Understanding Application Security in Android

BharatiBorde, Steffi Nigrel
Master of Computer Application, Mumbai University

Abstract— Security is the main concerns for every mobile users as it can consists of important data. Android is mobile platform which is an open source. Being an open source the vulnerabilities for all Android device increases extremely. Android developers have very few restrictions, this leads to increase in security risks for Android device users. In this paper we seek to understand the security model, application level security issues in Android.

Keywords— Android security model, security issues.

I. INTRODUCTION

Smartphones industry is rapidly growing which has led to an increase for mobile services. All smartphones applications support social, financial, and enterprise services for any users with an internet data plan. Smartphones users can download thousands of paid as well as free applications with one click from the application markets, for example, Google's Android Market Play store and Apple's App Store.

The markets that are flexible tend to have a lot of security challenges. Applications that are developed and integrated in smartphones are rough build permission systems, can invade privacy, can consist of malwares and have low security models which could led to misuse of the data on the phones as well as other applications that might contain extremely important data which could be misused. For example, an application could access the crucial information like passwords stored in the phone or access all the contacts on the phone. Markets are not in a state to provide high level security in more than a perfunctory way. Due to this, malicious applications can easily get into the application market.

This paper is an initiative to understand the application security on Android. Thus, one can deliberate about how secure applications are today.

II. BACKGROUND

Android is a Linux-based Operating System for mobile devices like smartphones and tablets, and it is an open source. Android is currently being developed by Open Handset Alliance that is led by Google and other companies.

Android offers a unified approach for developing application for mobile devices that is developers only need to develop for android operating systems and their applications can run on any smartphone that has android operating system.

Google released the first beta version of Android Software Development Kit in 2007 and the commercial version in September 2008. Google announced the next version, 4.1 Jelly Bean on June 27 2012. The current latest version available is Marshmallow which was released on October 15, 2015. The upcoming version of android operating system is android N. It is expected to release in mid-2016.

Android being an open source, the source code is available for free under software licenses.

III. ANDROID APPLICATIONS

Android applications are developed in Java language using the Android SDK, that is, Software Development Kit that can be used in several IDE's like Eclipse, and Google's Android Studio which is the official IDE for Android application development introduced on May 13 2016.

After the application is developed, it can be easily packaged and sold in stores like Google's Play Store or the Amazon App Store.

Many mobile devices are powered by Android in more than 190 countries around the world. Few brands that use android operating system in their mobile devices are Samsung, Motorola, Intex, Micromax, etc. It has the largest installed base of any mobile platform and is rapidly growing. More than 1 million Android devices are activated worldwideevery day.

IV. ANDROID PLATFORM SECURITY ARCHITECTURE

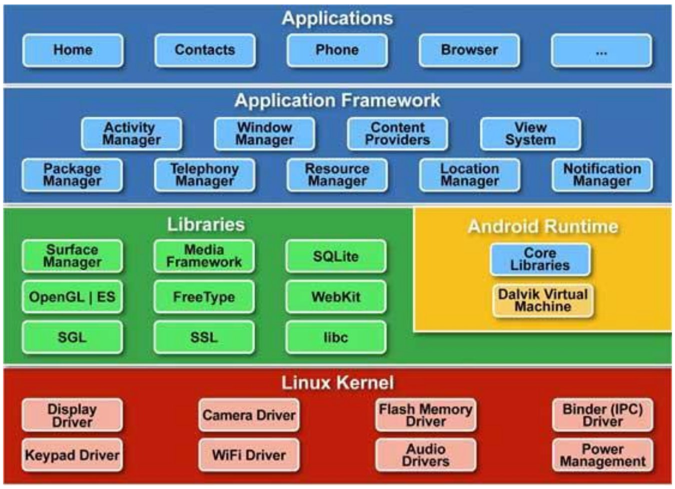

Fig 1. Android Architecture[1]

Android operating system is a stack of software components which is roughly divided into five sections and four main layers as shown in fig 1 [1]. Android is a secured operating system for mobiles by classical operating system security controls for protecting user data, system resources and provide application isolation.

Android provides following security features to achieve these objectives are first strong security at the operating system level through the Linux kernel, second compulsory application sandbox for all applications, third secure interposes communication, fourth application signing, and fifth application defined permission and user have to grant permissions.

Figure 1shows components and considerations at the various levels of the Android. Every component in android architecture assumes thatcomponent below them is more secure.

V. SECURITY ISSUES FACED BY ANDROID

Android is very secure as it appears, even with such robust security measures. There are many security problems faced in android, some of them are listed below.

A. It is easy to upload apps on Google's app market as it does not provide any security checks while uploading apps.

B. Many apps in android market can access as well as use services and data from another android app without asking for permissions of any kind.

