International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Detailed Analysis of Various Android Application Permissions: Problems and Solutions

Mohinder Kumar

Assistant Professor, Department of Computer Science and Applications,

Panjab University Regional Centre, Sri Muktsar Sahib

ABSTRACT

In this paper I have put my effort to describe the various security issues regarding the installation of Android applications. The main concern is that everything in the private Android mobile device is not private to user that holds the device. So being a wise head on ones shoulders one must be very particular about the data that he contains in the device. Every one today has some kind of Android mobile device and everyone wants to utilize most of the facilities available in the market of Android applications, like access to the internet banking, mobile banking, social web sites, online shopping web sites, dialers, messages, games, and even customized device configurations applications. Every kind of these utilities is available in the form of small application software that is known as App. To make use of these small applications one must install these applications on ones device before using that various applications that a particular app provides. But the first step to install these applications is very crucial from the security point of view. It is very important that from where we get that application software either it is available on some authenticated market store or any unknown web site; either it is free or paid etc. It is generally noticed that each one of us just goes to the internet, finds the app and install it from any web site where it is available. But that application can cause a security breach in your personal, official or any sensitive data that is available in his/her android phone or on the web site that he/she accesses from that android device. Everyone has a strong belief that the Android operating system is secure enough to protect everyone's personal data, or one can think that an application is available only after a lot of testing being performed by the applications market. It is true to some extent because fortunately the architecture of the Android operating system is so secure that every application cannot share data with another application. But to complete the various tasks an application needs a numbers of permissions from the user of that application. So ultimately the choice of permissions is up to the user and he/she must be aware of these permissions that what potentials a permission can have or not. So to make an optimal decision the various security issues are needed to be discussed with the society that includes our students, parents or even teachers that are very new to this modern market of Android applications.

I. INTRODUCTION

The various topics discussed in this paper are:

1) What are the Android application permissions
2) Why these various permissions are not secure
3) How to check android application permissions
4) Authentic and non-authentic web application store

5) Paid vs. free application permissions
6) How to manage Android application permissions
7) How to control Android application permissions
8) How to protect oneself
9) Solution in Android 5.0 Lollipop
10)Conclusion

II. WHAT ARE THE ANDROID APPLICATION PERMISSIONS

The permissions of an android application are something like access rights that are required by an android application to complete its task so that the user is well satisfied with the purpose for which he/she has installed that particular application. For example Google Maps demands the access rights to the exact location of an android device to show the exact position on the map. Each Android application operates in a sandbox therefore it is not possible for an application to interfere with another application's data. But an application must have to share some data with another application like Message application requires the contact information from Contacts application. So this is achieved by an application by declaring the permissions to add some additional capabilities[4][1][12]. These permissions are the part of android API and are defined as constants in the android API.To get the list of these constants follow this link http://developer.android.com/reference/android/Manifest.permission.html.

As an Android application developer these permissions are defined for each application using the **<uses-permission>** element in AndroiMenifest.xml file. As part of the security model, uses-permission tags declare the permissions you've determined your application needs to operate properly. The permissions you include will be presented to the user before installation commences. The permissions are required for many of the native Android services, particularly those with a cost or security implication (such as dialing, receiving SMS, or using the location-based services) [9].

<uses-permission android:name="android.permission.ACCESS_LOCATION"/>

The third party application developers can also define their own permissions with the help of **<permissions>** element to provide access to their component. The example of such permission element is

```
<permission android:name="com.paad.DETONATE_DEVICE"
android:protectionLevel="dangerous"
android:label="Self Destruct"
android:description="@string/detonate_description">
</permission>
```

There the description is visible to the user before installation of such application. The protection level can have the following values:

Table1.1 Protection levels of the permissions defined by the third party applications

Value	Description
Normal	A lower risk permission that is granted automatically by the AOS. But the user can review these permissions before installation
Dangerous	A higher risk permission not granted automatically by the AOS. The confirmation of the user is mandatory for such application.
Signature	A permission that the system grants only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.
signatureOrSystem	A permission that the system grants only to applications that are in the Android system image *or* that are signed with the same certificate as the application that declared the permission

III. WHY THESE VARIOUS PERMISSIONS ARE NOT SECURE-

The following table describes permissions the constants that falls in the "dangerous" protection level[15]:

