar applications of Android Tutorial, Learn Android Development and Developing Android Apps Basics, were shown. Learn Android Development asks for permissions to access Contacts, Location and Photos/Media/Files. Developing Android Apps Basics doesn't ask for any special permission.

App Choice Analysis:-

The main purpose of this analysis was to examine if the user is aware of the permission list. It was observed out of 50, 26 participants for set 1, 27 participants for set 2 and 18 participants for set 3, chose the application which did not ask any permission and 24 participants for set 1, 23 participants for set 2 and 32 participants for set 3 chose application which asked various risky permissions.

Table -1: Result Analysis of Experiment 1

Tasks	Set 1	Set 2	Set 3	Row Total
App without risky permission.(Low Risk)	26	27	18	71
App with risky permission (High Risk)	24	23	32	79
Column Total	50	50	50	150

It was observed that 47.33% participants chose applications asking no special permission and 52.66% participants chose application asking risky permission.

Questionnaire Analysis:-

The question to be evaluated is "What factors did you consider while choosing the application?" The analysis of the said question will tell whether the user is aware of the permission list and associated risk or not. It was observed as following:-

Table -2: Factors affecting selection of application analysis of experiment 1

Factors	% of participants chose
User Review	28
User Ratings	26
Permissions	14
Risk	10
Screen Shots	22

Only 10% participants chose risk applications considering the risk factor. Here, we can conclude that, since the permissions required were given in stand-alone manner, participants couldn't understand the risk associated with applications.

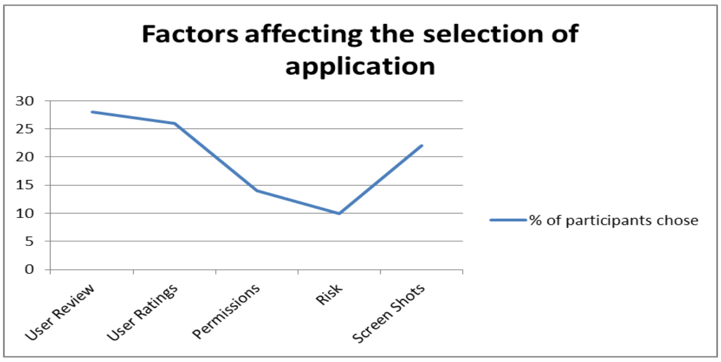

Chart -1: Graphical analysis of factors affecting selection of application of experiment 1

Experiment 2:-

The aim of this experiment is to examine how useful risk information may be for the user in selection of the application. In this experiment, three pairs of applications were presented to the user, one of the applications was low risk application and second one is high risk application. Risk was presented in percentage format. Participants have to choose one of the applications from the three set.

App Choice Analysis:-

The main purpose of this analysis was to examine whether the presence of a risk score influenced participants app-install decision making. It was observed that out of 50, 42 participants in set 1, 36 participants in set 2 and 30 participants in set 3, selected application with low risk and 8 participants in set 1, 14 participants in set 2 and 20 participants in set 3, selected application with high risk score.

Table -3: Result Analysis of Experiment 2

Tasks	Set 1	Set 2	Set 3	Row Total
App without risky permission.(Low Risk)	42	36	30	108
App with risky permission (High Risk)	08	14	20	42
Column Total	50	50	50	150

72% participants chose low risk application rather than high risk application and 28% chose high risk application. The results show that the risk score have significant impact on the participants' app selection, causing them to choose lower-risk apps more often.

Questionnaire Analysis:-

The question to be evaluated is "What factors did you consider while choosing the application?"

Table -4: Factors affecting selection of application analysis of experiment 2

Factors	% of participants chose
User Review	08
User Ratings	16
Permissions	18
Risk	52
Screen Shots	04

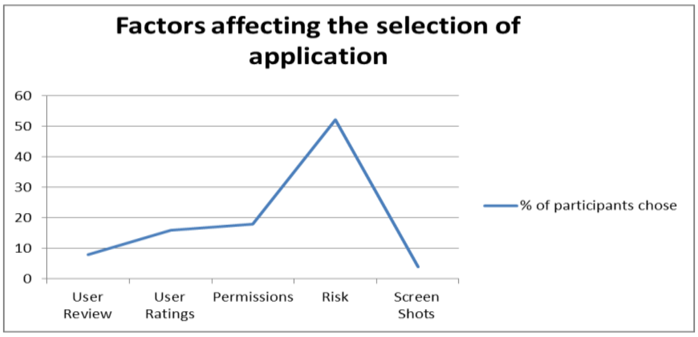

Chart -2: Graphical analysis of factors affecting selection of application of experiment 2

It was observed that 52% of participants chose risk as the factor they consider while installing the application. Subjective analysis demonstrates that, whenever risk was given, risk was considered to be important factor when selecting application for download.