C. Android's permission security model allow user to decide whether the app can be trusted or not, due to kind of permission security model more power is given to humans, which involves high amount of risks in Android systems.

D. The framework for android application cannot be trusted while developing critical systems, as the Open Source is available to all kind of developers as well as hackers too. For example, if the Android device consist of a banking app which has all the bank related information it could be easily hacked as android being an open source.

E. The developers of android operating system have stated that it is not their responsibility for any kind of security for any external storage.

F. All android apps on the android devices can easily access data in the device like GSM and SIM markets Ids without any permission from users.

Android platform provides many security features, but there is always high risk if user installs applications that are suspicious or allows permission to any application without looking into it.

VI. VULNERABILITY

Following are the list of reason why android application security is vulnerable

A. User as Admin :
As user is the admin, they can install any app that is available in the market as well as from outside. The user can download data and access unprotected data.

B. The Android Market :
The verification and security process for applications entering Google's app market is very low. New apps can enter easily within few hours. This leads to number of malicious app made available to users in the market.

C. Application Permissions :
Android apps ask for permission in the form of pop ups, the users don't understand the nature of the request. Many app is the market usually ask for accessing the user current location or read/send SMS, access IMEI, camera, get device details and so on. These request are integral for the functionality of the app but can equally be a risk factor for the users as they can record calls and transmit sign-in credentials to hackers.

D. Malicious Applications :
Many apps in market are made so that important data from user can be transferred and used for wrong reasons. This comprises the security of data which can be crucial.

E. Third Party Applications :
The great thing about android is the choices available for standard functionalities. User can install third party apps for standard functionalities in android devices like address books, keyboards, etc. from third parties. But this involves the risk as third party apps cannot be trusted easily and all the third parties are genuine.

F. Rooting:
Rooting in an android is similar to jail breaking in iPhones, this opens several functionalities and services to the users. For rooting android devices, it requires the device to be switched from S-On to S-Off where S stands for Security. Rooting a device allows the device to gain system- level access to android Operating System.

G. Remote Installation :

There are many apps available in the web market for the users to download and install on their android devices. This introduced much more accessible platform for discovering latest applications. One of the most famous third party app market is AppBrain, which provide similar services like Google's Play Store which actually beat Google to its first place.

H. Manufactures trust :
Manufacturers play an important role in privacy of the users. For example, recently it was uncovered that on HTC devices sits at root level and collects all information on users including their data related to their accounts, phone number, SMS, etc. Moreover, any app with internet access could gain this information.

VII. RESEARCH FINDING

Android uses two basic methods of security enforcement. First, all application run on their own with their individual IDs as Linux processes separately from each other. Due to this, vulnerabilities from one application will not affect other any applications in the android devices. As IPC mechanisms is provided by Android, which needs to be secured, second enforcement mechanism is used. Android implements reference monitor based on permissions to mediate access to application components so end user has the power to give the applications permissions only if required during installation time.

Phone Identifiers can be leaked easily through plain text request in android operating systems. IMEI a phone identifier can be used for tracking individual users. Phone identifiers are unique for every individual phone. Phone identifiers are used for analytics servers and for advertisements.

There are many tools available in the market for finding security bugs. But they are not able to find any logical security problems like interactions between components that are mostly unnecessary. As the complexity of software increases, most of the software companies have to understand the security risks of their applications code.

As android has created a mapping between API calls and permissions that require to execute the application. Therefore, android end users always need to check if their applications are leaking any of their personal information. Android Leaks help in minimizing the number of applications and the number of traces that a security auditor needs to verify manually.

As android is an open source software and the programmable framework, which makes it vulnerable to virus attacks. The title takes into consideration the fact that Smart phones are memory, battery and speed constrained and hence exploiting the cloud to do the reputation index computation of a given application. By referring to the calculated matrix of reputation built by a given application, the model will help users by notifying them about the risk of the application before installation. Applications are mainly classified as highly risky, medium risk, less risk and genuine all based on reputation they have built. The experimental results show that the applications that are highly risky should not be installed by the end users until they prove their quality by passing the thresholds set based on security model.

VIII. ANDROID SECURITY ISSUES AND PREVENTION

A. APPs:

Since android is an open platform and anyone can create apps and publish it in Google apps, these apps itself contains malicious which may steal or destroy data and sensitive tips from your phone. So, while installing any app, always try to check if the app has any of the security issues. A simple Google search provides you all the useful information about a particular app, therefore always search about apps before installing them. Always to keep your android phone secure, make sure that applications which you are already using has no major security concern and to keep your phone secure update your apps or apply the security patches to keep phone secure.

