Advances in Engineering Research, volume 122
7th International Conference on Applied Science, Engineering and Technology (ICASET 2017)

Analysis and Research on Security Mechanism of Mobile Intelligent Terminal Operating System

Mingxin Zhao[1, a]

[1] Computer Centre , Anshan Normal Collge Anshan, China

[a]email: zhao_mx@hotmail.com

Abstract. From the aspects of production and characteristic of mobile intelligent terminal operating system, and its application on mobile phones, etc., this article mainly introduces the development of mobile intelligent terminal operating system. The paper also analyzes the security problems of mobile intelligent terminal operation system, and the main mobile intelligent terminal operating system security mechanism. The study points out the development direction of the mobile intelligent terminal operating system security technology.

Keywords: Mobile Intelligent Terminal, Operating System, Security Problems

Introduction

Mobile intelligent terminal refers to the computing devices which run with embedded operating system, can be used on the move.In the broad sense it includes mobile phones, laptops, tablets, POS, even the on-board computer.But in most cases it refers to the smart phones and tablets with a variety of applications.Now mobile phone industry is generally accepted that whether to run the embedded operating system and whether it can support the third party software are watersheds between smartphone and the dumbphone.

The characteristics of the mobile intelligent terminal operating system

System kernel is very small

Mobile intelligent terminal operating system is used on small devices which has vey less hardware resources, in addition to running the operating system itself,it has to run the function modules. The operating system has only a management function, so the mobile intelligent terminal operating system must make the kernel very small to make the function needed running on limited resources.

System is designed for specific application

Due to the variety of the small devices, it is destined that the function of the mobile intelligent terminal operating system can't completely consistent. After all mobile intelligent terminal operating system eventually operates the underlying hardware of device, and closely relates to hardware, so different configuration are needed by different, different configuration are also needed by various people who have different requirement even with the same hardware resources.

System can be simplified by need

Mobile intelligent terminal operating system is used running on small devices, the hardware resources is limited. Some unnecessary features or modules will be removed in the process of migration in order to save resources. In addition, because it runs on small devices, whose function cannot be compared with computer performance, so the mobile intelligent terminal operating system is convenient for developing, on the other hand its integration level is higher, security is good. This feature of deep integration mode makes the function is organized in the form of modules, which is very convenient in the simplification of system functions.

Multitasking capability

Although the mobile intelligent terminal operating system is "castration" version of the computer desktop systems, its performance is no less, it fully inherits the multitasking capability of the computer operating system. Now people have more and more demands for function and performance, multitasking can be said to be the necessary element. When having a multitasking

ability, the user can use multiple functions at the same time, and can be convenient to switch between multiple functions.The most typical applications is a smartphone, with which users can watch e-books and listen to music at the same time.

Mobile intelligent terminal system security problems

Smartphones, tablets and other intelligent terminals has been widely applied in recent years, intelligent terminal applications have bring convenience to people, at the same time, the security of its operating system has attracted more and more widespread attention.

Android system, for example ,is the most common mobile intelligent terminal operating system ,which have the most market shares in numerous intelligent terminal operating system. its security now faces with unprecedented challenges because of its open source characteristics. Android is a open intelligent terminal operating system launched in November 5, 2007 by Google corporation. The Android system uses the hierarchical system architecture, which is divided into four layer structure, including from the upper to the lower, the application layer, application framework layer, system runtime library and the Linux kernel layer, as shown in figure 1 [1].

