Design on Terminal Security Platform for Android System

Chunqiang Li

School of Information Management, Beijing Information Science and Technology University, Beijing, 100101, China

642510571@qq.com

Keywords: Android system; mobile terminal; security platform; system design; key technology

Abstract. Android mobile terminal devices for security and sensitive data leaks and other problems, the design based on the Android mobile terminal security management platform, for the user carry on the security management for mobile terminal equipment and storage of data. Design platform to Android architecture as the foundation, through the analysis of the logical structure of the terminal security platform, designed to terminal security platform key technologies. Security platform is constituted by the safety protection system, safety management software and safety management system; specific key technologies include firewall technology, security policy design and terminal data protection. According to the research result of this paper and development of the Android mobile terminal security platform, to solve the mobile terminal equipment security and data security issues, and has a broad market prospect.

Introduction

With the popularity of Android mobile terminals, the sensitivity of the information stored therein is also rising, the attendant security issues gradually becoming major issues of concern. Bring security threat of Android system for many reasons, specifically, mainly in the following points [1,2]: First, open mode brings vulnerability. Android uses open application distribution model, while allowing users to install applications from application sources other than App Store applications, in other Android applications markets, mandatory safety checks may not have been well implemented; the second is the problem of permission mechanism. In the Android security model, the permissions of the application be declared at the time of its installation, and cannot be changed later. Third, the operating system vulnerabilities caused by the attack. Android system uses a sandbox to isolate the application so that the malicious code only runs in its own sandbox, in order to achieve the purpose of the protection system. But the Android system itself, there is many loopholes, a lot of malicious code to exploit these vulnerabilities to break sandbox, get the system root privileges. Fourth, the application software vulnerabilities caused by attacks. Software vulnerability refers to the problems existing in the design and implementation of the application itself, malicious code developers to exploit these vulnerabilities, attacks installed the application of mobile phone. For users to develop a practical, safe and reliable Android mobile terminal security platform with integrated solutions to help users solve the mobile terminal device security and data security problem, has important practical significance and application prospects.

Android Architecture Analysis

Android is essentially on a standard Linux system to increase the Java virtual machine Dalvik, and built on the Java Application framework in the Dalvik virtual machine, all applications based on the Java-Application framework. Android is divided into four layers, from the top to the lower are the application layer, application framework layer, system runtime layer and Linux core layer, shown in Fig. 1 [3,4].

(1) Application. Applications using the Java language, each application consists of one or more active composition, activities must be based on the Activity class as a super class, the activity is similar to the operating system process, but activity is more flexible than the operating system process, and is similar to the process, the activities switch between multiple states. Using Java's

cross-platform nature, based on applications of Android framework development cannot compile, running on any computer equipped with the Android system platform, which is the essence of Android.