Table 1.2 Permissions constants having "dangerous" protection level

Permission	Why Risky
AUTHENTICATE_ACCOUNT	Allows an application to act as an AccountAuthenticator for the AccountManager. Can be used for **phishing**
CALL_PHONE	Make phone calls that cost money and such an app can make the entire process automatic or hidden
SEND_SMS	Send SMS or MMS that can let an application send SMS on user's behalf. Can cost **a lot of money**
WRITE_EXTERNAL_STORAGE	Modify/delete SD card contents like pictures, videos, audios or documents etc.
READ_CONTACTS/ WRITE_CONTACTS	Use the contact list for read and write contact list respectively. Can be used for fake email **(spoofing)**
READ_CALNEDAR/ WRITE_CALENDAR	Read and Write calendar events that can contain contacts data as well
READ_HISTORY_BOOKMARKS/ WRITE_HISTORY_BOOKMARKS	Read/Write user's browsing history and bookmarks
READ_LOGS	Read the log files of other applications which included keystrokes—meaning your passwords and logins were included in this file
GET_TASKS	Useful to steal data about what the applications are running on device
SYSTEM_ALERT_WINDOW	A malicious developer/advertiser could use it to show very obnoxious advertising.

CAMERA	This can be used maliciously to snap unsuspecting photos
ACCESS_MOCK_LOCATION	Allows an application to create mock(fake) location providers for testing
CHANGE_CONFIGURATION	Allows an application to change locales settings like language settings etc.
CLEAR_APP_CACHE	Can slows down some applications
MOUNT_FORMAT_SYSTEMS	Can format the external storage
PROCESS_OUTGOING_CALLS	Allows an application to monitor, modify, or abort outgoing calls.
WRITE_SECURE_SETTINGS	Allows an application to read or write the secure system settings. For rooted phones, you should avoid apps that request this permission
READ_PROFILE	Allows an application to read the user's personal profile data.
READ_SMS	Can read the private information from SMS
WRITE_PROFILE	Can write contacts in contact list "me"
READ_SOCIAL_STREAM	Allow an app to read updates from social networking apps like Google+, Twitter, and Facebook
READ_ATTACHMENT	Can read the mail's attachment files
RECEIVE_MMS	Allows an application to monitor incoming MMS messages

Permission Groups (a simplified permissions on Google Play)

Google Play has combined these various permissions into groups that have made the tasks of permissions selection very easy to some extent. But more consciousness is needed when a particular group is present instead of individual permissions. Although the user can see the individual permissions under each group. All the permissions are categorized in to the following groups:

Table 1.3 Permission groups

Permission Group	Important Capabilities
In App Purchase	One can buy in app items like sword, key, virtual currency, find out in app offers, redeem in app promotional codes, refund and purchases.
Device & app history	App can read sensitive log data/system internal state/web bookmarks and history/running apps
Cellular data settings	App can control mobile data connection
Identity	App can read/modify/delete profile accounts, read/modify your own contact card
Contacts	App can read/modify contacts
Calendar	App can read/add/modify calendar events and can send email to guests without user consent
Location	App can access precise location address
SMS	App can receive/read/edit/send SMS/MMS

