Android App For Automatic Malware Detection via Reviews and Permissions

Pramila Kumari, Ramniwas Gujjar
Dept. of Computer Science & Engineering. St. Margret Engineering Collage, Neemrana, Rajasthan, India

Abstract*—In this paper a new technique is stated True App which will be used in the Automatic Malware Detection. "True" is that the truth, a word that itself depicts that it don't lies. "App" is any application; here it's a mechanical man application.*

In our app we have a tendency to be serving to our users in police investigation any harmful application. The users don't seem to be tuned in to the intensions of the developers WHO somewhere aiming to fetch your necessary files, deleting your knowledge, etc." true app" can facilitate these sort of users in police investigation any app that is already put in in there mechanical man phones or are aiming to install any new app in their phones. All the knowledge of the put in apps is saved on a server. The knowledge fetched from the server is going to be within the type of: package details, version range, installation and last changed dates, permission supported these permissions the malware ratings are given to every application.

If user attempting to put in any new app then an alert message relating to the confirmation can get displayed and at that time the knowledge are going to be accessed from the server.

Keywords—android, malware, mobile operating system

I. INTRODUCTION

Being a mobile operating system, android OS is a modified version of Linux, originally developed by a start-up, Android, Inc. As Google entered mobile market, it purchased Android and in a bid to encourage independent development works, it released the developer tools under the open source Apache License. The permissive licensing allows the OS and related software to be modified and distributed by enthusiastic developers, network operators & device manufacturers.

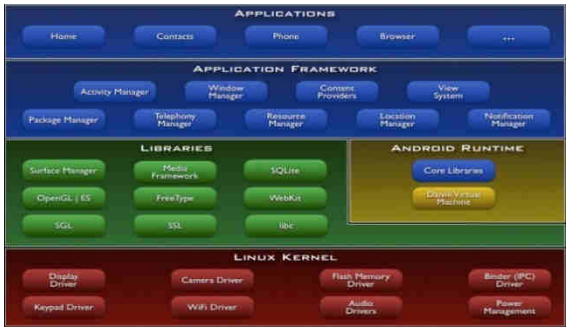

Fig. 1-1: Android Architecture

Android app permissions aren't requests, they're declarations. Unless you're rooted, you have no say – short of choosing to not install the app – in whether the app will receive all the permissions it requires.

When you install an app from the Play Store, you'll get a pop up listing all the permissions that the app requires things like access to your storage, phone calls, network communication etc.

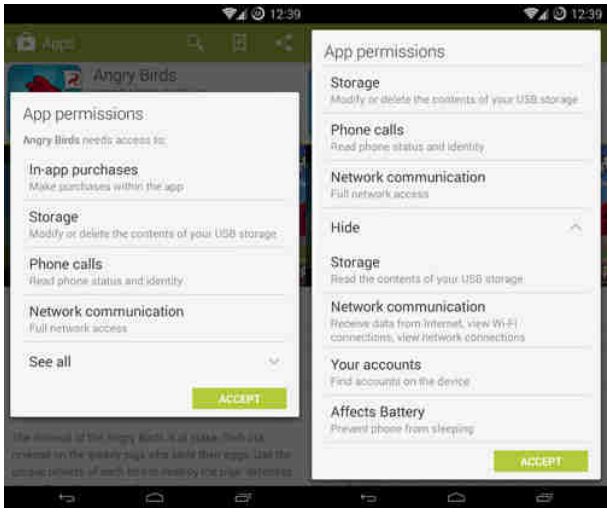

Fig. 1-2: Android Permissions at the Time of app Installation

It is comparatively to consider that the permissions list such as EULA (which means that nobody ever reads) but skipping of over these of the permissions could mean the differences between such as having the data securely on

the device or having all of it on the fingertips of the unscrupulous application developers.

5 Permissions You Should Be Wary Of

There are the few of the permissions which you should be wary of, and not because of they are necessarily dangerous, but also because there could be the wide-ranging repercussions if the data from these of the permissions were to fall into the incorrect hands. And also note that these are not of the only permissions that you should worry about and it's a start.

1. Location

There are two of the types of location permissions which an Android applications can require: one is "approximate location (network-based)" and the other one is "precise location (GPS and network-based)".

And what would the apps need my exact location for? And well, the navigation apps like Waze which will require such of the information to work. And similarly the social media applications which want to includes your location in the photos and in the uploads. And the applications which implements the location-based advertising will also require the access to such of the information. It is just one of the many of the sacrifices which you have to make when you are using the free or an ad-supported application.

