**Chapter 1 Android Operating System**

**1.1 About Android**

Android is a [mobile open source operating system](https://en.wikipedia.org/wiki/Mobile_operating_system) initially developed by Android Inc., which [Google](https://en.wikipedia.org/wiki/Google) bought in 2005, it is based on the [Linux kernel](https://en.wikipedia.org/wiki/Linux_kernel) and designed primarily for [touchscreen](https://en.wikipedia.org/wiki/Touchscreen) mobile devices such as [smartphones](https://en.wikipedia.org/wiki/Smartphone) and [tablets](https://en.wikipedia.org/wiki/Tablet_computer).

**1.2 Android Architecture**

**1.2.1 The Kernel**

Android runs on top of a Linux 2.6 kernel. The kernel is the first software layer, which interacts directly with the hardware. It take care of power and memory management, device drivers, process management, networking and security.

**1.2.2 The Libraries**The libraries component acts as a translation between the kernel and the application framework. The libraries are written in C/C++ but are exposed to developers through a Java API. One of the core libraries is:

* Media libraries: it allows access to audio and video recording and playback functions.

**1.2.3 The Dalvik Virtual Machine**

**What is a virtual machine?**

A virtual machine is a guest operating system running within another host operating system; it executes the applications as if they were running on a physical machine.

The Dalvik VM was written to allow application execution on devices with limited resources. Specially, mobile phones which are limited by the amount of memory available, and the processing power. The Dalvik VM executes a .dex (Dalvik Executable) file. A .dex file is a compiled Android program which is zipped with the application layouts into an APK file.

**1.2.4 The Application Framework**

The application framework is one of the building blocks of the final end-user application. It provides a bunch of services that a developer will find useful when writing applications, commonly referred to as the APIs (application programming interfaces).

**1.2.5 The Applications**

The Application component is the finished product that will be executed on the touchscreen devices.

**1.3 Android Permissions**

To maintain security for the system and users, Android requires apps to request permission before the apps can use certain system data and features. Depending on how sensitive the area is, the system may grant the permission automatically, or it may ask the user to approve the request. These permissions are declared in AndroidManifest.xml file.

**1.4 Android Security Issues**

**1.4.1 General Security Issues**

* In the latter part of 2010 and early 2011, a vulnerability issue was discovered in Android versions 2.2 and 2.3, respectively. The vulnerability is that an attacker can copy any file that is stored on the device’s SD Card without granting a permission or even without a visible cue that this is happening.
* The idea for android being open source itself is a problem; attackers can analyze each line of code to determine its weaknesses.
* Google play store is a bit of concern because of the relative ease of getting apps approved for sale. Malware apps can squeak through.
* In Android, other than google play store, it is possible to install the applications from unknown sources, like third-party android stores. It is one of the major security breaches in Android.

**1.4.2 Permission Escalation Attack**

It allows a malicious application to collaborate with other applications to access critical resources without requesting for corresponding permissions explicitly.

**1.4.3 Collision Attack**

Collision attack is a technique wherein two or more application share the same user ID so that they can access the permissions, which are granted to each other. For example. If application A has permissions to READ\_CONTACTS, READ\_PHONE\_STATUS and B has permissions to READ\_MESSAGES, LOCATION\_ACCESS, if both the applications use the same user id SHAREDUSERID, then it is possible for application A to use the permissions granted to itself and the permissions granted to B. Similarly, it is possible for application B to use the permissions granted to itself and the permissions granted to A. Every Android application has unique ID that is its package name. Android supports shared User ID. It is an attribute in AndroidManifest.xml file. If this attribute assigned with the same value in two or more applications, then they can access permissions granted to each other.

**1.4.4 Dangerous Permissions**

Dangerous Permissions can access critical resources of the mobile. Dangerous permissions can give the app access to the user's confidential data. If app lists a normal permission in its manifest, the system grants the permission automatically. If app list a dangerous permission, the user has to explicitly give approval for the app for the successful installation of the app. Example:

CONTACTS

READ\_CONTACTS, WRITE\_CONTACTS,

GET\_ACCOUNTS

LOCATION

ACCESS\_FINE\_LOCATION,

ACCESS\_COARSE\_LOCATION

SMS

SEND\_SMS, RECEIVE\_SMS, READ\_SMS,

RECEIVE\_WAP\_PUSH, RECEIVE\_MMS

STORAGE

READ\_EXTERNAL\_STORAGE,

WRITE\_EXTERNAL\_STORAGE