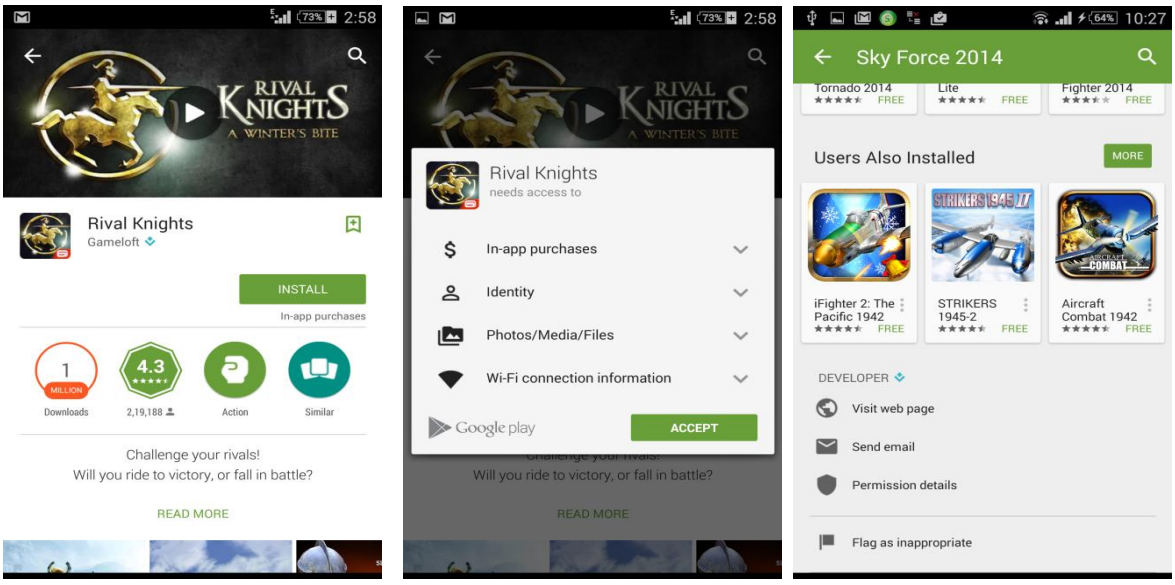
Phone	App can call, read/write call log, reroute outgoing call, make call without intervention
Photo/Media/Files	Read/modify/delete USB contents, format/mount/unmount external storage
Camera/Microphone	App can take/record pictures/audio/video
Wifi Connection Information	App can view Wi-Fi connections
Bluetooth Connection Information	App can broadcast/receive info from nearby BT devices
Wearable sensors/activity data	App can access data from wearable devices
Device ID & call information	App can read phone Id and status(number of call etc)
Other	App can read/write social streams

IV. HOW TO CHECK ANDROID APPLICATION PERMISSIONS

4.1. Checking permissions before/after installation

a. Before installation

In the latest Android devices the permissions are displayed after the user presses the install button (before accepting), but he/she can display the permissions list before pressing the install button by scrolling down the page and pressing the **Permissions details** link[12][13][14].



(a) (b) (c)

(a)First screen contains install button (b) after install but before Accept the permissions list is displayed (c)At the bottom of the first screen Permissions details link

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

b. After installation permissions can be checked by following the steps:

1) Click on Settings

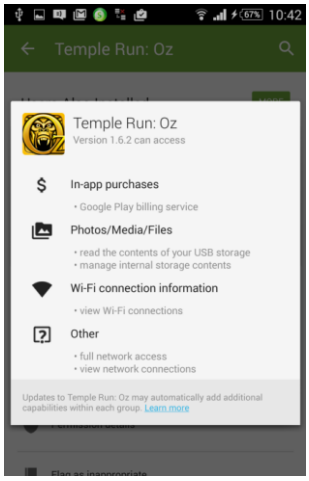
2) Select Apps under Device tab

3) Select the particular Application

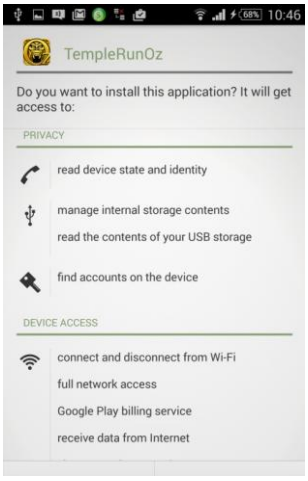
4) Scroll down to see the permissions

V. AUTHENTIC AND NON-AUTHENTIC WEB APPLICATION STORE

One can see the clear difference between the permissions of an authentic and non authentic web app store. Here the snapshots of the same game Temple Run Oz are displayed. The left one is from Google Play Store and the right one is from play.mob.org [6]. The second one demands more dangerous permissions like read device state and identity, find accounts on the device etc.



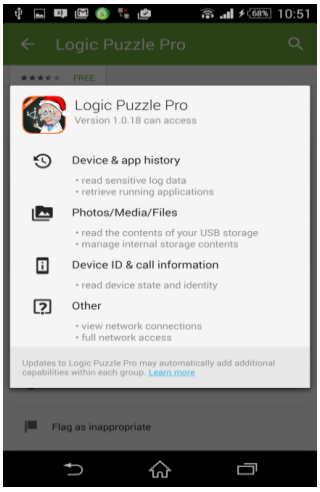
(a) Google Play Store



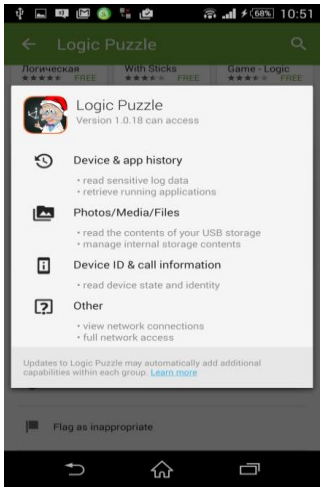
(b) play.mob.org

VI. PAID VS. FREE APPS ON AUTHENTIC WEB STORE (GOOGLE PLAY STORE)

One can see that permissions from paid and free versions are similar if the app store is authentic like Google Play store



