2012 Fifth International Conference on Intelligent Computation Technology and Automation

Analysis and Research of System Security Based on Android

Han Bing

North China University of Technology, Beijing, ,100144, China
jluhan_bin@163.com

***Abstract*—Android is a smart mobile terminal operating platform core on Linux. But due to its open-source software and programmable framework character, it leads the Android system vulnerable 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 can not 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, Abnormity Detection

I. INTRODUCTION

Android is a software stack for mobile devices that includes an operating system, middleware and key applications. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language.[1]

Android is planned to run on many different types of devices. For developers, the range and number of devices means a huge potential audience: the more devices that run Android applications, the more users who can access application. In exchange, however, it also means that applications will have to cope with that same variety of hardware.

Android platform is based on Linux technology and composed of operating system, user interface and application components. It allows developer freedom access and modify the source code. It is the free mobile terminal platform with open, the application program equality, no boundaries between applications, facilitate and rapid application development and other advantages. Its issuance breaks monopoly status of the Microsoft Windows Mobile operating system and Nokia's Symbian operating system in the smart mobile telephone platform, while the advantages of its platform also greatly enriched the variety of handheld device software functions. It becomes the intelligent terminal market leader.

Android platform is a set of software package for mobile devices, it includes an operating system, middleware and key applications. Android uses the most innovative characteristic. It allows anyone develop him own applications and freely distributed. But when open provides various conveniences for developers and users, it also increases the safety misery. Due to the lack application development and issuance of effective control, the user is likely downloaded and installed malicious written by software hackers. This will result in some or all of the features in the mobile telephone not work properly. So it deeply studies Android's security mechanisms, it can effectively enhance the protection ability and great significance

II. ANDROID PLATFORM ARCHITECTURE

Android has built-in tools and support which make it easy for applications to do that, while at the same time letting the system maintain control of what types of devices application is available to. With a bit of forethought and some minor changes in application's manifest file, it can ensure that users whose devices can't run application will never see it in the Android Market, and will not get in trouble by downloading it. This can explains how it can control which devices have access to its applications, and how to prepare its applications to make sure they reach the right audience.

Android provides an open development platform and offers developers the capability to build greatly rich and innovative applications. Developers are free to be superiority of device hardware, access location information, run background service, set alarm, add inform to the status bar, and so on.

Developers have full access to the same framework. The core applications use APIs. The application architecture is designed to simplify the reuse of components; any application can publish its abilities and any other application may then make use of those abilities. This same mechanism permits components to be replaced by the user.

From top to bottom Android platform is composed of the Linux kernel, system libraries, Android run time, application framework and so on five parts. It is shown in Figure 1 of the following:

A. Linux Kernel

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 equivalent to a abstract level between the hardware layer and other software in the systems,

B. Library and Android Runtime

Android includes a set of C/C++ libraries. Various components of Android system are use now. These functions are exposed to developers through the Android application framework. Android's core libraries provide most

978-0-7695-4637-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ICICTA.2012.152

of the function to the Java class libraries. Every Android application runs in its own process, and enjoys the proprietary instance distributed by Dalvik virtual machine, and support multiple virtual machines efficiently run on the same device.

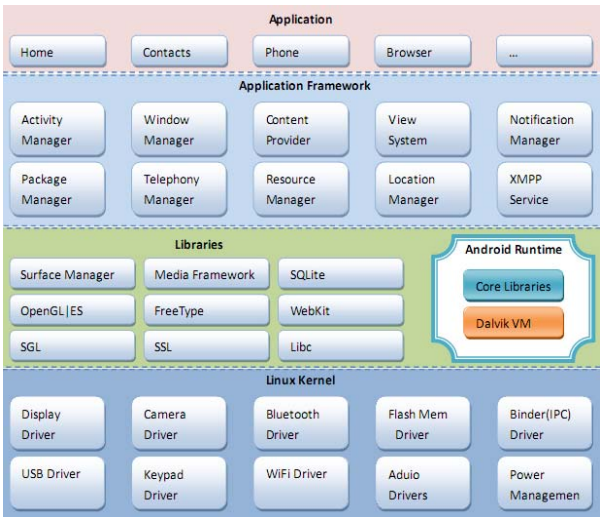

Figure 1. Android System Architecture

C. *Application Framework*

Upper core application program of Android system is reply on frame arrangement API development, application architecture can simplify component reuse mechanism. Any application can publish its own features. These functions can be used to any other application (of course, it is restricted from the framework constraints safety standards); and the same to reuse mechanism, the framework supports component replacement.