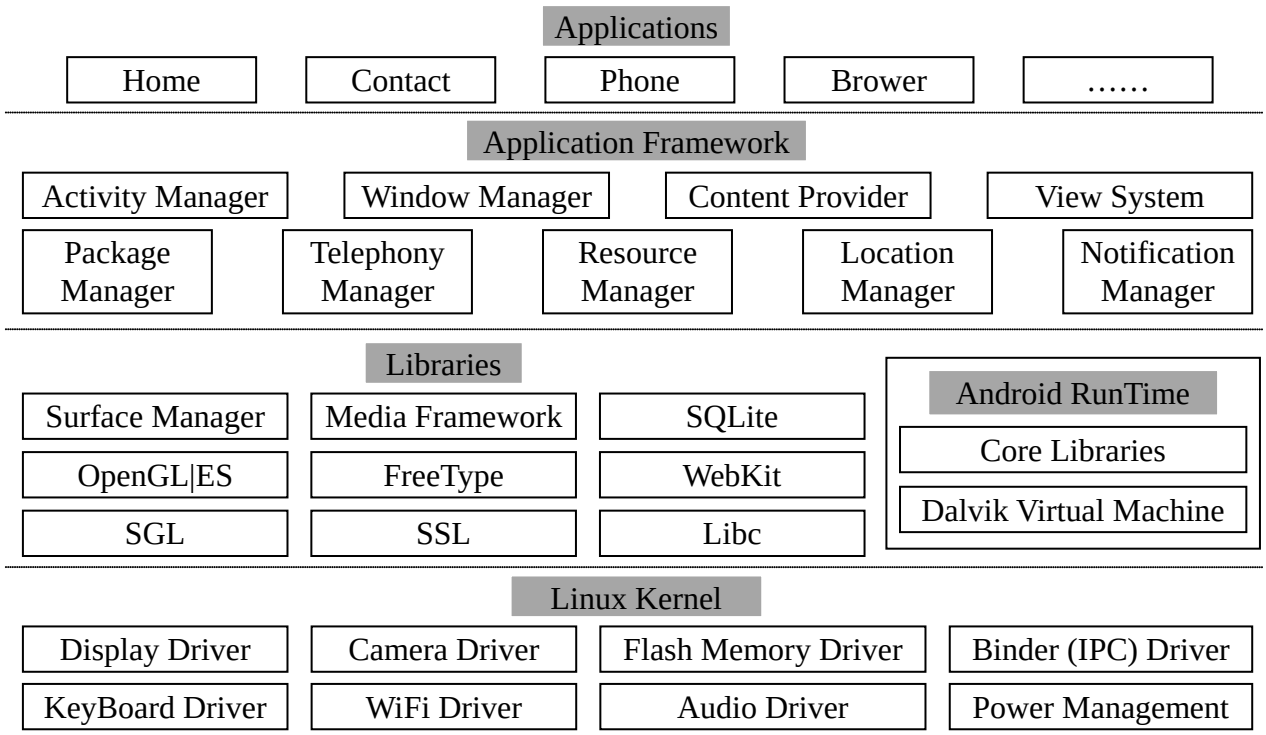

Fig. 1. Android Architecture

(2) Application framework. Android is an open platform, API almost all open to developers. As long as the system application has the function, developers can also provide through the application framework layer provided the API to achieve these functions. For example, the access device hardware information, receives device location information, start the background service and set the alarm clock. Android application architecture to facilitate the reuse of components, any application can release its function modules, other applications in compliance with security restrictions premise can reuse these function modules.

(3) The system runtime layer. It included libraries and Android runtime. Android contains some C/C++ libraries, used by various components in the Android system, to provide services through the Android application framework for developers. Mainly include the basic C library, multimedia library, bitmap and vector fonts, 2D and 3D graphics engines, browsers, database support. Android's various libraries are generally in the form of system middleware provides. Android runtime environment mainly refers to virtual machine technology (Dalvik). Dalvik virtual machine and general Java virtual machine (Java VM) is different, not the implementation of the standard Java byte code (bytecode), but Dalvik executable format (.dex) in the executable file. In the implementation process, each application that is a process (a Linux-Process).

(4) Linux kernel layer. The previous Android relies on Linux2.6 kernel, the latest Android4.0 series relies on the latest Linux 3.x kernel. Series of the Linux kernel provides Android system the basic network protocol stack, driving model, security, memory management, process management function. At the same time, the kernel also can be used as a hardware abstracted interface for software calls.

Logical Structure of Terminal Security Platform

Terminal security platform is constituted by the terminal security protection system, terminal security management system and terminal security management system, logic structure as shown in Fig. 2.

Terminal security management system, based on data provided by the terminal security platform, providing secure management personnel (system administrators, security managers) require management, monitoring, risk analysis, production of various types of management reports, while meeting the provincial, city, county in distributed environment industry safety management requirements. It is to build a complete technical support platform of terminal within the network security management system.

