Android Security Issues and Solutions

Akshat Sharma[1], Gowthamy. J[2], Suyash Sharma[3], Ajaz Karim[4], Ashish Ranjan Jha[5]

[1]B.Tech (CSE), SRM Institute of Science and Technology, Chennai, India
[2]Assistant Professor, SRM Institute of Science and Technology Chennai, India
[3]B.Tech (CSE), SRM Institute of Science and Technology, Chennai, Indi,
[4]B.Tech (CSE), SRM Institute of Science and Technology, Chennai, India
[5]B.Tech (CSE), SRM Institute of Science and Technology, Chennai, India

---

Abstract: *Android mobile Operating system is one of the top used and user-friendly operating system around the world. It runs on all devices like smartphones, smart TVs&amp; tablets which are the main devices which the user uses in day to day work. Android is an open sourced operating system and with that comes many security issues. Hackers can easily discover and exploit the systems vulnerabilities. In this paper, we concentrate on examining the security of android which is permission based and develop an application that evaluates the overall security level of the system. Also to provide solutions to maximize security and keep the system in good working condition without any security breach.*

Keywords:- Android; Permissions; Security; vulnerabilities; Security breach.

1. INTRODUCTION

Android is a versatile open sourced, based on Linux kernel operating system that allows mobile phones, PCs, smart TVs, tablets and different devices to run applications and projects. As per recent survey Android dominated the smart phone market with share of 84.1%. Being open sourced it provides developers huge opportunity to develop, sell and distribute applications. In Android, other than play store, it is possible to install the applications from unknown sources which needs to ticked in settings. This is one of the major security breaches of Android system. Due to this, hackers find this operating system as an easy target to prey on personal information like saved bank accounts using various malware.

Google Play Store offers various applications that states the security level of an application[2]. Some application analyzes installed applications based on permissions like access to mic, contacts, camera or other privacy breaching features. The first part of the paper discuss about the application itself and the help we can get from the application.

Second portion of the paper covers the possible security attacks in Android. These can be of many types which is totally user based. Applications contains a set of permission which the user has to agree to access the application. Naive users can simply go for normal installation and can let the application access to critical resources like mic, contacts etc. Other option is installation of application without the user's content, in other words a spyware. These malicious applications can get access to all the critical resources unknowingly to the user.

As Android security system is Permission based so permission itself is an important term thus, can be categorized. So, the third portion covers the types of permissions.

Lastly this paper covers the preventive steps to stop our critical resources to be exploited and thus to maximize security.

2. PROPOSED ARCHITECTURE

The main reasons for attack are performed on android devices due to malicious applications , as they are vulnerable because they are mostly downloaded from third party sources .Android shared user ID is one of the major reason for misusing app permissions. The users are not aware of the apps which are misusing the permissions which increase the vulnerability present in previous and latest android versions.

- Application Signature: Any Android application has an extraordinary mark. Mark based arrangements check the substance or examples of an application against a word reference of malware marks. In the event that they locate a coordinating, they can make a move. This strategy is to some degree constrained by the way that it can just recognize a restricted measure of developing dangers, e.g. nonspecific, or to a great degree wide, marks.

We have proposed an android application which shows the permission that are dangerous for the users which increases the vulnerability that causes the risk of draining critical data without asking extra permission from the user. The app displays all the permissions granted to it by the user and all the harmful permission are shown in red thus the user can manually deny the app from accessing permission which are harmful as shown by the app. We have added a screenshot of the app above which shows the dangerous permission granted to the app.

Future developments can be made by reminding the user at every time (can be specified by the user) that this app is having permission to access critical resources keeping the user satisfied and peace of his/her mind that he has control over his/her system.