D. *Applications*

Android applications are written in Java programming language. The Android SDK tools compile the code—along with any data and resource files—into an Android package, an archive file with an .apk suffix. All the code in a single .apk file is considered to be one application and is the file that Android-powered devices use to install the application.

The Android platform default includes a set of core applications. It includes home, browser, communication services, contacts and other applications. These applications are written by the Java programming language. It can provides developers a reference. As the Android platform applications equality, developers can write their own applications to replace the default applications provided by Android.

III. ANDROID SYSTEM SECURITY

The core design idea of Android security architecture is as the following. In the default settings, all applications do not have permission for other applications, systems or users greater impact on the operation. This includes read and write user privacy data (contacts or e-mail), read and write other applications files, access the network or block devices and so on.

Android's security mechanism is mainly reflected in two aspects: Android system security and data security. Android system security is referred to the protection of smart terminal itself to operating system. It can prevent unauthorized user external access and authorized service permission. It includes users' behaviour detection, operating authority and other measures. The data security is referred to ensure the integrity and legitimacy of stored data, it requires the system can properly transmit data, the authorization process successfully read data.

A. *Android system security protection*

Android system safety inherited the design of Linux in the design ideology, Android provided security, memory management, process management, network management, drive model and other core service in the kernel. The kernel part is actually a abstract level between hardware abstraction layer and other software group. In practice operation, each Android application runs in its own process. Android system applications are run in some low-level function such as threads and low memory management; Android itself is a separate operating and permission system. In the operating system, each application runs with a unique system identity (Linux user ID and group ID). Each parts of the system were also using their own independent identification mode. The most security functions of the system are provided by the permission mechanism. Permission can be restricted to particular specific process operations, and can also restrict URL permission to access specific data segment.

B. *Android Data Security Protection*

Android is a operating system with privilege-separated. Each application runs with a distinct system identity in android. Parts of the system are also separated into distinct identities. So Linux separates applications from one another and the system.

Additional finer-grained security features are provided by a "permission" mechanism that enforces restrictions on the specific operations that a particular process can perform, and per-URI permissions for granting ad-hoc access to specific pieces of data.

Data security mainly relies on software signature mechanism. Android and applications are both needed sign. When it releases, at first it need generate a public key and private key through development/tools/make_key. The tools ./out/host/linux-x86/framework/signapk.jar provided by Android, the main role of signature is to modify program limited to the same source. The system has two main ways to detect. If the program is upgrade install, it needs check whether the signature certificate of old and new program are consistent. If it is not the same, it will failed install. To application permission for the protected level of signature or signature or system, it will check the certificate of permission requester and permission of declarer is the same.

It uses AndroidManifest.xml file to achieve software's data security function. When the specified software services is called, the system first checks AndroidManifest. Xml file in the software, namely the software master configuration file. Which contains a <uses-permission> label to declare operating authority :

```
<manifest>
  <uses-permission
android:name="android.permission.READ_***" />
<uses-permission android: name="android.permission.
RECEIVE_***" />
<uses-permission
android:name="android.permission.SEND_***" />
</manifest>
```

According to the permission declaration, system checks the relevant permission when software installation and calling. If the system will successfully execute when it own with the permission, otherwise it reject operation.

IV. ANDROID SECURITY PERFORMANCE IMPROVEMENT

Although the Android security mechanisms has ensured through the system and data security mechanisms, but it does not mean that there is no android security risks. Current there is security risks exist and combined with today's mobile devices against attack, this paper has deeply researched on the android mobile devices based on Linux kernel attacks.

To ensure system security requirements, it is necessary to implement detecting malicious software on mobile devices. The software has evaluated the running process. This framework relies on a lightweight agent and continuous samples various characteristics on the device. Using self-learning, adaptive method to analyze the collected data, and then infer the device's health status. Framework provides API extraction keyboard, touch screen, scheduling and memory and Linux kernel operating.

Android devices have developed many applications. The SDK provides many tools to facilitate. These tools could be accessed according to the command line or Android Development Tools. As Android could straight call the tools Developing with Eclipse. So it needs the preferred method when it develops applications.

When it selects to develop another IDE or a simple text editor and calls the tools on the command line or with scripts. As it will have to call command line tools manually on occasion, this is a less streamlined way to develop. At the same time it will have access to the same number of functions that it would have in Eclipse.