(a) Paid version



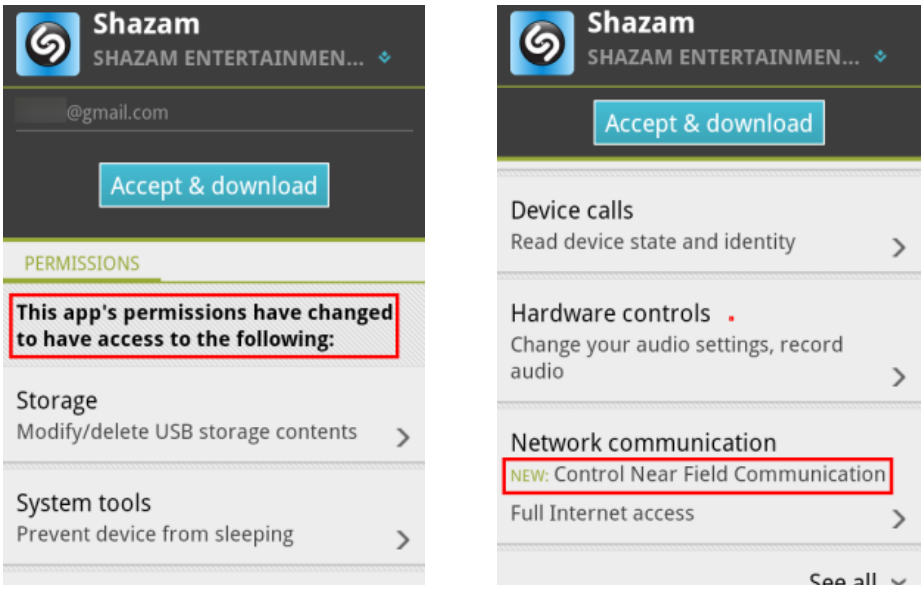
(b) free version

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

VII. MANAGE PERMISSIONS

Manual vs. Auto Update

Even though the Apps can be updated automatically that save a lot of time but even some of the Apps demands manual update because the developer of these Apps have added some new permissions and if someone ignores the permission at this time ,can be in grate trouble. By carefully watching one can see that every new permission is prefixed with **New** word.



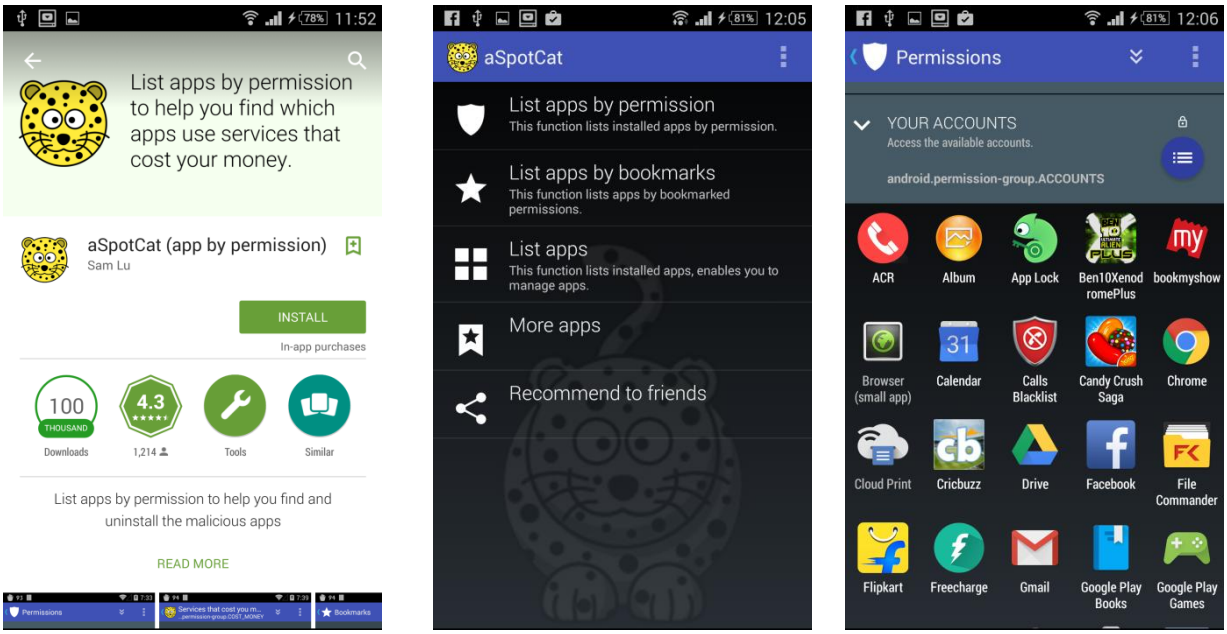
It is safer to turn off the auto update option. To make this option off execute the following steps:

1) Open the play store
2) Go to My apps
3) Select any App
4) Touch the Menu
5) Uncheck Auto-update

VIII. HOW TO CONTROL ANDROID APPLICATION PERMISSIONS

Unfortunately there is no direct way to turning on/off individual permission until the device is not **rooted**. There are some apps that allow the user to have a greater control over permissions like the Permission Manager [free App on Google Play Store is available to manage the application permissions in your device. This app will present you with a list of apps from where you can choose an app to alter its permissions[4]. You can turn individual permission on or off by swiping. This app will list the top 5 apps with the most numbers of dangerous permissions. The pro version lists all such apps. The red border signifies a dangerous permission, a yellow one a normal permission and green a completely safe app.] and The Permission Denied [A paid app for permission controlling.] Although to root a device has its own advantages and disadvantages. But fortunately the user can analyze the permissions of his/her device with some available apps like aSpotCat (no root is required). The aSpotCat is an app that Lists the apps by permissions, by bookmarks etc. One can easily check which apps are dangerous and which are not by analyzing this app.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



(a) (b) (c)

(a) the a Spot Cat app (b) Various options to analyze permissions (c) all apps that access the user account information

Depending on the analysis one can easily come too the result that which apps are more dangerous or which are not[10]. For example in the (c) snapshots all the apps are displayed that can access the account information from the device so all these have potentials to breach the security of the user.

IX. HOW TO PROTECT ONESELF

For those who are not interested in too much technical aspects can also protect themselves by following these very simple tips

9.1) Install app from an authentic web store

The first step must be wise. Always download the apps from trustworthy and authentic app stores. Here a list of some popular and safe app store is given:

- Android (Google) Market
- Amazon AppStore
- Sony App store
- SlideMe
- Archos AppsLib
- Motorola's Market

9.2) Comments are very useful

The review comments of the users are very important and must have a look on these comments[2][3][9]. Not only the top three are but go through these comments and see what the views of all are. These review comments are also important when the user is going to update an app because updates must be treated as a fresh installation. It is possible that an app has added more permission than the previous version. In such case automatically update is off and the user has to update the app manually. So this time also review comments are important to see.

9.3) Rating of an app is crucial

Every app has some rating between 1 to 5 stars. An app having rating 3 to 5 are safer. So always prefer an app having a good star rating.

9.4) Permissions should be checked before installation

An app can do a number of things when it is installed in one's device. So try your best to check the permissions and understand the reason why these permissions are required. For example a game that wants to access your contacts is questionable every time. In such case one can ask the reason to the developer by emailing[2]. If the developer justifies all the permissions then one can go for installation of the particular app.

9.5) Developer's web site is available

It is always better to check whether the developer has a web site or not .For example Bookmyshow app has a web site so it is treated as a safe and well established app. Many of the banking apps are also fallen under this category[3].

9.6) Update app must be taken as fresh installations

When you are going to update an app be sure to read the permissions, comments, and rating etc. if the updates are manual then it is sure that app demands some new permissions. So have a deep look on the permissions.

9.7) Public Wi-Fi is not always secure

Public Wi-Fi are not always safe so whenever you use public Wi-Fi access ,nerve use a web site than demands username or password .it is a good practice to check the phishing in such case by mailing to your friend.

