Android system security vulnerability and response measures

Yingbo Li, Xiao Lu, Jing Fang*

National Computer Network Emergency Response Technical Team/Coordination Center of China

Beijing, China

fj@cert.org.cn

Keywords：Android system; security threat; Coping measures; Vulnerability Introduction

Abstract. Android is a smart mobile operating system with a huge market share, its security has received widespread attention by researchers and customers. The system architecture of Android is introduced, the security mechanism of Android is analyzed, the platform classification and characteristics are summed up, as well as the security aspects in developing and using and corresponding evasion method is presented.

1. Introduction

In recent years, with amazing development and the continued increase in market share, Android platform has become one of the operating systems giants in the field of Intelligent Terminal field. At the same time of providing convenience, a growing security challenges and threats is experienced. Related data show that the number of android operating system users, mobile phone manufacturers equipped with Android operating system and applications on the Android platform have been quite large. Although the current Android system has a relatively good security full mechanism to ensure the safety, under the huge commercial profits, a large number of attackers find various ways to attack users. With the accelerated popularity of Android platform applications, related security threats also began to show. Due to the strong Great features and rich applications of Android intelligent operating system, Android intelligent terminal is playing an increasingly important role in household use. As a large number of important information stored in Android intelligent terminal, so it has become the preferred target of malicious attacks. Behaviors like privacy information disclosure, malicious deduction and system damage bring huge losses to users, so it is urgent to solve the security problem of Android.

2. Architecture of Android

After several years of Microsoft Corp monopolizing the computer operating system, the appearance of Android system finally makes people experienced open source operating system popularize in users not have computers. Android system is an open source software stack for mobile devices based on Linux, the idea of layered is adopted in Android system architecture, from the low level to the top respectively is the Linux kernel layer, the system run library layer, application architecture layer and application layer. Layers work together with distinct level and clear architecture.

2.1 Kernel layer

This is the bottom of the Android platform, which provides a device driver dynamic and core system services. It principally composed by Linux kernel (Linux Kernel) and Android extended kernel (extension Kernel). The main development language of Android platform is C. As an abstraction layer between the hardware and software, this layer provides lots of core services for the upper operating system. The main modules include security management, memory management, process management, network stack, and various drivers, etc..

2.2 System runtime layer

This layer contains some C/C + + local library and runtime environment, some core features of local library provides can be used by different components in Android system, they provide services by Android application architecture, Android runtime environment includes Java library and Dalvik virtual machine.

2.3 Application framework layer

This layer is designed for developers, including various components that used for applications, and the component can be reused, it is implemented by Java language through calling the lower service functions. By providing core framework APIs, developers can make various applications. Under the premise of framework security constraints, whatever application can call these core functions API to publish their own functional components.

2.4 Application layer

The layer is located on the top of the platform, which is the Assembled layer of Android platform software, all of Android software are located on this layer, the application of Android includes (home) E-mail, SMS/MMS, calendar, maps, browse, contact management, etc.. These applications are typically written with Java Language by calling by calling API that the application framework layer provided; it allows interaction between Java code and other code (usually C and C++, the formation of the code called the local code).

3. Analysis on the security mechanism of Android system

Android is development based on Linux, so it inherited the security mechanism of Linux system, such as the independent access control in Linux mechanism. At the same time, Google also added a special right to protect Android system. In addition, according to the characteristics of more privacy data, limited computing power, three important security mechanisms are set up like the sandbox operation, signature and authentication application.

3.1 Run of sandbox

Also is Application isolation mechanism. A sandbox is provided when running, which can run independent in a process. Different signatures of the application will be assigned different user identity at the time of installation, and run in different system processes, any data stored in the application will be granted to user ID, which cannot be accessed by other applications, Communication between the programs through the binder mechanism, which cannot directly access memory space, user ID can protect accessible folder, data and memory. This mechanism ensures the application isolation, once a problem shows when application is running; it can eliminate the virtual machine instance to ensure the whole safe operation. If containing malicious behavior, the further operation is prohibited, so it will not cause any harm to the system.

