Analysis and Research of System Security Based on Android

Loshima Lohi
Asst. Professor
Carmel College, Mala

Abstract: **Android may be a smart mobile terminal operating platform core on Linux. But thanks to its open-source software and programmable framework character, it leads the Android system susceptible to get virus attacks. This paper has deeply researched from the Linux system security mechanism, Android-specific security mechanisms and other protection mechanisms. And on this basis, Android devices have achieved closely guarded on normal state. So that attackers cannot use the kernel module or core library to get highest access permission and be attacked. Meanwhile, to further strengthen the security of Android devices, it enables them to properly handle the high-risk threat. This paper also strengthened intrusion detection system (HIDS) based on the host in order to detect malicious software and strengthen the Android system-level access control.**
Keywords – Android, System Security

INTRODUCTION

Android is a software stack for mobile devices that has an OS , middleware and key applications. Android SDK is used to develop android applications. It uses Java programming language. It is planned to run on differing types of devices. Android platform is based on Linux technology. It is composed of OS, interface and application components. Its issuance breaks the monopoly status of Microsoft windows mobile OS and Nokia's Symbian OS. It allows anyone to develop him own applications. So there's an opportunity that a user is probably going to download and install malicious software's written by software hackers.

ANDROID PLATFORM ARCHITECTURE

Android has built in tools. Android platform composed of Linux kernel, system libraries, android run time, and application framework then on five parts. Android relies on Linux 2.6 version. It provides core system services security, memory management, process management, network group, driven model. The core part is similar to an abstract level between the hardware layer and other software within the systems. Android includes a set of C/C++ libraries. Android's core libraries provide
most of the function to the Java class libraries.

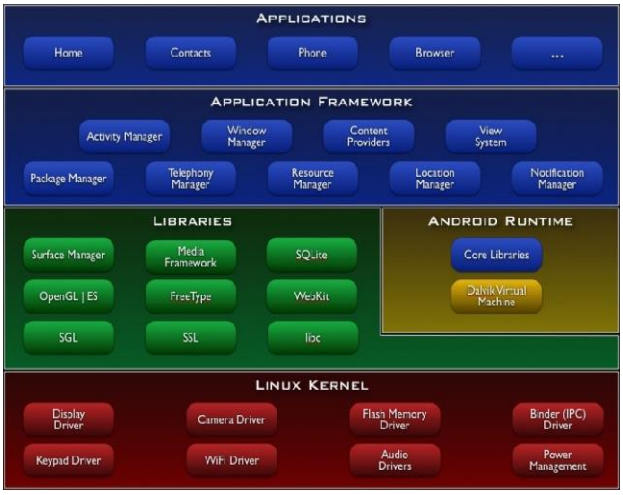

Fig 1: Android Architecture

ANDROID RUNTIME

Android runtime consists of two components. First, a set of core libraries. Second, the Virtual machine Dalvik. Java programs are received and translated by the VM Dalvik. Applications will be encapsulated in Dalvik. A VM is available for every and each program even though some programs are running in parallel.

APPLICATION FRAMEWORK

An application framework is a software framework that's used to implement a typical structure of an application for a selected OS. Any application can publish its own features. These functions can be used by any other application.
Now like most of the main software and operating platforms on the world Android also comes with a software development kit which is termed commonly as Android SDK. Android SDK provides you the API libraries and tools for building and developing new applications on Android operating environment using the java programming language. This procedure of developing the applications on Android platform in java programming language using the tools and API libraries provided by Android SDK is named as Android Application Framework.

BASIC FEATURES SUPPORTED ANDROID APPLICATION FRAMEWORK

Android Application Framework supports the features that made us use and luxuriate in the wide selection of applications for kind of uses. Here are some of the important features:
1. WebKit engine based integrated browser.

2. Optimized graphics powered by the advanced graphics library.
3. SQL for storage of structured data.
4. For various types of video, audio and image formats media support.
5. Device emulator, tools for debugging, etc.

In the above mentioned list we did not mention some of the hardware dependant features as these tend to largely vary as per the device, though nevertheless android application framework support them. Some of the device dependant features supported by android include GSM telephony, network connection profiles such as Bluetooth, Edge, 3G, WiFi, utility features such as camera, compass, GPS, etc.

APPLICATIONS

Applications are written in Java programming language. The Android SDK tools compile the code into an android package, an archive file with a .apk suffix. The android software platform comes with a set of basic applications. These applications can run simultaneously.

Android initially came into existence with the sure fire concept that developments are given the ability and freedom to make enthralling Mobile applications while taking advantage of everything that the mobile handset has to offer.

Android is built on open Linux Kernel. This particular software for Mobile Application is formed to be open source, thereby giving the chance to the developers to introduce and incorporate any technological advancement. Build on custom virtual machine android gives its users the addition usage and application power, to initiate an interactive and efficient application and operational Software for your phone.

Google's mobile operating device, the android is its awesome creation within the definitive creation of Software Applications for the mobile arena it also facilitates the g-juice in your mobile thus initiating an entire new world of Mobile Technology experience by its customers.