2. Phone Status and Identity

This is the bit of the problematic permission, and because the "read phone status and identity" will encompasses everything as innocuous as needing to know when the phone call is coming in, or to having access to the crucially important data such as your mobile IMEI number.

And while this permission is so often safe, and the potential for wrongdoing is also huge, so you have to do exercise caution when applications which require this permission. And if there does not seem to be any of the real reason for the application to require this permission, then it might be a good idea to consider twice before of installing such of the applications.

3. Read and Modify Your Contacts

This permission which is required to "Modify your contacts, and read your contacts" will give the application unfettered access to your contacts information database. And while both can be problematic, and the "modify" permission is also especially it is dangerous since it would let application will read all the contact information which have on your phone. And it includes how often you can communicate with particular of your contacts.

The SMS apps, the contact management apps, the dialer replacement applications and even some of the social media applications will now requires almost both of the applications, but applications which are without any of the social aspects to them for these permissions.

4. SMS and MMS-Related Permissions

These permissions could potentially cost you about lot of the money, if the malicious applications use these permissions to send the illegitimate SMSes or tack on the extra charges onto each of the SMS and the MMS you send.

The permissions like "read your text messages" and the "receive text messages permissions" can also be potentially dangerous and can results in your privacy being compromised. And if there is no actual reason for applications to require these permissions, then you can avoid it.

However, there are perfectly valid reasons for an application to require these permissions, and especially if it's an SMS application. And again, a bit of reasoning will save you and your phone to be harmed by such applications.

5. Account-Related Permissions

The Permission like "Find accounts on the device" will let the application check with the Android's built in Accounts Manager on whether you have any of the accounts on services such as the Google, the Facebook and so on.

The permissions like "Use accounts on the device" will let the applications ask for the permission to use the accounts. And once this permission is then granted, the application won't then have to request for it again; and the concern, of course, comes if the application is malicious and then continues to do things in the background in your name.

And another of the related permission to watch out for is the "create accounts and set passwords", one which lets the application authenticate the credentials. And the malicious application can take the advantage of this permission to get into your password by phishing your details.

Ways to Stay Safe

There are the few things which you can do to stay on the top of the application securities permissions but instead, in order to look at the application itself and the use of reasoning to figure out whether the application really requires these of the permissions.

And you can also send the email to the developer of the application asking about the permissions. And if the reply isn't satisfactory, or if you don't get the reply at all, then you can avoid installing the application.

And you should also take the advantage of the huge of the Android community if you are unsure about the security of the particular application. And read the reviews on the Play Store and also check the forums and the Android-centric news sites to see that if there have been any of the complaints about the app recently. And also it's a bit of the work, sure, but better be safe than to feel sorry.

Managing App Permissions

And if you've let applications have access to any of the accounts such as the Facebook or the Google, it is good

idea to go to your account settings and then manage your account permissions, if the website also has such of the feature.

And you can also check that what the permissions certain applications have by entering into the menu Settings > Apps. And just select the application and scroll down to see what the permissions application has.

Permissions Manager Apps

And you can also use the application such as the Permission Explorer, which lets you filter by the categories, the applications and the permissions, and can give you more detailed 19categorization of the permissions granted to the application. And other similar applications which you can try are the Permissions Observatory and the App Permissions.

And regardless of the application you can choose, and spending some time in going through all of the permissions of applications currently installed on the Android device should help you in establishing whether that there are any of the applications with the problematic permissions and that need to be revoked or also perhaps even to be uninstalled entirely.

Revoking App Permissions

And once you have found some of the offending apps, it is the time to decide on the course of action. And there's currently no direct way or method to manage application's permissions in the latest version of the Android, since Google chose to remove AppOps feature from the Android 4.4.2.

However, if your device still running on the Android 4.3, it wouldn't hurt to give the AppOps a go to see that if it helps you to access the built-in permissions manager.

And if you are running the stock, or the unrooted 4.4.2 (or the version prior to 4.3), then you're pretty much out of the luck when it comes to revoking application permissions short of the completely uninstalling the application. And however, if you having the rooted device, then you have few more of the options.

Permissions Manager Apps (Rooted)

If you on your device the Exposed Framework installed on it, then you can give Xprivacy and Xprivacy is among one of the best permissions manager applications which are available, letting you to tweak, to block and even to revoke almost every of the permissions an application might require. And you can also use Xprivacy Installer in order to help you install both of the Exposed Framework and the Xprivacy itself.

And if you are willing to install the completely new ROM, or even plan to do so anyway, then there are also certain of the custom ROMs that come with the permission management features which is built-in.