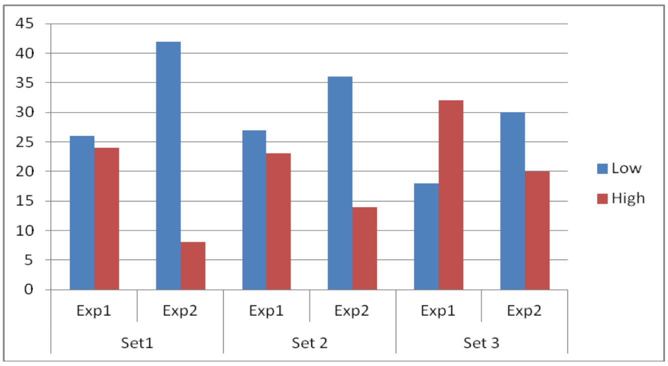

Chart -3: Graphical analysis of experiment 1 and experiment 2

Experiment 3:-

In risk communication, it is insufficient to just give information about risk to users. The important thing is how the risk is communicated to the user. The usability of the security information and how that information is presented to the user is equally important because its effectiveness depends on how the user comprehends and acts on the information. Risk score is represented in three ways. The first way is the one in which risk is represented as percentage, second is the one in which risk is represented as low mid and high, third is the one in which risk is represented as graph. The main aim of this experiment is to know which of the three methods is more understandable to the user.

Table -4 Choice of risk analysis

Type Age	Percentage	Low/Mid/High	Risk Graph	Row Total
18-22	16	06	03	25
22-40	04	08	03	15
40 and above	02	07	01	10
Column Total	22	21	07	50

It is observed that 64% of the participants' in the age group of 18-22 chose Percentage risk score as most understandable one. 70% of the participants' in age group of 40 and above chose Low/Mid/High as the one which can be more understood.

By using Chi-Square test it can be concluded that there is dependence between age and risk score preference. It can be inferred that participants' in age group of 40 and above preferred low/mid/high type and people in age group of 18-22 preferred percentage risk score.

7. PERFORMANCE ANALYSIS

To evaluate the performance of the application on the Android phone, different experiments were performed. All the experiments were performed on Lenovo K4 phone. To measure the energy overhead produced by proposed application, we performed following tests. We charged the battery of our device to 100%. We noted the change in battery for 100 minutes. 10 readings were taken in all. The readings were noted at an interval of 2 minutes. The values were noted and an average was taken for these 5 readings. During the experiment three system applications were run uniformly. Those were Calculator, Contacts and Browser and Email. For each application we performed common operations for all set of experiment. Addition of three digit number was done for Calculator, opening contacts and miss calling a number and opening Mumbai University home page for browser. This experiment was conducted for two types of environment: one is without installing the application and other is after installing the application.
The readings were as follows:-

Table -5 Battery Reading

Time Interval (in mins)	Battery reading without application	Battery reading after installing the application
0 – 10	99	97.5
10 – 20	98.5	95.5
20 – 30	95.4	94
30 – 40	92	91
40 – 50	88.2	87
50 – 60	86.4	85.2
60 – 70	85	83.4
70 – 80	83.8	81.8
80 – 90	82.2	79
90 – 100	80	77
Mean	89.05	87.17

From the mean, it is obvious that there is no significant difference between Average Battery before installing the proposed application and average battery usage after installing the proposed application. Hence, we can conclude that the proposed application doesn't have any energy overhead. Graphical representation also shows almost overlapping line which denotes that there is no significant decrease in battery due to proposed application.

