Research on Security Architecture of Mobile System

Weiwen He

School of Information Engineering, Guangzhou Nanyang Polytechnic, Guangzhou 510000, China
hww2018@163.com

Keywords: Mobile system; Mobile devices; Security threaten; Security protection system; Security policy

Abstract. With the development in mobile technology and communications infrastructure become more sophisticated and popular, more and more people have not only in the office handling daily affairs units, they with mobile phones， PDA, and laptops and other mobile terminals via public communications networks to access the unit's internal resources and applications. But this also through the public network access unit network introduces new security threats, the traditional VPN has failed to meet the existing smart phone/tablet PCs and other mobile terminals, secure access needs: on the one hand, how to ensure security in open networks in the mobile end-user identity and access security, data confidentiality and Mobile transmission process consistency and integrity and other safety requirements; on the other hand, due to the mobile terminal is easy to lose, how to ensure that data is stored within the mobile terminal security. Therefore, this paper studies security system and the security threat based on the framework of Android mobile system, and puts forward some corresponding preventive measures.

Introduction

Nowadays, more and more mobile terminal equipments enter the internal network, search through all kinds of enterprise interior data, and at the same time reveal variety of business. This gives a disastrous blow to the enterprise information security administrators ,because administrator can not control all these devices. This means that there are hidden safety troubles throughout the process of using huge a large number of business data transmission. That is to say, the mobile devices are not isolated now, they are all connected to the terminal of cloud service entrance. In addition, there are many users who connect their mobile terminal data synchronization to their home computers directly, which makes the enterprise core data stored in unsafe place probably. In this paper, the security model of the Android mobile platform will be discussed, to explain this equipments' behavior and how it produce threats to companies' sensitive data.

Android System Structure

Android system is the environment executed on the mobile device applications. The Android platform frame includes 5 parts: the Linux kernel layer. The Android core system services bases on the Linux 2.6 kernel. The memory management, process management, network protocol and drive models all dependent on this kernel layer. At the same time, the Linux kernel is as an abstraction layer between the hardware and software. The Android library which is above the Linux kernel is a set of c /c++ library, and is used by various components of the system. The Android function environment includes the Dalvik virtual machine and the core library. Dalvik runs .dex files. The core libraries are written in Java language, providing a large number of Java 5 SE package subclass and some android special libraries. Application framework is written in the Java language, which is the basis for the development of android. The layer is mainly composed of a view, a notification manager, and an activity manager which is used to call components directly by developers. The Application layer writes programs in Java language in a virtual machine, including the android system tied to the core application, such as SMS short message procedure, calendar, browsers, and programs which can be downloaded by user. The

  DOI: 10.25236/icess.2019.259

Android platform framework is exhibited in figure 1.

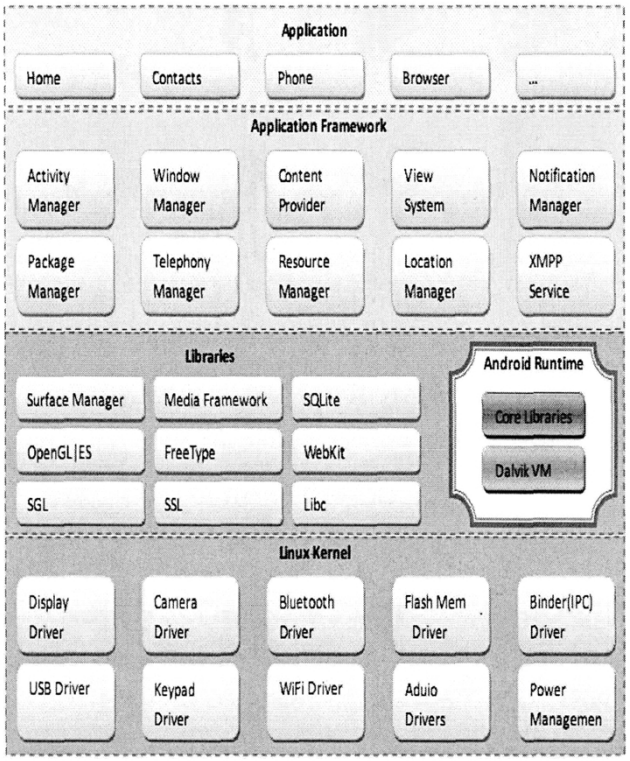

Figure. 1 Android platform framework

Android Security System

In the Android security mechanisms (e.g: Table I), there are both the traditional Linux security mechanism and Dalvik virtual machine security mechanisms, as well as android's unique security mechanism .