B. MOBILE Ads:

While using an application, your app youmay see various ads. Android always allows developer to show ads from their ad inventory in order to cast the apps. When user clicks on ads in the app, the user visit advertiser's site, which can secretly install a Trojan or introduce viruses or any backdoors to your phone.To keep your android phones always avoid clicking ads unnecessarily.

C. ANDROID OS:

Android phone used Linux kernel and android library, which may have vulnerability. Since it is almost impossible to find all the major security flaws before the release of the new version. Always make sure that your android application is updated to its latest release. You will find an automatic update option in "about the phone" under your phone setting option.

D. APP IMPERSONATION:

Each android application has its own digital signature that identifies that app with the vendor. If a hacker make an application with a fake ID and find a way to bypass the process of Android checking the ID with the actual vendor, hacker can have access to your sensitive data. Always while downloading any financial app, verify the identity of the vendor.

For example if any of the bank website has a link to Google play store for download their apps in your mobile use it. Most of the times avoid searching your bank's app in Google Play because you may mistakenly get aduplicate app with fake ID of your bank.

E. PERMISSION:

Many android end users do not pay more attention to the permission that are asked by the apps. Many apps ask for permissions more than they require to perform the tasks. For example, many gamingapps ask for user's phone number which is not needed. Therefore it is user's responsibility to check if an app is asking for sensitive data. Android being an open source, it is possible for checking the permission that are required by the app for execution. Therefore, users must always read the statement for permission carefully during installation.

IX. TOP TEN ANDROID SECURITY TIPS

There is no doubt that the Android mobile operating system (OS) is a commanding force in the world of smart phones. But it is also the most acquiescent to malware, the least secure fresh out of the box and the most fragmented. Security will be your biggest priority, if you will be using Android devices whether a tablet or phone for business purpose.

Following are few security tips that could be followed so that Android becomes a much more secure and reliable mobile operating system.

1) Users must always remember to disable app from getting downloaded from unknown sources. If app are installed from non-official sites rather than Google's Play app store one's android device can easily get infected with malware. In the Settings menu of any Android device is a check box that is used to enable and disable installing 'unofficial' apps. An Android that keeps itself legit is far safer.

2) Upgrade to Android 3.0 or above.Android 3.0 was the first version in Android to incorporate file system encryption, after almost three years into system's life in market. Devices that do not support any kind of encryption are more acquiescent to damaging data loss. Therefore, encryption is important to avoid data loss.

3) Download an anti-virus app for your device. Now a days Android malwares and viruses are a widely -identified part of the smartphone world, there are many solutions available toreduce or remove them. Most of the big antivirus (AV) companies have their own Android anti-malware apps, including Kaspersky, AVG, Avast and Norton. Recommended free Android AV apps include Lookout (where there is also a premium version available) and Trust Go. Read more about mobile security*.IBM extends cloud business with Trustier mobile security*.Mobile security model flawed, says Mobile Helix*.Mobile security watershed - from SOAP to SUDS*.BAE Systems and Vodafone join forces for mobile security.

4) Never get connected to any unsecured or unknown Wi-Fi networks. An unknown or unsecured Wi-Fi network might seem to be a great gift for free internet, but an older version or outdated version of Android operating system in particular device could prove risky. Public Wi-Fi network might have 'middleman' attack, in which any data that is inputted in the device can be intercepted or changed by a third person or hacker or third party and can be used against the user itself. The data that can be intercepted or changed by be password or personal details, like credit card details or email credentials.

5) Install a remote lock app.Supposing, if your android device is stolen or lost, if you have an lock app the data can yet be secure not used against you. There are apps available in Google's play store that will do this, reacting to either a command from a web interface or via text. Popular remote wipe and lock apps include Cerberus and Avast Mobile Security.

6) Important and sensitive data should always be kept under an extra encryption layer for protection. Keeping important data in a generic note on a phone or tablet could be the worst idea as it can be easily hacked. There are many apps available that store your data in multiple layer of protection and encryption.

7) Be aware of SMS threats Premium. SMS threats are equally responsible for the surge in Android malware. The O bad threat, can send premium rate SMS texts, install other malicious apps and execute other malicious code. If there is mysterious activity on a phone bill, then check that if these kinds of apps are present in your device or not.

8) Use the Chrome browser. Since Android 4.1 was introduced, phones and tablets have come with the stock of Android browser as well as Chrome installed as standard for browsers. Chrome is comparatively more secure than the any other version. Chrome has been subject to less insecurity in earlier days. It is also found that Chrome is most likely used by most of the Android devices, and in almost all the mobile devices Chrome is pre-installed. It will out as the future default browser for Android.