3. APPLICATION STRUCTURES

Android device application is developed using JAVA Programming Language. The application with the help of already loaded packages in Eclipse was used to create an application with simple user interface. The resource related information is kept in resources.arsc file. The electronic signature are held by META-INF. SHA1 Hash algorithm is used by electronic signature. Developed program can be installed in smart device or the emulator after signing by private key of developer. The most important file named AndroidMenifest.xml which contains the essential information of application such as name of application, permission, activities, Android API version, service and content provider information. Before the execution of app this .xml file should be notified to Android system[1].

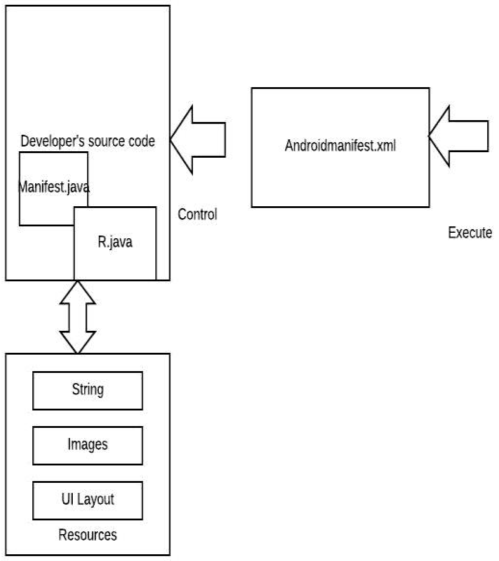


Fig. 1 Relationship between Application and Permissions

When apps requires access to system resources they need to send request for permission of Android system through AndroidManifest.xml. It lets the developer decide their own permissions which are over 200. Permissions are verified for accessing particular databases when client apps have the required permissions and vice-versa[1].

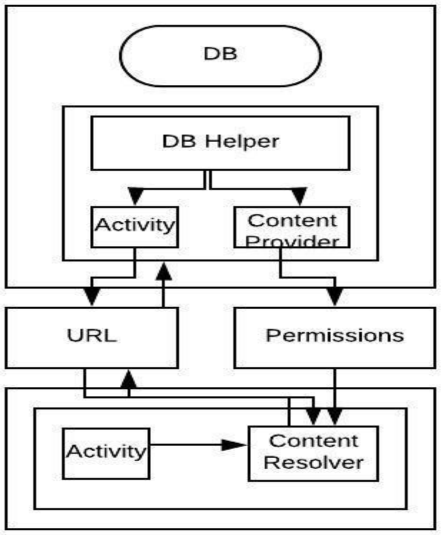
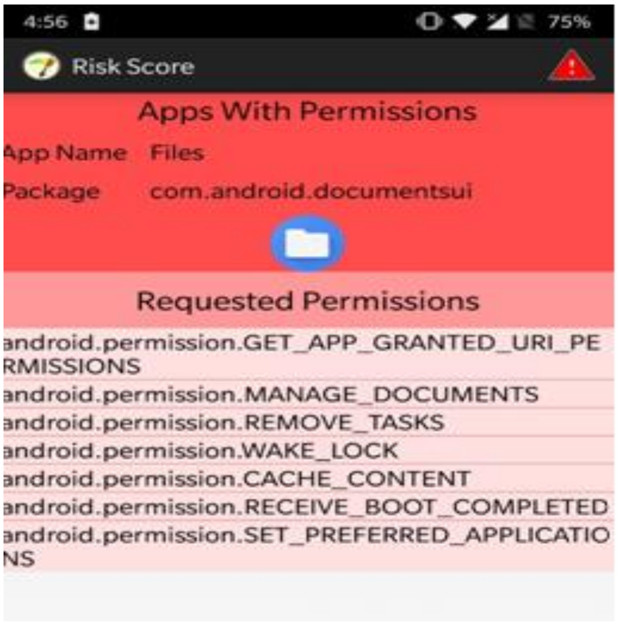


Fig. 2: Database Sharing Between Application



Apps With Permissions

App Name Files

Package com.android.documentsui

Requested Permissions

android.permission.GET_APP_GRANTED_URI_PERMISSIONS
android.permission.MANAGE_DOCUMENTS
android.permission.REMOVE_TASKS
android.permission.WAKE_LOCK
android.permission.CACHE_CONTENT
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.SET_PREFERRED_APPLICATIONS

Fig. 3 Screenshot of the Proposed Application

4. ANDROID SECURITY ATTACKS

Once the permissions are granted, the permissions remain static for Android versions less than 6. But, in Android versions, 7.0 and higher the app permissions are classified into normal permissions and dangerous permissions.