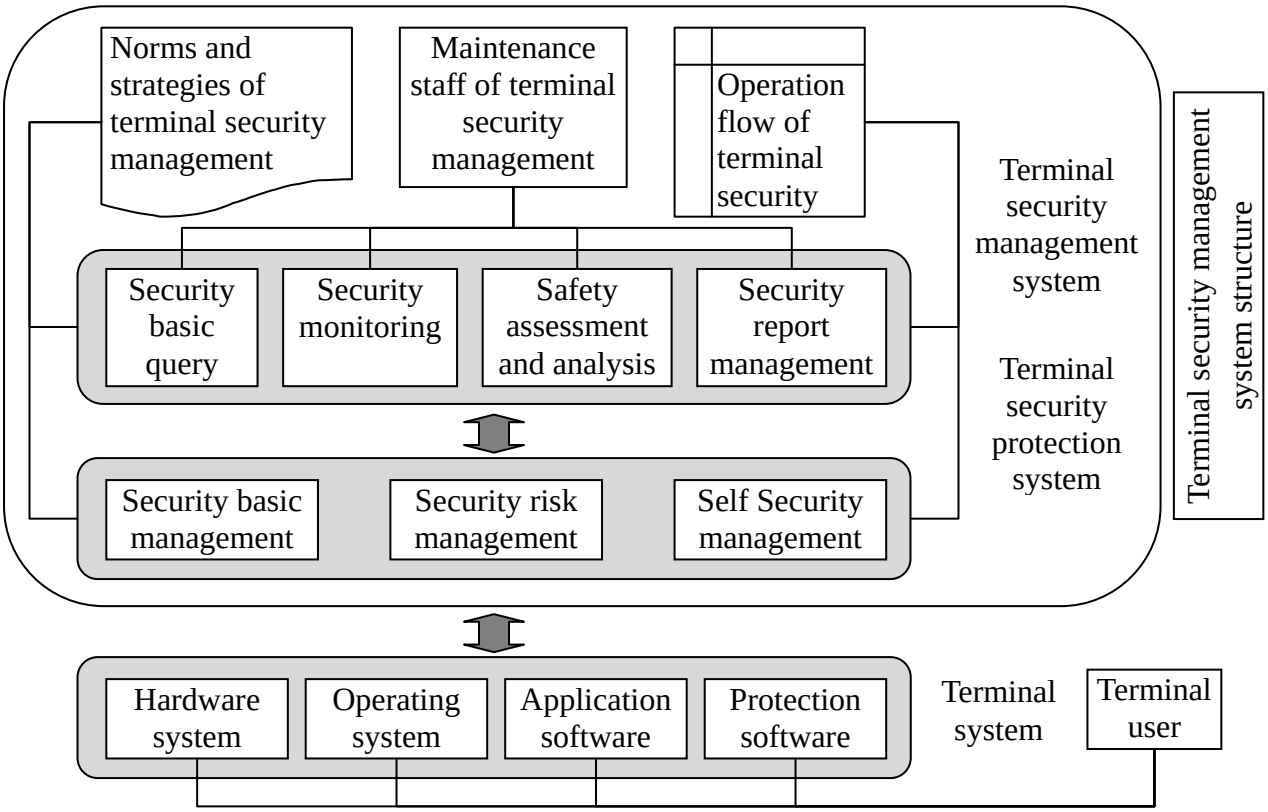

Fig. 2. Logical structure of terminal security platform

Terminal security protection system, responsible for the collection and maintenance of terminals information, terminal security risk management and protection, monitoring and control of terminal security event, providing acquisition and transmission of various types of data required for the management platform. Implement various types of security incidents, "advance prevention, a matter of defense, post-processing," the three-dimensional, process-oriented defense. It is the basis to build a comprehensive, integrated within the network terminal security system [5,6].

Terminal security management system is constituted by the terminal security organization system, terminal security operation system, terminal security policy system and terminal security technology system. Wherein the terminal security technology system mainly is consists of terminal security protection systems and terminal security management system.

Android system end-user to achieve security operation through terminal system, the system consists of four parts, namely, hardware systems, operating systems, application software and protection software.