3.2 Authority audit

In order to inform the key functions use to users, Android defines and achieves the rights mechanisms, namely an access control framework based on capability. The corresponding API interface must be used when application access the system resources, each type of API is homologous to the corresponding permissions. One authority mainly contains 3 aspects: authority name, authority group and protection level. A permission group is a different set of permissions that are divided according to their functions. An application can apply for corresponding rights according to the system resources or other application components, when the application is installed, the system installation program will allow users to check the permissions, so as to determine whether to accept or reject the application of the installation.

3.3 Signature mechanism

All Android applications require developers to use a certificate to complete digit signature, required to be packaged into. APK file, this file must be signature when packed, which is different from digital certificates in information security domain. The purpose of signature is to check whether the test file is modified and protect the file. Also, it use signature to identify the application

of the author and establish trust relationships. This digital certificate is controlled and used by the developer, which is used to carry out the application of the package of self-certification, which does not require the authority figures and certificate signature.

4. Security threats of Android system

4.1 Analyze of security threats of Android system

Android system generates a variety of vulnerabilities. On the one hand, because of Linux kernel, many Linux security vulnerabilities are inherited in the Android system, such as root vulnerability. Java language is used in Android application; however, it also has conventional vulnerability like cross site scripting, SQLite database injection, buffer overflow and local rights. On the other hand, due to its own characteristics, Android platform has some of its unique Vulnerability type.

First is the authority control vulnerabilities. In order to notify the key function situation to users, Android defines and achieves the right mechanism. However, in fact, with increase of functions and possible developer's negligence, some sensitive components does not set permissions, which will cause intended attack leapfrog permission through access some components.

Second is WebView vulnerability. With the development of mobile Internet, a lot of Web interactive services are provided based on Web interaction. Android platform provides a rich class and interface to access the Web page, WebView is commonly used for web browsing and user interaction, it is the class of WebKit module Java layer as UI interface, and it provides operations like interface interaction, web browsing and other operations. Once WebView have the security vulnerabilities, the loss may be unable to estimate.

Third is components exposed vulnerabilities. Android applications are composed by some fragmented and connected components and bind by a project. The Android platform defines 6 different components; various property rights can be configured in Android Manifest.xml, and can set whether visible. Thus, this means these components can receive applications from third parties, if enough security audit does not get, it is quite possible that he component are exposed to the outside and called by attackers or malicious data injection, affecting the normal operation of the application.

4.2 Characteristics of Android system security vulnerability

General malicious behavior can be divided into privacy theft, tariff loss, system damage, etc., but it will cause huge loss if use Android vulnerability, and even cause security event. The cause of such a large security threat can be attributed to 3 aspects:

One is great harm. Ordinary malicious applications can cause a certain type of security issues by constructing code such as privacy leaks. However, the purpose of using security vulnerabilities attack is to control user terminal, once a malicious event occurs, it is often accompanied by some damages like private leakage, cost loss, system damage. And even if the user found malicious behavior, it is also difficult to prohibit and prevent. Such as the use of root to access to the terminal illegally once hackers get the root permissions, you can control the terminal.

Second is concealed. The use of security vulnerabilities is generally not well-known, therefore, it may use characteristics of hidden malicious attacks. Making use of the vulnerability of the application would not apply for any permissions, security software is therefore unable to intercept, so during the period of installing to utilization, user are not aware of their own intelligent terminal has been charged.

Third is the large scope of the impact. Android platform vulnerabilities are patched slowly, the operating system is difficult to repair on the first time, but the application amount of Android operating system is large, thus, there are vulnerabilities in Multi terminals for a long period. Hackers can embed malicious code through a simple text message, resulting in thousands of users have been attacked.

5. Response to security threats

The research on Android system security has been aroused much attention, both system level and application level have better achievement, but this does not mean that the security of Android system is studied already completely.

