RESEARCH ARTICLE OPEN ACCESS

An Overview of Android Operating System and Its Security Features

Rajinder Singh
Department of Computer Science and Applications DCSA Panjab University SSGRC Hoshiarpur

ABSTRACT
Android operating system is one of the most widely used operating system these days. Android Operating System is mainly divided into four main layers: the kernel, libraries, application framework and applications. Its kernel is based on Linux. Linux kernel is used to manage core system services such as virtual memory, networking, drivers, and power management. In these paper different features of architecture of Android OS as well security features of Android OS are discussed.
Keywords **–** Dalvik VM, Linux, Sandbox

I. INTRODUCTION

Android operating system is one of the most widely used mobile Operating System these days [1]. Android mobile operating system is based on the Linux kernel and is developed by Google. Android operating system is primarily designed for smartphones and tablets. Since Android is an open source it has become the fastest growing mobile operating system. Due to its open nature it has become favorite for many consumers and developers. Moreover software developers can easily modify and add enhanced feature in it to meet the latest requirements of the mobile technology [2]. Android users download more than 1.5 billion applications and games from Google Play each month. Due to Its Powerful development framework users as well software developers are able to create their own applications for wide range of devices [3]. Some of the key features of Android operating system are: Application Frame work, Dalvik virtual machine, Integrated browser, Optimized Graphics, SQLite, Media Support, GSM Technology, Bluetooth, Edge, 3G, Wi-Fi, Camera and GPS etc [1]. To help the developers for better software development Android provides Android Software development kit (SDK). It provides Java programming Language for application development [1]. The Android software development kit includes a debugger, libraries, a handset emulator based on QEMU (Quick Emulator), documentation, sample code, and tutorials [4].

II. ARCHITECTURE OF ANDROID OPERATING SYSTEM

Android operating system is a stack of software components. Main components of Android Operating system Architecture or Software Stack are Linux kernel, native libraries, Android Runtime, Application Framework and Applications.

2.1 Linux Kernel

Linux Kernel (Linux 2.6) is at the bottom layer of the software stack. Whole Android Operating System is built on this layer with some changes made by the Google [5]. Like main Operating System it provides the following functionalities: Process management, Memory Management, device management (ex. camera, keypad, display etc). Android operating system interacts with the hardware of the device with this layer [6]. This layer also contains many important hardware device drivers. Linux kernel is also responsible for managing virtual memory, networking, drivers, and power management [7].

2.2 Native Libraries Layer

On the top of the Linux Kernel layer is Android's native libraries. This layer enables the device to handle different types of data. Data is specific to hardware. All these libraries are written in c or c++ language. These libraries are called through java interface. Some important native libraries are:
Surface Manager: it is used to manage display of device. Surface Manager used for composing windows on the screen.
SQLite: SQLite is the database used in android for data storage. It is relational database and available to all applications.
WebKit: It is the browser engine used to display HTML content.
Media framework: Media framework provides playbacks and recording of various audio, video and picture formats.(for example MP3, AAC, AMR, JPG, MPEG4, H.264, and PNG).

Free Type: Bitmap and Font Rendering
OpenGL | ES: Used to render 2D or 3D graphics content to the screen
libc: It contains System related C libraries [5].

2.3 Android Runtime

Android Runtime consists of Dalvik Virtual machine and Core Java libraries. It is located on the same level as the library layer [5]. Dalvik Virtual Machine is a type of Java Virtual Machine used for running applications on Android device. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine. The Dalvik VM allows multiple instance of Virtual machine to be created simultaneously providing security, isolation, memory management and threading support [8]. Unlike Java VM which is process-based, Dalvik Virtual Machine is register-base. Dalvik Virtual Machine run .dex files which are created from .class file by dx tool. dx tool is included in Android SDK. DVM is optimized for low processing power and low memory environments. DVM is developed by Dan Bornstein from Google [9].

2.4 Application Framework

The Application Framework layer provides many higher-level services or major APIs to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications [6]. These are the blocks with which developer's applications directly interact. Important blocks of Application framework are:
Activity Manager: It manages the life cycle of applications.
Content Providers: It is used to manage the data sharing between applications, manages how to access data from other applications.
Telephony Manager: it manages all voice call related functionalities.
Location Manager: It is used for Location management, using GPS or cell tower.
Resource Manager: Manage the various types of resources used in Application [8].

2.5 Application Layer

The Applications Layer is the top layer in the Android architecture. Some applications come pre-installed with every device, such as: SMS client app, Dialer, Web browser and Contact manager. A developer can write his own application and can replace it with the existing application [8].