Table I Android System Security Mechanism

System architecture layer	Security mechanism
1、Linux Kernel	File access control
	POSIX User
2、The Android local libraries and Running environment	Memory management unit （MMU）
	Mobile equipment safety
3、Application Framework	The application of access control
	Component package
	Signature mechanism

Android is the core of the Linux operating system and based on the Java platform, using Dalvik's virtual machine to explain the Java language. The Android security model is based mainly on three aspects: the traditional access control, isolation, and a security mode basing on authority and signature mechanism [1].

Mobile Applications System Threats

Mobile equipment (client) security.

The Android operating system is based on the Linux kernel and uses mobile device security designs , no longer dependent on third party security software. It only relies on its own platform security to ensure that users data will not be threatened. But how secure the platform is should be examined through the study of android platform security model, discussing its effectiveness to the current mainstream attacks.

Attacks on the core program of the system.

Core system programs include the system local library, the Dalvik Java virtual machine, and the foundation Java class library. The system library mainly involves various underlying functions and complex calculation functions, which are used by the system processes or Dalvik through the JNI (Java Native Interface) . These functions are written in C / C + +， lacking mandatory type safety mechanisms. At the same time, the Dalvik process occurring errors through the JNI using the system function can lead to the Dalvik collapse process, so it can lead to memory space occupied or malicious code executed. Dalvik is all applications running environment, which security will affect all applications. Vulnerabilities in the Android system mainly focus on the customization of SQLite, WebKit and the new library today.

2) Attacks on the application programs.

The application programs include the android system and the applications installed by users. Because the users installed applications were from a variety of sources, which cannot be verified, the most easy means of attack is through these applications. In the process of installation, users are unable to identify malicious programs and normal programs, choosing to trust the application, and ignoring the associated safety tips, giving all permissions, which will greatly weaken the core security mechanism(application access control). Malicious programs can get higher jurisdiction by forging signatures. Now the Internet's most popular browser attacks, such as cross-site scripting、 URL coding、social engineering，as well as the SQL injection attacks for the SQLite database，will be widely used by attackers in the mobile internet. These attack methods are diversity and simplicity, so that the applications have become the emphases for hacker; At the same time, because of the existence of the underground gray chain, the attacks based on application programs are more commercial value, such as malicious debits, flow access and so on.

3) Data loss and integrity threats

When the user’s equipments exist more sensitive information, we should pay special attention to the risk of data loss. Users can access their mobile equipments containing a sensitive data enterprise email attachment. If their equipments are stolen, in some cases, the attackers will be able to access the sensitive attachment by passing from the apparatus extracts the built-in SD flash memory cards simply. Data integrity attack refers to the attackers trying to damage or modify the data on the devices. Attackers may try to launch such attacks, for example, encrypting user's data until they pay the ransom fee.

Information security of mobile communication transmission process.

Information may be intercepted and deleted during mobile equipment and enterprise application server processes. So the mobile application system must guarantee the consistency and security of data.

The internal (server) security.

The security protection system can generally refer to the existing enterprise information system security policy (for example, network security, firewall policies, system access strategies) . It can fit the requirements for the security.

The Security System Based on the Structure of the Android Mobile Application System

Mobile terminal security solutions.

The following will studies some feasible、effective security solutions.

1)Using safety web browser

Some security software vendors introduce safety browser applications (for example, UC browser、QQ browser、360 browse、Opera and so on), to protect the user's web browsing process on the Android platform. These applications replace the original system's built-in browser with third party software installed on the devices. Safe browsers can prevent web attacks and social engineering attacks effectively， preventing the download of malicious software through the browser .

