AN OVERVIEW OF ANDROID OPERATING SYSTEM AND ITS SECURITY FEATURES

ANUJ KUMAR[1], NITIN KUMAR VERMA[2]

MCA 4TH SEM ASSISTANT PROFESSOR

[1]*DEPARTMENT OF CCSIT,TEERTHANKER MAHAVEER UNIVERSITY , MORADABAD UP INDIA*

anujraghav628@gmail.com

kvnitin7882@gmail.com

Abstract— **An android operating system is a generally used operating system .this operating system is mainly divided into four layers-**
(a) Kernel (b) libraries (c) application framework (d) applications
Kernel is based on Linux. This Linux kernel is used to manage core system service's like virtual memory ,networking ,drivers, and power management. In this paper different features of architecture of android operating system of android operating system and security feature of android operating system are discussed tablets. Android has become fastest growing mobile operating system because android has open source nature.

Keywords:- **Dalvik VM, Linux, Sandbox**

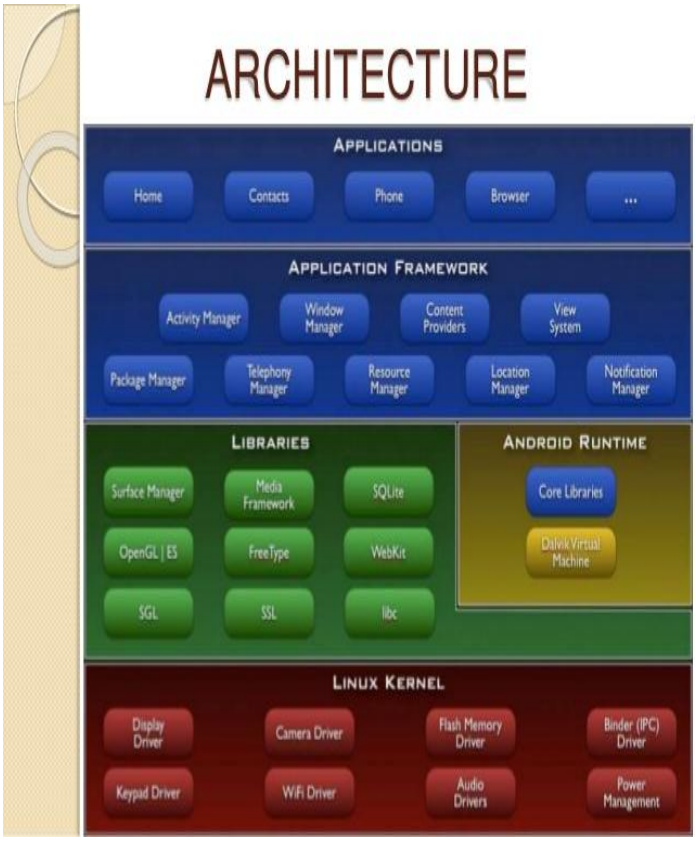
I. INTRODUCTION

Android operating system is the generally used mobile Operating System .the Android mobile operating system is based on the Linux kernel and developed by Google. The Operating system is basically aimed for smartphones and tablets. Android is an open source it has become the fastest developing mobile operating system. It has open nature so it has become favourite for many clients and developers. Likewise software designers can easily modify and add better feature in it to meet the modern necessities of the mobile technology. Android users can download more than 1.5 billion applications and games from Google Play each month. Due to Its Influential development framework clients as well software designers are able to create their own applications for wide range of devices . Some features of Android operating system are- Application Frame work , Dalvik virtual machine, Integrated browser, Optimized Graphics, Media Support, GSM Technology, SQLite, Bluetooth, Edge, 3G, Wi-Fi, Camera and GPS etc. for helping the developers for well software development Android provides Android Software development kit (SDK). It offers Java programming Language for application development . The Android software development kit holds a debugger, libraries, a handset emulator based on QEMU (Quick Emulator), papers, sample code, and tutorials

II. VERSIONS OF ANDROID

And now google is working on its latest update of android "O" that will be launched in different devices very soon

III. ARCHITECTURE OF ANDROID OPERATING SYSTEM:



Android operating system is a stack (LIFO) of software components. Main components of Android Operating system Software Stack are Linux Kernel , Android Runtime, Application Framework and Applications, native libraries.