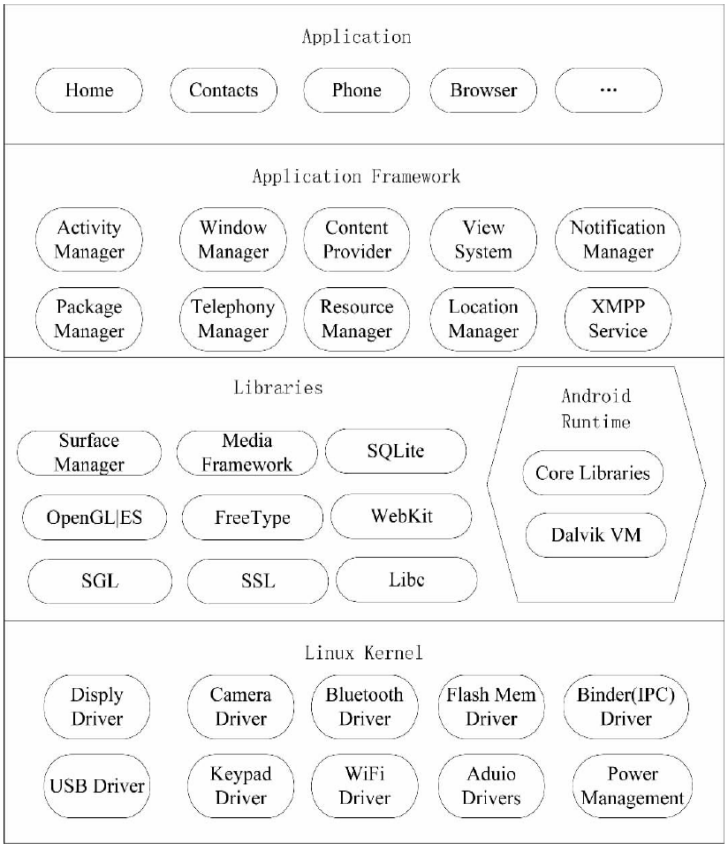

Fig.1 Android hierarchical system architecture

Being a operating system with free open source code, the Android system brings a lot of convenience to people's life, but this characteristic also provids convenience for the malicious software and viruses. Android attract the participation of industry chain by the characteristic of free open source has achieved a huge industrial chain charisma and remarkable market achievement. But recently the industry has more and more doubt with the problems behind this open source mode.

Intelligent terminal open original closed terminal operating system, the interaction between terminals and the Internet is more and more direct, as one of the important link, the security of the terminal operating system is very important. The threats to terminal operating system security mainly include the operating system backdoor, operating system vulnerabilities and abuse of API (application programming interface) [2].

The back door of the operating system refers to method of controlling or getting access to the program or system which is created in the development process .The design of the back door is based on two considerations. First, the back door can make it possible that the developer can enter the system to repair the defects of the system. The other is the deliberation the developer set up on purpose to control the operating system. Most of these backdoor is not known by the user, but it will bring a huge security risks to users when it is misused. There are many kinds of the back doors, the simple one ,for example, can create a new account in system to facilitate hacker to enter the system. the complex one can bypass the system security certification and obtain the authority of reading and writing the system, etc. Android, for example have a remote control software named " kill switch", can invasion system remotely , delete application program and data in the user equipment. In July 2014, the iOS system developer, Jonathan revealed a few back doors, they can steal a large amounts of data from iPhone, such as the user's location information, these hacker program runs while the users cann't be aware of it,nor prohibit it. Edward snow den, the announcer of "prism" , also said that the national security agency can monitor the user through a microphone even if the iPhone users have turn it off[3].

The defects of the operating system is mainly refers to the technical problems or vulnerability existing in the system itself in the design, it could be used by hackers to attack or control the whole system by Trojans or viruses. Through domestic evaluation to more than 4.25 million applications from the various channels, China software test center found that the malicious behavior such as mobile Internet application software malicious deduction, remote control, stealing privacy, malicious spread, consumption expenses, is very common. is very, Eighty percent of mobile malwares have more than two kinds of malicious behavior above.

API abuse is mainly due to the lack of perfect and effective mechanism of authorization and code signature in the use of API. This gives all sorts of malicious code a opportunity to abuse system API to carry out illegal activities. Many applications abuse the foreground service interface (Service. start Foreground () API) to make the application running in the background, can't be killed, and get away with the inform manager (notification manager) of the operating system by making an exception notification object. That is strongly threaten the privacy security of users. And cann't be detected by user. Although the versions after Android 4.3 provides the right to know and disposition of the running application, but only take temporary solution not effect a permanent cure.

The security policy in mainstream mobile intelligent terminal operating system

Google Android

Google Android is open source operating system, relies on the open source Linux kernel. Android protects application data file on Linux operating authorization protection level, only authorizes the user ID access permissions, the system resource is authorized when user installing applications, the authorization will not be repaid.