III. DIFFERENT SECURITY FEATURES OF ANDROID OS

Android Operating system should ensure the security of users, user's data, applications, the device, and the network. To achieve the security of these components Android provides these key security features [10]:1) Security at the Operating System level through the Linux kernel. 2) Application sandbox for all applications 3) Secure interprocess communication. 4) Application signing. 5) Application-defined and user-granted permissions.

3.1 Linux Kernel

Android operating system is based on Linux kernel. Due to its open source nature it is researched, attacked and fixed by many research developers. So Linux has become stable and secure kernel.
Linux kernel provides Android with several key security features including:
a) A user-based permissions model
In the Linux file system each file and directories has three user based permissions. owner, group, other users. owner - The Owner permissions apply only the owner of the file or directory. group - The group permissions apply only to the group that has been assigned to the file or directory. other users - The other Users permissions apply to all other users on the system. Each file or directory has three basic permission types: read - The read permission means user's ability to read the contents of the file. write - write permissions mean's user's ability to write or edit a file or directory. execute - The execute permission means user's ability to execute a file or view the contents of a directory [11]. This permission model ensures that proper security is maintained while accessing android files.
b) Process isolation:
The Android operating system assigns a unique user ID (UID) to each Android application and runs it as a separate process.
c) Extensible mechanism for secure IPC.
d) The ability to remove unnecessary and insecure parts of the kernel [10].

3.2 The Application Sandbox

A sandbox is a security mechanism for separating running programs and limiting the resources of the device to application. It is often used to execute untested code or programs from untrusted users and untrusted websites. By using sandboxing technique limited access to device's resources is given. Therefore security of the system is increased. Sandboxing technology is frequently used to test unverified programs which may contain a virus or other malware code, without allowing the software or

code to harm the host device. With the help of sandbox untrusted program access only those resources of the device for which permission is granted. Permission is denied if it tries to access other resources of the device [12].

3.3 Secure inter-process communication

Some of the applications still use traditional Linux techniques such as network sockets, file system and shared files for inter-process communication. But android operating system also provides new mechanism for IPC such as Binder, Services, Intents and ContentProviders. All these mechanism allows developers to verify the identity of application and also used to set the security policies [13].

3.4 Application signing

In order to install and run applications on Android OS they must be digitally signed. With this mechanism Android OS identifying the author of an application. This feature also used to establishing trust relationship between applications.
If an application is no signed properly then it cannot be installed on the emulator also. Some standard tools such as Keytool and Jarsigner are used to generate keys and sign application .apk files [15].

3.5 Application-defined and user-granted permissions

Permissions are an Android security mechanism to allow or restrict application access. By default, Android applications have no permissions granted, making them safe by not allowing them to gain access to protected APIs [14]. Some of the protected APIs include: Camera functions, Location data (GPS) ,Bluetooth functions, Telephony functions, SMS/MMS functions and Network or data connections. These resources are accessed only through the operating system [10].

IV. CONCLUSION

From above discussion it is clear that Android Operating System follows a variety of security mechanism. When a developer install an application a new user profile with that application is created. Each application run with its own instance of Dalvik VM. So applications cannot access each other's data. If applications want to access shared data or resources then they require permissions. All Android applications are signed so users know that the application is authentic. The signing mechanism allows developer to control which applications can grant access to other application on the system.

REFERENCES

[1] http://www.engineersgarage.com/articles/what-is-android-introduction.
[2] http://en.wikipedia.org/wiki/Android_(operating_system)
[3] http://developer.android.com/about/index.html
[4] http://en.wikipedia.org/wiki/Android_software_development
[5] http://www.tkhts.com/android/android-architecture.jsp
[6] http://www.tutorialspoint.com/android/android_architecture.htm
[7] http://www.compiletimeerror.com/2012/12/blog-post.html#.UuYiIGC6bIU
[8] http://www.android-appmarket.com/ android-architecture.html
[9] http://ptcoresec.eu/2013/05/02/part-1-getting-to-know-android/
[10] http://source.android.com/devices/tech/security/
[11] http://www.linux.com/learn/tutorials/309527-understanding-linux-file-permissions
[12] http://en.wikipedia.org/wiki/Sandbox_(computer_security)
[13] http://developer.android.com/training/articles/security-tips.html
[14] http://www.ibm.com/developerworks/library/x-androidsecurity/
[15] http://developer.android.com/tools/publishing/app-signing.html