A. Linux Kernel:

Linux Kernel is at the lowest layer of the software stack. Entire Android Operating System is built on this layer with some changes made by the Google . Like main Operating System it provides the following functionalities: Process management, Memory Management, device management (ex. camera, keypad, display etc). Android operating system relates with the hardware of the device with this layer . This layer also manages many important hardware device drivers. it is also responsible for managing virtual memory, power management and networking, drivers.

2.2 Native Libraries Layer

The Linux Kernel layer has highest Android's native libraries. This layer allows the device to handle different types of data. Data is specific to hardware. these libraries are written in c or c++ language. These libraries are called through java interface. Some significant native libraries are: Surface Manager: it is used to manage display of device and used for creating windows on the screen. SQLite: SQLite is the database used in android for data storage. It is relational database and available to all applications. Web Kit: 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.

B. Android Runtime

Android Runtime holds of Dalvik Virtual machine and Core Java libraries. It is placed on the same level as the library layer. Dalvik Virtual Machine is a form 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 permits multiple instance of Virtual machine to be created simultaneously providing security, isolation, memory management and threading support . Dissimilar Java VM which is process-based, Dalvik Virtual Machine is registerbase. Dalvik Virtual Machine run .dex files which are created from .class file by dx tool. dx tool is included in Android SDK. DVM is improved for low processing power and low memory environments.

Dan Bornstein is developed the DVM in google.

IV. APPLICATION FRAMEWORK :-

The Application Framework layer offers many higher-level services or major APIs to applications in the form of Java classes. Application developers are permitted to make use of these services in their applications. These are the blocks with which

developer's applications directly interact. Important blocks of Application framework are: Activity Manager: It achieves the life cycle of applications. Content Providers: It is used to achieve 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 several types of resources used in Application .

A. Application Layer

The Applications Layer is the highest layer in the Android architecture. Some applications come preinstalled with all device, such as: Web browser SMS client app, Dialer, and Contact manager. A developer can write his own application and can replace it with the existing application

V. DIFFERENT SECURITY FEATURES OF ANDROID OS:-

The Android Operating system must ensure the security of users, user's data, applications, the device, and the network. To accomplish the security of these components Android offers these key security features (A) Security at the Operating System level through the Linux kernel. (B) Application sandbox for all applications (C) Secure interprocess communication. (D) Application signing. 5) Application-defined and user-granted permissions

A. Linux Kernel :-

Android operating system is made 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 offers 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. 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 takes 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 . 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 .

B. 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.

C. 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 Content Providers. All these mechanism allows developers to verify the identity of application and also used to set the security policies .

D. Application signing

In command 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 founding trust relationship between applications. If an application is no signed accurately then it cannot be installed on the emulator also. Some standard tools such as Keytool and Jarsigner are used to create keys and sign application .apk files .

E. Application-defined and user-granted permissions

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

VI. CONCLUSION

From above conversation it is clear that Android Operating System follows a variation 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. Hence applications cannot access each other's data. If applications want to access shared data or else resources then they require permissions. All Android applications are signed so users know that the application is authentic. The signing mechanism allows designer 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_(opera ting_system)
[3] http://developer.android.com/about/index.html
[4] http://en.wikipedia.org/wiki/Android_softwa re_development
[5] http://www.tkhts.com/android/android-archit ecture.jsp
[6] http://www.tutorialspoint.com/android/andro id_architecture.html
[7] http://www.compiletimeerror.com/2012/12/blogpost.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_(comp uter_security)
[13] http://developer.android.com/training/article s/security-tips.html
[14] http://www.ibm.com/developerworks/library /x-androidsecurity/
[15] http://developer.android.com/tools/publishin g/app-signing.html