2) KBTA(Knowledge--based Temporal Abstraction) technology

We can adopt the method of light Knowledge Based Time Abstraction (KBTA) to detect the malicious software and it can be activated by equipments with limited resources[2]. Deploying the KBTA and the basic knowledge of time abstraction, we can monitor the data (e.g. the number of the operating processes) and incidents (e. g: software installing). The security ontology serves as the basis of time abstract knowledge and the process of obtaining the higher level and meaningful concepts and modes from the original time-oriented security data is called the time abstracting[3]. This method is applicable to the Android equipments to detect the malicious software. The assessment results showed that the proposed method is effective in detecting the malicious programs (the general detection rate is 94%) and feasible in operating (the average CPU usage is 3%) in mobile devices.

3)Sandbox technology

Sandbox solutions provide a safe working environment to the system, on which users can access enterprise email, calendars, contacts, the company website, sensitive documents and other enterprise resources through sandbox[4]. All data and data transmission in sandbox are encryption processed through sandbox. Before using sandbox users must first pass login through the enterprise server's authentication and authorization system. Sandbox is configured by the enterprise manager. If one device is lost, it is very easy to cancel its authorization.

Equipments is divided into two regions according to this solution. One is a security area for the enterprise data to be used, and the other is a private data area for individual users[5]. The advantage of this is that users can access internal data safely by using their own equipment, protecting enterprise information effectively, such as internal websites, e-mail and calendar. Sandbox also can serve very well to prevent both malicious and inadvertent data loss.

4) PIFAC (Platform-independent and Flexible Access Control Framework) technology

PIFAC is a cross platform based on a mandatory access control security module ,which has been applied to Windows, Linux desktop and server systems and Rterms embedded system platform. It abstracts platform features, so can be transplanted to new platform easily.

PIFAC includes three parts: a security server, an operating system Hook layer, and the strategy[6]. The security server realizes storage and judges implementation strategy, being a independent platform part; The role of the operating system hook layer is to intercept visits which main body(refers to initiating access to object entity, process mainly) faces to object(refers to all preserved information entities and other resources, such as directory, file and network access port) in system, different systems have different implementation strategies. The implementation of a Hook layer in the Android system is required, and formulate corresponding strategy according to the system configuration. Figure 2 shows the framework for the PIFAC in Android system.

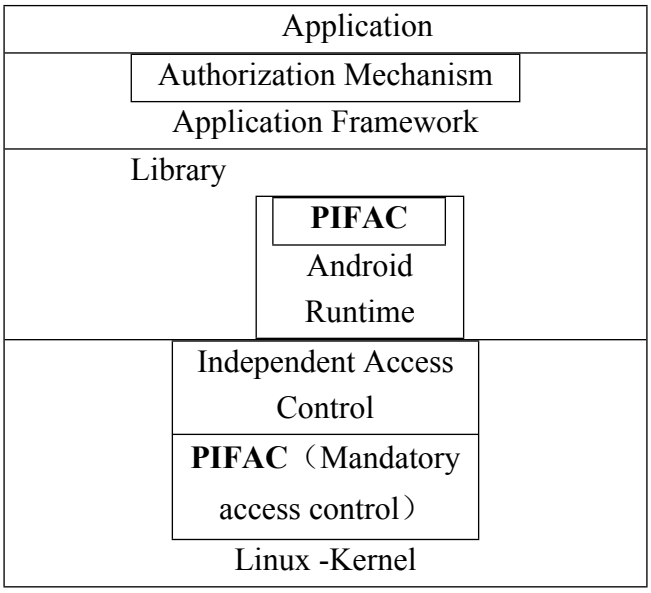

Figure. 2 PIFAC Implementation Framework

Information security of Mobile communication process.

The security technology generally includes data encryption, authentication service, and virtual private network (VPN) technology, based on SOA technology scheme. This paper mainly analyses the framework of the SOA security mechanisms.

The approach of this security mechanism is to use user authentication on the web server, such as BASIC authentication. The APIs which handle the HTTP protocol on the mainstream smart phone platform support the BASIC authentication, thus ensuring the service interface on the server can be accessed only by the authorized users, and with an SSL certificate , using the HTTPS protocol instead of HTTP protocol for transmission on the server side, which can guarantee the security of Web Service . Because data encryption lies in the transport layer, the programs do not need an additional process to HTTPS.