We at Arokia IT are technically equipped to initiate any level of those amazing software applications using the android genius from Google. Around within the year 2007, Google announced its Android OS and Open Handset Alliance with these two major contributions to the mobile industry that ultimately changed our experience with mobile interface.

OPEN HANDSET ALLIANCE

Open Handset Alliance is an amalgamation of Tech Companies with common and particular interest within the mobile user enhancement experience. Companies like Google, HTC, Motorola, Samsung, Telecom Italia, T Mobile, LG, Texas Instruments also as Sony Ericsson, Vodafone, Toshiba and Hawaii are Tech giant supported their core abilities and strengths, while keeping and pursuing the characters and goals of every company, their basic idea of this joining of hands was the feature-rich mobile experience for the end user. This alliance meant the sharing of ideas and innovation, to bring out these ideas into reality. This provided the millions and millions of Mobile users the experience that they never had.

Like the Apple iphone, Android OS allows third party developers to innovate and build Applications and software for mobile devices. Android is an open, flexible and stable enough to associate itself with newer and newer evolving Technologies. Android's vast range of easy to use tools and wide selection of libraries provides Mobile Application developers with the means of a tremendous mobile operating software to come up with the foremost efficient and rich Mobile Applications changing the world of many mobile users.

SERVICES

A service is a component that runs within the background to perform long-running operations. For example, a service might play music in the background while the user is during a different application, or it'd fetch data over the network without blocking user interaction with an activity.

ANDROID SECURITY

a) Android's Five Key Security Features:

1. Security at the OS level through the Linux kernel
2. Mandatory application sandbox
3. Secure inter process communication
4. Application signing
5. Application-defined and user-granted permissions

b) Android System Security

In the default settings, no application has permission to perform any operations that might adversely impact other applications, the OS, or the user. Android's security mechanism is especially reflected in 2 aspects - Android system security and data security.

c) Android Security: System-Level Security Features

The Linux kernel provides Android with a group of security measures. It grants the OS a user-based permissions model, process isolation, a secure mechanism for IPC, and the ability to get rid of any unnecessary or potentially insecure parts of the kernel. It further works to stop multiple system users from accessing each other's resources and exhausting them.

ANDROID APPLICATION SECURITY FEATURES

This user-based protection allows Android to make an "Application Sandbox." Each Android app is assigned a unique user ID, and every runs as a separate process. Therefore, each application is enforced at the method level through the Linux kernel, which doesn't allow applications to interact with each other , and provides them only limited access to the Android operating system. This gives the user permission-based access control, and he/she is presented with an inventory of the activities the Android application will perform and what it'll require to try to to them, before the app is even downloaded. The same goes for file system permissions – each application (or user) has its own files, and unless a developer explicitly exposes files to a different Android application, files created by one application can't be read or altered by another.

a) Android Application Security Scans

When building and testing the safety of Android apps, developers should follow Android security best practices

and keep the following in mind when performing security tests:
• Inbound SMS listeners (command and control)
• Unsafe file creation
• Improper database storage
• Unsafe use of shared preferences
• Storage of sensitive data on mass storage device
• Content provider SQL injection
• APN or proxy modification

b) Android Security: Geared Towards User-Friendly Security

All of Android's more technical security measures are designed to be simply presented to the user, meaning that they will be easily controlled through the interface. Straightforward methods of improving your Android device's security can include: using a password or pin, setting your phone to lock after a period of inactivity, only enabling wireless connections that you use, and only installing Android apps you trust and have personally vetted.

Google also only allows tested and proven secure Android applications into its marketplace, meaning that the user has less of an opportunity of putting in a malicious app. Furthermore, the Android security system prompts the user to permit the installation of an application, meaning that it's impossible to remotely install and run an application. Users can further make sure that their Android device is secure by regularly installing system updates.

c) Android system security protection

Android system safety inherited the planning of Linux within the design ideology. In practice, each Android application runs in its own process. In the OS, each application runs with a singular system identity. Most of the security functions are provided by the permission mechanism. Permission are often restricted to particular specific process operations. Android is privilege separated. Data security mainly relies on software signature mechanism. It uses AndroidManifest.xml file. When specified software services are called, the system first checks this file. To make use of protected features of the device, one must include in Android Manifest.xml, one or more tags declaring the permissions.

ANDROID ANTI THEFT SECURITY

The ultimate security for Android device just in case it's ever lost or stolen. Advantages of this feature are accurate tracking, encoding , Spy camera activation and Device lock down. It also validates permissions for send SMS messages, hardware controls, take pictures and videos, your location, fine (GPS) location, receive SMS , read SMS or MMS, edit SMS or MMS, full internet access, read contact data and write contact data.

REFERENCES

[1] Android Open Source Project. "Security Overview." Tech Info. N.p., 2012. Web. 18 June 2012. http://source.android.com/tech/security/index.html .
[2] http://www.arokiait.com/whatis-android.htm
[3] Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on 13 February 2012
[4] Transcript of Analysis And Research Of System Security Based On Android Analysis and Research Of System Security Based On Android By Raghunath