One of the popular one is CyanogenMod has the feature Privacy Guard one which, as of last year, also comes with Android 4.3's and the AppOps integrated into it. Also the other ROMs such as the Purity ROM also have the similar feature. [1]

II. IMPORTANCE AND RELEVANCE OF THE STUDY

There are many definitions of malicious software, malicious code, and malicious content, often called malware. Two similar definitions of malicious code and malicious software that are feasible for this thesis are noted below.

1. Malicious code is defined as:

Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computing system encompasses Trojan horses, viruses, worms, and trapdoors.

2. Malware is defined as:

Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do. In the digital world developing and distributing malware is of interest to individuals and organizations with unethical or illegal intentions.

A few examples of malware behaviour are to:

• Delete crucial files on a computer to render it unusable without a recovery process.

• Log every keyboard input to see what the user's type.

• Steal personal or sensitive information or files from a computer.

• Use a computer's resources for the purpose of the malware, e.g. send spam emails,

DdoS another system, or brute-force encryption keys.

Often, the malware author will want to maximize the spread of the malware and will look to implement a mechanism where his software can copy itself to other, similar devices.

Malware provides no legal notice to the affected user. This threat includes Trojans, worms and viruses.

The implementation of malware detection systems in mobile devices is also a relatively new plan. Security tools and mechanisms used in computers don\'t appear to be doable for applying on smart phones as a results of the excessive resource consumption and battery depletion. Hence, we've got an inclination to determined to perform the entire analysis technique on an obsessive remote server. This server area unit about to be used exclusively to collect information and observe malicious and suspicious applications at intervals the golem platform.

Their framework consists of the many parts which supply enough resources and mechanisms to look at malware on the golem platform. First, we have a tendency to've

developed a light-weight shopper referred to as Crowdroid, which can be downloaded and place in from Google\'s Market. This application is answerable of look UNIX Kernel system calls and deed them preprocessed to a centralized server. In line with a crowd sourcing philosophy, users will facilitate with deed non-personal, but behavior-related data of each application they use.

Another Paper is "A Survey on machine-driven Dynamic Malware Analysis Techniques and Tools". This survey article provides a top level view of techniques that area unit supported dynamic analysis that area unit accustomed analyze probably

Malicious samples. It to boot covers analysis programs that use these techniques to assist a person\'s analyst in assessing, throughout a timely and applicable manner, whether or not or not a given sample deserves nearer manual review as a results of its unknown malicious behavior.

This article focuses on the techniques which can be applied to research potential threats, and discriminate samples that unit mere variations of already known threats. To boot, it presents the presently offered tools and their underlying approaches to perform machine-driven dynamic analysis on likely malicious code.

Analysis:

Smartphone platforms have become a lot of and a lot of widespread lately. To shield sensitive resources within the smart phones, permission-based isolation mechanism is employed by fashionable Smartphone systems to stop untrusted apps from unauthorized accesses. In Android, Associate in nursing application has to expressly request a collection of permissions once it's put in. However, when permissions square measure granted to Associate in Nursing application, there's no thanks to examine and prohibit however these permissions square measure utilized by the app to utilize sensitive resources. Whereas these malware apps square measure clear examples containing undesirable behaviors, sadly even in purportedly benign applications, there might even be several hidden undesirable behaviors like privacy invasion. This paper can provide a systematic approach to malware analysis. A study of malware and dynamic malware analysis are going to be performed. I will be able to attempt to propose a brand new framework supported recording equipment approach to get and analyze golem application's activity. It'll be capable of identifying between benign and malicious application.

III. IMPLEMENTATION

To extract info from barely purpose on the truapp, we have a tendency to should bit the screen for a second resulting in generation of a dialog. The read connects to the server giving all the knowledge for the app.