4.1 A FAKE ID

All android application consists of their own unique identity, the feature of impersonating one application by allowing identities to be copied increases the vulnerability. The Fake ID that gets impersonated but is recognized as trusted one by user breaches allows malicious applications to be recognized as trusted source. This could potentially allow malicious software to steal user information from a trusted application and even take control of the security mechanisms on a device as the android package installer doesn't verify the chain of certificates.

4.2 PERMISSION ESCALATION ATTACK

The Android's permission mechanism asks for the permission only at the time of installation of android applications[3]. This conceptual weakness leads to privilege escalation attacks which allows android applications to circumvent restrictions. It allows a malicious application to collaborate with other applications so as to access critical resources without requesting for corresponding permissions explicitly.

4.3 TIME OF CHECK AND TIME OF USE ATTACK (TOCTOU)

Android permission are represented as strings and also equivalent, they can belong to different applications but have similar names [3] [4]. No naming rule or constraint is applied to a new permission declaration.

4.4 SPYWARE

Spyware is an type of malware apk file, which generally automatically gets downloaded when the user visits to malicious website and app gets automatically installed [3]. In android devices the app can be downloaded and installed other than Google play store which becomes one of the major reasons for security threats in Android operating system.

4.5 NFC Exploitation

NFC is the primary technology that allows for features like Android Beam [5]. This technology has been increasingly used in cashless payment systems such as Google Wallet and now Android Pay. The hacker installs Trojan relay software in victim's phone which increases the physical distance between the victims and hackers phone. The hackers could utilize the NFC property in the victim's phone to steal money from the physical credit cards in his or her pocket, rather than through Google Pay, when the cards come in contact with the victim's phone. The often the wallet is near phone the instance for attack becomes much more probable.

5. UNDERSTANDING PERMISSIONS

The Android operating system uses the security tool as Permission based. These Permissions as discussed are declared in AndroidManifest.xml file. Once the permissions are granted, the permissions remain static for Android versions less than 6. But, in Android versions, 7.0 and higher the app permissions are classified into normal permissions and dangerous permissions.

5.1 Normal Permissions

Normal Permissions are the permissions which are not declared in AndroidManifest.xml file and are granted automatically.
Eg: SET_WALLPAPER, UNINSTALL_SHORTCUT.

5.2 Dangerous Permissions

Dangerous Permissions are the permissions that can access critical resources of the mobile. If app lists a dangerous permission the user has to forcefully give access the permissions the app requires for successful installation.
Eg: READ_ACCOUNTS, WRITE_EXTERNAL_STORAGE.

6. CONCLUSION

Android's problem of keeping their operating system secure has increased over the years mainly because of system's limitations, design vulnerabilities and also being the most popular operating system in the industry. This paper shows how to avoid the misuse of permission of an application through a proposed tool. This will increase the security of the users by avoiding information breach. The proposed app will tell the danger level of an selected app so that we can accordingly deny that application access to sensitive resources.

7. REFERENCES

[1]. J. Joshi and C. Parekh on Android Smartphone Vulnerabilities: A Survey.

[2]. I. Khokhlov and L. Reznik on Android System Security Evaluation.

[3]. Karthik S and Dr. S. Bini on Android Security Issues and Solutions.

[4]. S. I. A. Yasin and T. Naqash on Android (Nougats) Security Issues and Solutions.

[5]. [The NFC] - https://www.player.one/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497.

[6]. "Permission Removal to enhance security for Android based mobile devices" – BenMArtini.