9) Put a lock on your lock screen. Simple but most necessary, anyone who concern about Android security should put some lock screen protection on their phone. Normally all Androids devices comes with optional security measures pre-installed, accessed in the security submenu of settings.

10) Stolen phone? Check out Plan B many of the users have done it – if you lost your phone or it gets stolen, at this point of time just before planning to buy phone insurance or install a phone tracker. There is one last point of call.

X. SECURITY TIPS

Android has security features built into the operating system that significantly reduce the frequency and impact of application security issues.

The system is designed so you can typically build your apps with default system and file permissions and avoid difficult decisions about security.

Some of the core security features that help you build secure apps include:

1. The Android Application Sandbox, itdifferentiate your android app data and code execution from other apps.*.An application framework with strong implementations of common security functionality such as cryptography, permissions, and secure IPC.

2. Technologies like ASLR, NX, Pro Police, safe_iop, Open BSD dlmalloc, Open BSD calloc, and Linux mmap_min_addr to reduce risks associated with common memory management errors.

3.An encrypted file system that can be enabled to protect data on lost or stolen devices.

4.User-granted permissions to restrict access to system features and user data.

5.Application-defined permissions to control application data on a per-app basis.

Storing Data is one of the most common security concerns for an application on Android is whether the data that you save on the device is accessible to other apps.

There are three fundamental ways to save data on the device:

1) Using internal storage by default, is one of the most simple and effective technique. Because files that you create on internal storage are accessible only to your app. This protection is implemented by Android and is sufficient for most applications.

2) You should generally avoid using the MODE_WORLD_WRITEABLE or MODE_WORLD_READABLE modes for IPC files because they do not provide the ability to limit data access to particular applications, nor do they provide any control on data format. If you want to share your data with other app processes, you might instead consider using a content provider, which offers read and write permissions to other apps and can make dynamic permission grants on a case-by-case basis.

3) To provide more protection for your personal and sensitive data, you might choose to encrypt local files using a key that is not directly accessible to the application. For example, a key can be placed in a Key Store and protected with a user password that is not stored on the device. While this does not protect data from a root compromise that can monitor the user inputting the password, it can provide protection for a lost device without file system encryption. As we know that internal storage does not allow reading or writing data to other application. Using external storage Files created on external storage, such as SD Cards, are globally readable and writable. Because external storage can be removed by the user and also modified by any application, you should not store sensitive information using external storage, you should perform input validation when handling data from external storage. We strongly recommend that you not store executable or class files on external storage prior to dynamic loading. If your app does retrieve executable files from external storage, the files should be signed and cryptographically verified prior to dynamic loading. Using content providers Content providers offer a structured storage mechanism that can be limited to your own application or exported to allow access by other applications. If you do not intend to provide other applications with access to your Content Provider, mark them as android: exported=false in the application manifest. Otherwise, set the android: exported attribute "true" to allow other apps to access the stored data. When creating a Content Provider that will be exported for use by other applications, you can specify a single permission for reading and writing, or distinct permissions for reading and writing within the manifest. We recommend that you limit your permissions to those required to accomplish the task at hand. Keep in mind that it's usually easier to add permissions later to expose new functionality than it is to take them away and break existing users. If you are using a content provider for sharing data between only your own apps, it is preferable to use the android: protection Level attribute set to "signature" protection.

XI. CONCLUSION

Now a days more than 1 million Android device activated. Android has very few restrictions for developer, increases the security risk for end users. In this paper we have reviewed security issues in the Android based Smartphone. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. Android provides more security than other mobile phone platforms. Kirin will help mold Android into the secure operating system needed for next-generation computing platforms.

XII. ACKNOWELEDGMENT

This paper is a part of academic research on Understanding Application security in android made in partial fulfilment of the course of Masters in Computer Application

XIII. REFERENCE

1. http://www.tutorialspoint.com/android/android_tutorial.pdf
2. Kaur S. and Kaur M., Review Paper on Implementing Security on Android Application, Journal of Environmental sciences, Computer Science and Engineering and Technology.
3. Android Open Source Project. Security and Permission. http://developer.android.com/guide/topics,security/permissions.html.
4. Android Open Source Project. Publishing on GooglePlay. http://developer.android.com/distribute/googleplay/publish/preparing.html.
5. WWW.google.com
6. http://www.isca.in/COM_IT_SCI/Archive/v1/i6/3.ISCA-RJCITS-2013-030.pdf.
7. Android Programming Book Http://www.coreservlets.com/android-tutorial/.
8. Fernflower-java decompiler. http://www.reversed-java.com/fernflower/.
9. AdMOB. AdMob Android SDK: Installation Instructions. http://www.admob.com/docs/AdMob_Android_SDK_Instructions.pdf. Accessed November 2010.