Key Technologies of Terminal Security Platform

Android system terminal security platform technology has a lot, this article only study the following three key technologies:

(1) Firewall technology

Firewall is an important tool to ensure the network information security, is a kind of information security protection system, in accordance with the specific rules, allow or limit data transmission through. Firewall is located between the internal network and the external network, establishing specialized network protective barrier between the public network and a private network, in the network between a security gateways, protect internal network or special network not incursions by external lawbreaker. Firewall is mainly composed of filtering data packet, virtual gateway service, functional verification and rules four parts, the main functions include monitoring of network flow, prevent internal data leakage and enhance network security.

Android terminal firewalls to achieve relying on Linux powerful firewall tool Netfilter/Iptables. Netfilter exists in Linux kernel space, the provisions of the network data packets in the kernel space is filtered or release some set of rules; Iptables exist in user space, to configure specific policies for filtering rules. Netfilter is a common framework of Linux kernel, the definition of the five key points, and provides the corresponding hook functions, and in the entrance of the hook function can intercept data packets and the corresponding processing. kernel if it detects a hook function in the corresponding entry point were registered, the data packets through this entry point will be processed after the data into the hook function that will be processed in accordance with the rules, including blocking, release and prohibit such acts. The working principle is shown in Fig. 3.

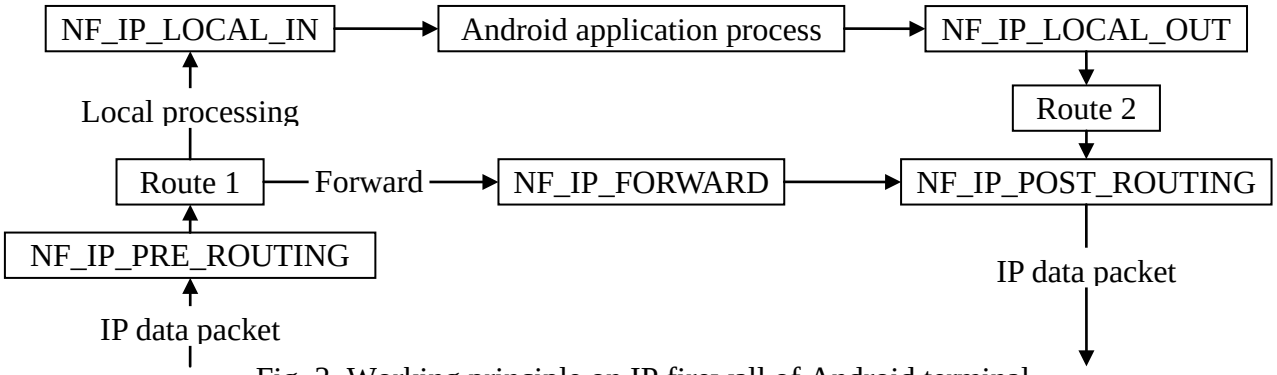

Fig. 3. Working principle on IP firewall of Android terminal

(2) Security policy design

Users can set up mobile terminal remote security management strategy via safety service platform, such as remote encryption policy, remote locking strategy, remote positioning strategy, SIM protection policies, boot self startup strategy, flow monitoring strategies. Policy file is AML format, users through the safety service platform set in advance mobile terminal security strategy, and then pushed from the server to the client in order to achieve guide of perform operations on the client. Users can customize the mobile terminal whether to accept remote lock, remote location, remote lifting, remote encryption instruction, whether to open the SIM card protection and boot from the start, and the ability to define flow monitoring strategies of the mobile terminal, implementation flow exceeds the warning function, timed reminder flow usage function. The organizational forms of security policy files are as follows [7]:

```
<policies>
    <lock>Y</lock>                  // Whether the remote lock
    <locate>Y</locate>              // Whether the remote location
    <en_decrypt>Y</en_decrypt>      // Whether the remote encryption and decryption
    <sim_protect>Y</sim_protect>    // Whether to open the SIM card door
    <self_start>Y</self_start>      // Whether to open the boot from the start
    <network_flow>                  //Network traffic warning
        <max>100M</max>             // The maximum flow rate is 100M
        <times>24h</times>          // Every 24 hours to remind traffic usage
    </network_flow>
</policies>
```