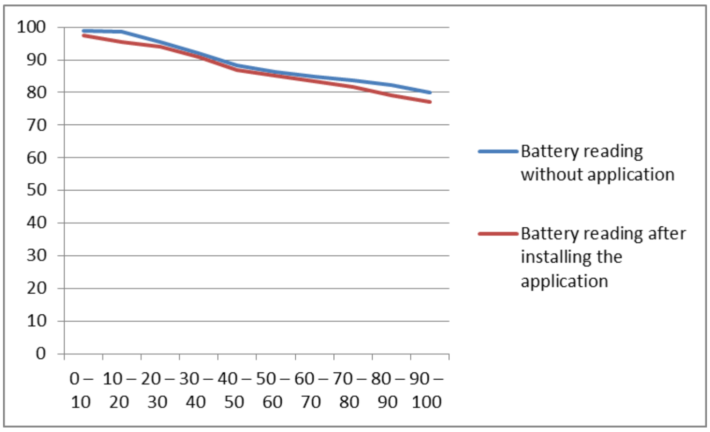

Chart -4: Graphical Analysis of Energy Overhead

8. CONCLUSIONS

Risk Communication is important mechanism in Android. When a user downloads and installs an application from Google PlayStore then a list of permissions is displayed. This list of permission is ignored by the users due to lack of technical knowledge. By using the proposed system, risk related to particular installed application is displayed. Risk is displayed in four forms: risk score in form of percentage, graph, low/mid/high and color. Risk is presented in such a way that it became easy for the user to understand the risk and prompts users to keep low risk applications and uninstall high risk application.

To analyze the efficiency of the proposed application, energy overhead was calculated. It was observed that the proposed application didn't create much energy overhead. A survey was conducted to check whether the users understood permission list better or risk score. Results of the survey showed that without risk score 47.33% of user chose low risk application and 72% of user chose low risk application when risk score was presented. It was also observed that, 70% of the users in age group of 40 and above preferred Low/Mid/High type of risk presentation. Hence, it can be concluded that representation of risk score helped user in using low risk application and uninstalling high risk application.

REFERENCES

[1]. XF. Xie, M. Wang, R. Zhang, J. Li, and QY. Yu, "The Role of Emotions in Risk Communication," Risk Analysis, vol. 31, no. 3, pp. 450-465, 2011.

[2]. Christopher S. Gates, Jing Chen, Ninghui Li, Senior Member, IEEE, and Robert W. Proctor, "Effective Risk Communication for Android Apps" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014

[3]. Kelley, P., Consolvo, S., Cranor, L., Jung, J., Sadeh, N., and Wetherall, D. "A conundrum of permissions: Installing applications on an android smartphone" in Financial Cryptography and Data Security, vol. 7398.2012, 68–79.

[4]. Adrienne Porter Felt et al, Android Permissions: User Attention, Comprehension, and Behavior, In SOUPS '12 Proceedings of the Eighth Symposium on Usable Privacy and Security, Article No. 3, 2012.

[5]. E. Chin, A.P. Felt, V. Sekar, and D. Wagner, "Measuring User Confidence in Smartphone Security and Privacy," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-16, 2012.

[6]. A.P. Felt, K. Greenwood, and D. Wagner, "The Effectiveness of Application Permissions," Proc. Second USENIX Conf. Web Application Development (WebApps '11), 2011.

[7]. Sachin Bhokare, "Effective Risk Detection and Summary Risk Communication for Android Apps", International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2014

[8]. M. Nauman, S. Khan, and X. Zhang, "Apex: Extending Android Permission Model and Enforcement with User-Defined Runtime Constraints," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), pp. 328-332, 2010.

[9]. M. Backes, S. Gerling, C. Hammer, M. Maffei, and P. von Styp-Rekowsky, "AppGuard—Real-Time Policy Enforcement for Third-Party Applications," Technical Report A/02/2012, Saarland Univ., 2012.

[10]. Jinseong Jeon, Kristopher K. Micinski, "Dr Android and Mr Hide: Fine-grained security policies on unmodified Android."

[11]. V.Hemalatha, K.S.Hemapriya, P.R.Joshna, S.T.Santhanalakshmi, "Computing Malware Scores for Mobile Applications", International Journal of Engineering Research.

BIOGRAPHIES

Mr. Hari Rajai is an android application developer, currently a PG Scholar from ARMIET College, Department of Computer Engineering. He is currently working as a Teaching Assistant in K.C. College of Engineering & Management Studies & Research

Mr. Sachin Bojewar has 25 years of rich teaching experience and is currently working as an Associate Professor in Vidyalankar Institute of Technology