9.8) External storage is never Secure

Many of the apps can read/modify and delete the data on the external storage so external SD cards are not the safer place to store the information like backups of contacts etc.

9.9) GPS and Location apps

One must treat the location tracking with care and be sure to give it only the most trusted party like Google Map.

9.10) Post your own comments

One must post his/her own comments and rate a particular app. These descriptions are visible to all users. If you found a good or bad app you must rate and comments it according your experience[12]. It will help to all.

X. SOLUTION IN ANDROID 5.0 LOLLIPOP, 6.0 MARSHMALLOW AND 7.0 NOUGAT

Although not much steps have been taken by the Google to have more control over the application permissions but some new policies might make the user safer. For example the apps from Google Play always verified by Google to protect you and your device from harm. By default, your device does not allow the installation of apps from sources other than Google Play. That means if you choose allow the installation of apps from sources and install apps from sources other than Google Play, it is more likely that apps will be installed that could harm you or your device[7]. If you allow the installation of apps from unknown sources, then Verify Apps feature protects you when installing apps outside of Google Play by continually checking your device to make sure that all apps installed are behaving in a safe manner, even after installation. The detail of how this works can be found under the **https://support.google.com/nexus/answer/2812853** link [11][15].

The Android Lollipop also put a new security barrier for third party applications. Now the user can allow only a single folder under external storage to use for an application not the entire external storage. The folder can be any of the user's choice. This will also help to protect the external storage data from the privacy point of view.

The Android Marshmallow has put more control over apps permissions by providing some new methods. First of all the apps are required permissions as when they need not at time of install and one by one. So the user can deny if any risky permission is demanded. Most of the apps run without any error even after not assigning all the permissions. That's great. And these permissions for any app can be viewed within the settings menu which shows the permissions the app does or doesn't have. You can also view it by permission type that lets you see how many apps have access to the same thing such as contacts.

In Android Nougat 7.0 the security is improved as for as the permissions are concerned.

Android devices come with built-in software called Verify Apps, which regularly checks to make sure all apps are behaving on your device. If a harmful app is detected, Verify Apps will display an alert, or block the app entirely. Android 7.0 allows users to turn app permissions on and off at will, providing more control over privacy than ever before. For example, you can now allow an app that takes photos to access your device's camera, but not its location or other private information.

XI. CONCLUSION

Everyone with an Android device should know that your private information isn't treated as private. A user can ask that why every app demands so many permissions and do every app uses these permissions. The answer is that these app demands these permissions because they cannot complete the user's task without these permissions. But the apps must be installed from safe web stores and authentic online market .However the user has not full control over these permissions without some technical knowledge. But ultimately it is up to the user what to download and what to not, and this is the most important thing he/she must need to remember.

REFERENCES

[1] Kim J, Android App Permissions and Security : What You Need to Know, Wireless Security, 2014

[2] Unuchek R, All About Android App Permissions, Kaspersky Lab, 2017

[3] Z Fang, Ying Li et al Permission Based Android Security : Issues and Countermeasures,ResearchGate, 2014

[4] Wei Wang,How to Manage Android App Peermissions to Protect Your Privacy, 2015

[5] Y. Zhou, X. Jiang Systemetic Detection of Capability Leaks in Stok Android Smartphones, ResearchGate,2012

[6] J Hildenbrand,Android App Permission- HowGoogle Get it Right, Androidcontrol, 2012

[7] Timothy Vidas, Nicolas Christian, Lorrie Cranor , Cubing Android Permission Creep, ResearchGate, 2011

[8] C Marforio, A Francillon, S Capkun, Application Collusion Attack on the Permission-Based Security Model and its Implications for Modren Smartphone Systems, ResearchGate,2012

[9] A Souppouris,How an Android app could transmit your personal data without any permission, , The Verge,2012

[10] A Rodriguez,Android's Permission Problem, PC World, 2012

[11] Letterbug et al. Six key security features in Android Marshmallow 6.0 , ReserahcGate 2016.

E Books References

[12] Professional_android_4_application_development by Reto Meier Wrox Publisher

[13] How has Android Nougat security improved? By Jack Wallen

[14] Android Lollipop 5.0 Quick start guide by Google

Online Web Sites for References

[15] www.androidpermissions.com

[16] www.developers.android.com

[17] www.play.google.com

[18] www.androidforums.com

[19] www.support.google.com