Application component is designed reusable as the main target, system requirements components having safety consciousness, malicious behaviors across application components is difficult to complete. System mainly includes four components, Activity, Service, Content Provider, and Broadcast receivers, these components have the independent periodic scheduling process, other applications can arouse component to run through use of Intent, Content Provider, or IPC Binder. System requires components must set security perfect to prevent being aroused maliciously[4].

Android operating system is designed with application isolation mode, that is an effective system security mechanism.Using the model application isolation is also a kind of effective system security mechanism, but the use of the model may lead to the prevention of some application functions, such as connecting to the Internet, starting the camera, obtaining location information, etc., that will influence the effect and function of application. So Google corporation make up her mind that the developer should be given sufficient freedom on the premise of operating system security, to prosper

the application market and to promote the Android operating system. After improvement, different applications can share dates and components through sharing user ID, and can run in one process.

Apple's iOS 3.2

The security mechanism in Apple's iOS operating system is completely different with the Android operating system. According to apple's business model, applications based on iOS operating system can only be issued by official apple's app store. Before entering the distribution channels applications are required to be examined by apple's app store, to ensure the safety of application. Applications reviewed by store is considered as safe applications, it can get a lot of important system permissions which are sensitive in the Android operating system, such as Internet access, starting the camera, location information, etc. The app store examine whether the application contains malicious code as well as whether the application uses the system API correctly to ensure the safety of application.

The iOS operating system have an important security measure called the Security Server daemon, it is mainly responsible for safety services such as trusted chain access, root certificate management. Any application must use the key chain, certificate, key, etc, through the Security Server.But this service is not implemented in the form of the API. Here is relatively important Security Server in the iOS operating system:

(1) Keychain Services API, is a system service to realize the storing passwords, keys, certificates and other secret data. It need the cooperation with encrypt/decrypt system service, data storage service and common encryption dynamic library etc.

(2) The CFNetwork, is a system service to realize the creation and maintenance of secure data flow, the service can also increase the authentication letter in the message. It create a secure connection by calling related system security service in background.

(3)The Certificate, Key and Trust Services, can provide services such as creating, managing and reading the certification information, adding authentication information to the key chain, creating the encryption key, encrypting/decrypting data, data signature , signature identification, managing the trust policy, etc. In the process of the realization of the above services, one need to call the public encrypted dynamic link library and other core OS layer service.

(4) Randomization Services, is a service that generates pseudo random numbers for all kinds of encrypting operations in system. Pseudo random number is produced by specific algorithm, the algorithm cannot be derived with the generated random number. To generate pseudo random number, this service needs to call the random number generator in core operating system layer[5].

The tendency of mobile intelligent terminal operating system security mechanism

Intelligent terminal system security is a system engineering, system architecture should be reinforced step by step, including adopting the technology of safety kernel and startupin the kernel layer , preventing illegal authorization and illegal Getroot; adding security access control In general function library.

Due to the diversity of mobile devices, so the smartphone operating system should have a variety of terminal management function, namely the function of data synchronization. It should have the ability of locking mobile phones or destroying data in remote when necessary.

The classification of the intelligent management for the application will no longer be blank in the operating system in the future. Developers will redesign the smartphone operating system, to provide a automatic and intelligent management mode for various types of applications. Based on intelligent classification management, it integrate various types of applications, so that the applications will no longer be dispersed and independent from each other, effectively improve the efficiency of users application.

References

[1] Hall S P ,Anderson E. Operating systems for mobile computing inCollrges,2009,25(2):64-71

[2] Tsai F S, Etoh M,Xie X et al. Introduction to mobile information retrieval. IEEEIntelligent Systems, 2010,25(1):11- 15

[3] Krishnamoorthy S, Agrawala A. Poster: A context aware framework for mobileapplications//Proceedings of the 9th international conference on Mobilesystems, applications, and services(Mobi Sys'11).Bethesda, Maryland,USA,2011:403 404

[4] Varshney U, Vetter K. Mobile commerce: Framework, applications and networking support. Mobile Vetworks and Applications, 2002，7(3):185 -198

[5] Matthias Lange , Steffen L, et al . L4Android: A Generic Operating SystemFramework for Secure Smartphone/ / Proceedings of the 1st ACM workshop onSecurity and privacy in smartphones and mobile devices，Chicago-Illionis，USA，2011: 39-50