(3) Terminal data protection

After the user terminal is lost, users are faced with terminal data (including SD card data) loss and leakage risk. Get terminal users can use disableKeyguard method of KeyguardLock, with boot from the start to bypass the native system lock screen, also can directly use the card reader to obtain data on the SD card. In addition, the application data on the terminal may have been snooping. The existing security products in the user terminal is lost can only provide lock screen, positioning and alarm functions, cannot protect the files on the SD card. These security features are mostly remote control via SMS. For some there is no SMS mobile terminals, such as tablet computers, you cannot use the remote control function [8,9].

Lock screen function to prevent people who receive terminal, bypassing the native lock screen functionality for the user to operate the terminal. The SD card file encryption function can be achieved on important files and folder encryption, even using the card reader cannot from the SD card access important information. Application lock function prevents others from using certain important applications in the terminal without permission. In addition, the system does not use SMS for remote control of the terminal, but through the long connected to realize the remote control of the terminal, as long as the terminal is connected to the Internet, can through the clouds carry on the remote control for terminal. Through long connection, the current status of cloud terminal was collected, including contacts, text messages, e-mail and so on. Cloud also is able to collect real-time location information of the client, and call some site map API show the customer's current location and moving track for device recovery provides the possibility. When the user's terminal has very important information, in order to prevent information leakage, through the clouds to the terminal data is erased. In addition, the system also provides the user terminal data backup function, and can replace the equipment after use data restore function to restore important data onto new mobile devices.

Conclusion

With the rapid development of mobile Internet, mobile terminal security problem has become increasingly prominent. Because of the openness characteristics of the Android system, determine it will become the main target of the various attacks. From the current security status of view, security threats continue to increase, all kinds of terminal-based security products cannot perfect guarantee Android mobile terminal security. According to the research result of this paper and development of the Android mobile terminal security platform, to solve the mobile terminal device security and data security issues, has a broad market prospect.

Acknowledgement

This work is supported by Major special project of nuclear high-base (2012ZX01039-004-48); School fund of Beijing information science and technology university (0925020).

References

[1] Junho Choi, Woon Sung, Chang Choi, Pankoo Kim, "Personal information leakage detection method using the inference-based access control model on the Android platform," Pervasive and Mobile Computing, vol. 24, no. 12, pp. 138-149, 2015.

[2] Digital enterprise network, "Security analysis of mobile terminal operating system Android," http://articles.e-works.net.cn/security/article115828.htm, 2015-12-30.

[3] Hui Zhao, Min Chen, Meikang Qiu, et al, "A novel pre-cache schema for high performance Android system," Future Generation Computer Systems, vol. 56, no. 3, pp. 766-772, 2016.

[4] Cynthia&Sky, "The basic structure of Android," http://www.cnblogs.com/lijunamneg/archive/2013/01/18/2866953.html, 2015-12-30.

[5] J. Wu, J. Wang, "Android Terminal Common Security Issues and Workarounds Analysis," The Journal of New Industrialization, vol. 5, no. 5, pp. 55-61, 2015.

[6] H. Qian, "The Design and Implementation of Mobile Terminal Security Management System based on Android," Master's degree of Beijing University of Posts and Telecommunications, 2012.

[7] J. Y. Fu, Z. F. Ma, Q. L. Huang, et al, "Mobile Terminal Security Management System Based on Android," Computer Engineering, vol. 40, no. 11, pp. 77-82, 2014.

[8] H. Qian, "Research and Implementation of a Cloud- mobile Based Security System for Android Devices," Master's degree of Beijing University of Posts and Telecommunications, 2012.

[9] Xu Jiang, Lili Liu, Simeng Yu et al, "Research on a monitoring terminal for a fibre grating sensing device based on Android," Pacific Science Review, vol. 16, no. 6, pp. 23-28, 2014.