Currently, there are two kinds of harm as for portable Android intelligent device, one is due to many vulnerabilities in Android operating system kernel, it is quite easy to cause damage to operating system and applications, resulting in rogue software occupy resources, phone system collapse, etc.. Another is due to lack of powerful firewall and virus protection mechanism, it can easily lead to damaged data file, finally is in the absence of effective supervision and auditing, which cannot distinguish the danger source, resulting in platform software mixed together, malicious code is popular. Therefore, Security protection technology and design is also a topic of information security.

5.1 Protection of operating systems and procedures

It provides basic kernel protection mechanism. But these protective mechanisms are difficult to deal with in a variety of possible human invasion behavior. Based on such situation, Android developer aims to improve the operating system mechanism, strengthen the security of the system. By establishing the mechanism of black and white list of users, the known virus and malicious code added in black list, the white list will be run on this terminal. Installation of mobile phone security on the intelligent terminals, which is similar to the mature products like firewall, so monitoring the invasion of mobile phones and malicious behavior on real-time can play a role.

5.2 Protection against personal data information

Users should develop a good habit of using intelligent terminals, not download software arbitrarily, particularly some advertising box pop up on the interface, which must be choose whether download or install after identified; it is not accessible in public place that is wireless network of no password and no verification code; do not make operation of money and privacy under the distrust wireless network; download the official website application software in the formal application store; try to download application software in formal store; do not submit personnel information in unfamiliar software. At present, there are companies developed the data Anti leak products, it is similar of using terminals and computers, first need identity authentication, it is only by this that can access the terminals, the authentication mode will be adopted in the network access, These protect techniques will establish a protective umbrella for using intelligent terminals.

5.3 Strengthening protection of system platform

From the point of view of vulnerabilities mining, the related research of vulnerability has strong limitations, mainly focused on security related API error and component exposed vulnerabilities. Establishing and perfecting Security vulnerability database system construction will find a new way for Android security research.

All kinds of protection products on the market are emerging endlessly; a unified security detection standard, effective supervision and security rating system will be conducive to the timeliness and accuracy realization of Android.

6. Conclusion

Android system rises suddenly with a new force, in just a few years, Android system has become the deserved king of mobile platform domain, in the future, with this open operating system and the wide range of application, its technical design and development will meet with more personalized needs, which will give security researchers with great opportunities and challenges. Android vulnerability is analyzed in this paper, Android platform vulnerabilities cannot be completely avoided, this will be an important subject in the field of information security needs to be further studied.

References

[1] Wei Sun. Security analysis of Android mobile terminal operating system[J]. Vol34(4), 105-108,2013.

[2] AppBrian Stats. Number of available Android applications [EB/OL].[2014-01-08]. http://www.appbrain. com/stats/

[3] Jian Liu, Kexin Sun, Sunlv Wang, Android system code vulnerability analysis based on control flow mining[J]. Journal of Tsinghua University(Natural Science Edition), Vol52(10):1335~1339,2012.

[4] Bugiel S, Davi L,Dmitrienko A.et al.Practical and lightweight domain isolation on android[C]//Proc of the 1st ACM Workshop onSecurity and Privacy in Smartphones and Mobile Devices. New York: ACM. 2011. 51-62.

[5] Zhenfei Tong, Research on the static detection scheme of Android malicious software[D]. Nanjing University of Posts and Telecommunications,2012.

[6] Shaolin Jiang, Jinshuang Wang, Tao Zhang, Review of Android security research[J].Software and Computer Application.Vol29(10)205~210,2012.

[7] Lange M, Liebergeld S, Lackorzynski A, et al.L4Android: a generic operating system

[8] framework for secure smartphones [C]//Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011: 39~50

[9] Lisheng Wang, Xizhe Ye, Research and Implementation of Based on Android firewall[J]. Computer Security, 2009(20)36－38.

[10] Jing Tian, Analysis and application of Android security mechanism, Mechanical Industry Press,2013,5.

[11] Bin Li, Design and implementation of of behavior analysis of Android system software based on sandbox[D]. Beijing University of Posts and Telecommunications,2013.

[12] Fengsheng Yang, The inside story of Android,1th edition,Jun,2011.