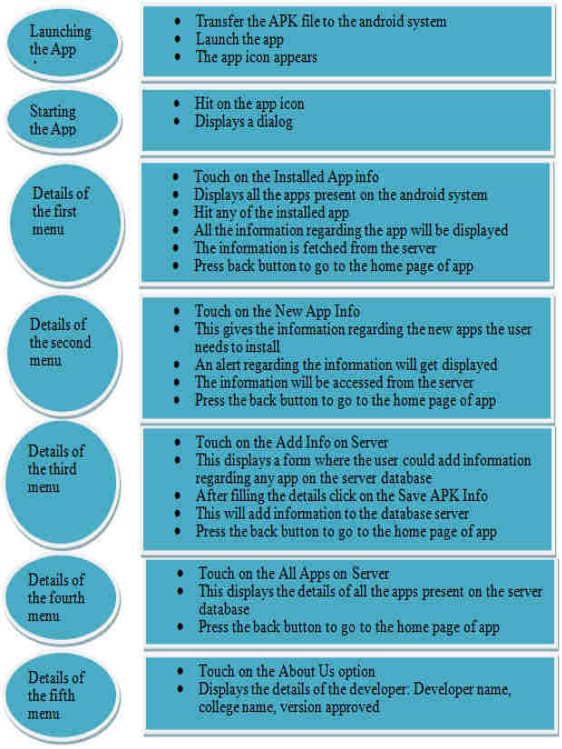

Fig 1.3: Workflow of truapp

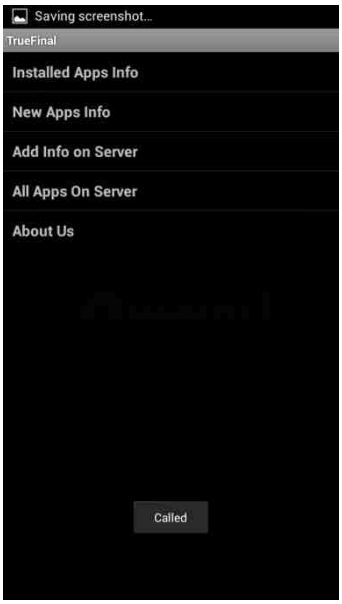

Fig 1.4: Application Homepage

Software modules being used in Android application can be better described in form of different activities used. An Activity is a library entity which describes the response of a layout to the user behavior i.e. serves as an interface. The behavior or activity is defined through a class file and an associated layout. Multiple activities have been use here so as to handle different functional requirements:

a. AboutUsDemo.java

- Shows the information of the developer name, college name and the version approved.

b. AllAppsActivity.java

- Shows all the details of the installed apps. These details can then be fetched on our android device by clicking on app. This stores the details of the app like app name, company name, app id, app rating, etc

c. ApkAdapter.java

- The adapter acts as a bridge between adapter view and the underlying data for that view. Here it is retrieving various kinds of information related to the application packages that are currently installed on the device.

d. ApkInfo.java

- This will set values to each app regarding its version, modified date, ratings, etc.

e. ApkData.java

- This will store all the data in the form of packages so that it could be accessed easily.

f. ApkInfoActivity.java

- This describes the information of the new apps to be installed on an android device of a user. The data is fetched from a server and an alert regarding the new app get displayed.

g. InsAppDemo.java

- This describes the permissions allotted to every application so that user could be aware of the app that it is either safe or not.

h. JSONParser.java

- Important class used to define the behavior of the entity which would handle the transaction with remote server using network connection
- Data is formatted as Java Script Object Notation (JSON) objects.
- The method getServerResponse (url, method, params) returns a JSON object.
- If the method is “POST”, then an Http Client is used to simply send instructions or data contained in “params” to the remote server designated by “url”. The response received contains no appreciable data apart from success or failure execution information when this connection method is used...
- If the method is “GET”, then an Http Client is used to simply send information contained in “params” to the remote server designated by “url” and the response is received from the server containing required data when this connection method is used.
- The response received is built to strings and encoded into JSON format to be parsed latter by other object so as to retrieve information.

i. NewApps.java

- This tells about the new application’s information. Here the user itself can add information for any application and can save this information on the server. If any user is trying to install the new app the alert regarding that application is shown.

j. SearchAppsActivity.java

- This will generate a list of all the apps consisting of their details in the form of strings. Whenever user is searching for any app the information is displayed form the server regarding the app.

k. ServerApp.java

- This tells about the applications which are on the server.

l. TrueFinalActivity.java

- This is the main activity for all the apps. All the information is present here for all the apps. If a user runs any app this activity is called and all the information is displayed regarding the current app.

IV. REQUIREMENT SPECIFICATION

Hardware

- Any Android Enabled Handheld
- Android OS Version : Gingerbread & Above
- Google APIs 9

Software

- Server Side : Database Server – MySQL 4.1 or higher
- Server Side : PHP – PHP 4.4.0 or higher (5.2 recommended)
- Server Side: JSON
- Client End : Network Enabled system with Eclipse IDE and ADT Plug-in (for emulator use & debugger)

V. CONCLUSION

Malware can be perceived as the tool or the weapon of an individual or organization intending an unethical or illegal act concerning computers and data. Such applications of malware detection are always required for protection of our device.

REFERENCE

[1] http://www.hongkiat.com/blog/android-app-permissions/
[2] http://www.slideshare.net/rajakhurram/lecture-12-malicious-software
[3] http://www.androidhive.info/2012/05/how-to-connect-android-with-php-mysql/
[4] http://www.welivesecurity.com/2014/10/22/botnet-malware-fight/