As the Android system is based on the Linux kernel, so it there exists a lot of vulnerabilities like Linux, it has become the focus of the current target attacked by hackers. Because it exist loophole, hackers have developed a number of exploits to steal users' privacy, deductions and other malicious software. The malicious software can start malicious processes in the background through automatic network. It stole the privacy content of mobile telephones and directly threat user's security.Intrusion detection system framework is designed as the following in figure 2:

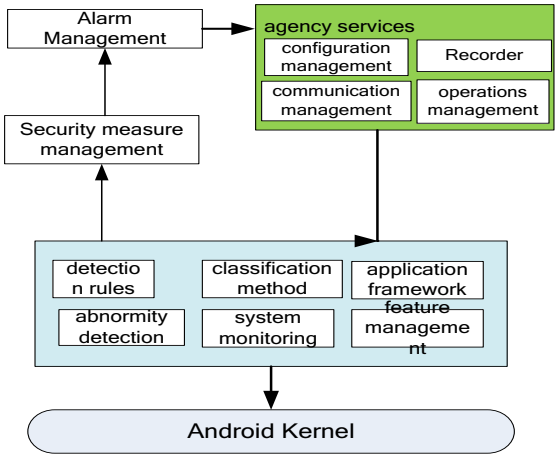

Figure 2. Intrusion Detection System Framework

In order to further strengthen the Android system and underlying access control which belong to privileged user in critical Linux process. System adopts SELinux to avoid an attacker controlling the system process using high-privilege. When the system is running SELinux on Android. Experiments show that Android devices running on SELinux is feasible. The user can establish a customized security policy to improve the system security level

V. CONCLUSIONS

The Android's goal is to establish a enormous installed base for developers to take advantage. One of the method it will accomplish this is according to different kinds of hardware running the same software environment. But it also recognizes that only developers know which kinds of devices their applications make sense on. It has built in tools to the SDK and set up policies and requirements to ensure that developers remain in control of their apps, today and in the future. With the information it just read, and the resources listed in the sidebar of this document, it can publish its application with the confidence that only users who can run it will see it.

In this paper, it has analysis Android system's security mechanisms with widely used in mobile platforms. It has separately introduced its system architecture, security mechanism and safety problems. Through it has analysis Android security mechanisms and its components, it has set to the Android security, safety mechanism side, system security and data security. It has promoted system security to system permission. At the same time it analysis the Android security risks, it has deeply researched the attack based on Linux kernel. It has proposed security mechanisms based on SELinux policy theory to ensure system security on application program framework layer. Not only from the Linux kernel layer, it uses Android's security framework to ensure system security from the application layer intrusion, so it is essential to research and develop the method to protect the Android framework. This work will be the reference base to the Android further security analysis.

ACKNOWLEDGMENT

The work is supported by "Science Park Cup" Students scientific and technological innovation projects "Design and Implementation of Personalized smart telephone lock/ unlock " of North China University of Technology in 2011.

REFERENCES

[1] http://developer.android.com/guide/basics/what-is-android.html

[2] Android Kernel Issues.http://www.kandroid.org.

[3] Benj amin Speckmann.The Android mobile platform[EB /OL].[2008-04-26].

[4] http: // www.emich.edu /compsci /projects /Master_thesis-Benjamin_Specklnann.pdf.

[5] Gong lei, zhou chong, Development and Research of mobile terminal application based on Android, [J]. Computer and Modernization, 2008.86-89.

[6] Shabtai A,Fledel Y,Elovici Y.Securing Android-powered mobile devices using SELinux.IEEE Security & Privacy,2010:36—44.

[7] Chatterjee, S. Abhichandani, T. Haiqing Li.TuIu, B. Jongbok Byun. Instant messaging and presence technologies for college campuses[J] . IEEE Net wo rk, 2005, 19 (3) : 22-33.

[8] Chan Yeob YeunSalman Mohammed Al-Marzouqi. Practical Implementations for Securing VoIP Enabled Mobile Devices. International Conference on Network and System Security (NSS 2009) 3rd.

[9] ED P Saint..Andre. RFC3921, Ex tensible messag ing and presence pro tocol (XM PP) : instant messag ing and presence[S] . [S. l.] . IETF, 2004.

[10] Shin W,Kwak S,Kiyomoto S,et al.A small but non-negligible flaw in the Android permission scheme.IEEE International Symposium on Policies for Distributed Systems and Net-works,2010:109—110.

[11] Shin W, Kiyomoto S, Fukushima K, et al. A formal model to analyze the permission authorization and enforcement in the android framework . International Symposium on Secure Computing (SecureCom-10) 2010:944—945.

[12] Enck W , Ongtang M , McDaniel P . Understanding android security. IEEE Security & Privacy, 2009;7(1):53—54.

[13] Shabtai A,Kanonov U,Elovici Y.Intrusion Detection on mobile devices using the knowledge based temporal-abstraction method.Systems and Software,2010;83(8):1527—1536.

[14] Prince McLean.Inside google's Android and Apple's iPhone OS as business models.roughlyDrafted Magazine.November 10,2009.