In addition, Web Service can achieve data encryption on the SOAP message layer through Web Service security specification (WS-Security[7]), and ensures data consistency and security. The basic principle is that by extending the SOAP data, in which append the encrypted user authentication information, the data can not be cracked even if intercepted.

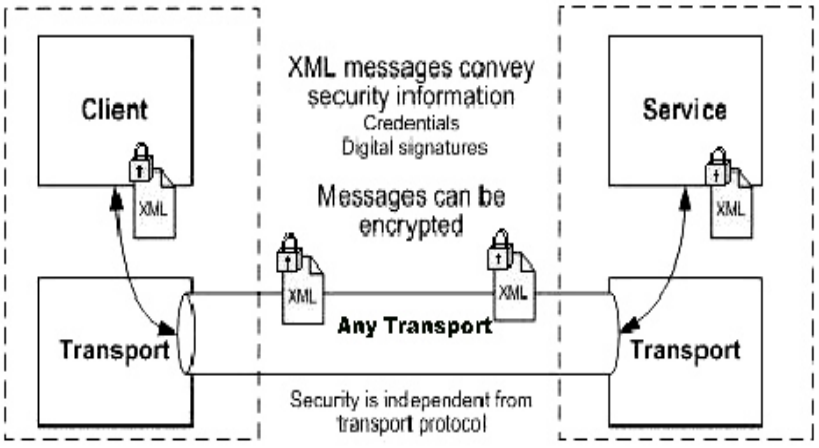

Figure. 3 SOA Security architecture diagram

Summary

With the continuous development of computing and network communications technology, the security threats of the enterprise application systems are constantly changing. Users' demands rise ceaselessly, and enterprise mobile platforms strengthen user data security constantly at the design level. From the underlying design, we refine access control permissions, isolate application and data encryption access. On the other hand, this design requires users to weigh the various authority security, to ensure different levels of reliability. Although mobile communication technology brings more enterprise users, it increases data security risks when enterprises use mobile application systems.

In summary, mobile application systems improve the productivity and profitability of the enterprises greatly, but also increase the risks to enterprise data security and increase the cost of enterprise management. This article studies Android-based system's platform security model to increase users security awareness, and to help enterprises efficiently manage and prevent various risks.

References

[1] Fu Yi Yang, Zhou Dan Ping . Analysis to Security Mechanism of Android [J]. Information network security, 2011, 10(9) :19-20.

[2] Shabtai A, Kanonov U, Elovici Y. Detection, alert and responseto malicious behavior in mobile devices: knowledge-based approach. RAID, 2009

[3] [Shabtai A, Kanonov U, Elovici Y. Intrusion Detection on mobile devices using the knowledge based temporal-abstraction method. Systems and Software, 2010

[4] Li Qi. The principle of virtual firewall CPU protection mechanism and improvement [J], software,2010, 31(10):37-40.

[5] Pan Li. The characteristics of the mobile phone virus and protect against it [J]. The computer and telecommunications, 2011,25- 27.

[6] Hu Da Lei, Zhou Xue Hai. Research and Implement of Platform-independent and Flexible Access Control Framework. Computer system application, 2010,19(3):17-20.

[7] OASIS.WS-Security--Specification[EB/OL]. http://www.oasis-open.org/home/index.php

[8] Antonín, Slaby, Tomáš, Kozel, Hana, Mohelská. Mobile services and architectures[C]// Proceedings of the 13th WSEAS international conference on Communications. World Scientific and Engineering Academy and Society (WSEAS), 2009.

[9] Sun L , Huang S T , Wang Y W , et al. Application Policy Security Mechanisms of Android System[C]// High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on. IEEE, 2012.

[10] Xing Z , Wei H . The structure design of database security monitoring system based on IDS[C]// International Conference on Computer Engineering & Technology. IEEE, 2010.

[11] Zhang Y H , Huang R . Design and Implementation of the Smart Home Security Control System Based on the Android Platform[J]. Advanced Materials Research, 2013, 753-755:3120-3124.