Risk Analysis and Safety Protection of Android Phone

Haiyan Wang, Yanqing Deng, Ping Zhang
Jiangxi Industry Polytechnic College

Keywords: Android; Safety mechanism; Privacy protection

Abstract. With the all-round development of science and technology, the Android phones represented by Android begin to become an important part in people's lives gradually. People perform voice calls, sending and receiving mail, processing all kinds of information, enjoying the convenience through the Android mobile phones, but at the same time the user's personal privacy is facing with great threat. At present, Android system has become the most malicious software platform for the Android mobile phone operating system, and theft of individual privacy has become the main means of attack of malicious software. So, it has become the focus of Android security research and discussion about how to guarantee the users' privacy information in the Android mobile platform security. Android framework, application components are introduced firstly in this paper, and Android system and the risks of personal privacy information under the current mobile phone protective mechanism are analyzed in detail. Finally, in order to solve the security problems that faced by personal privacy, a kind of double users privacy protection system model is designed.

Introduction

As the rapid development of industrial science and technology, mobile operating system and mobile data communications technology, the hardware cost is continuously reduced, the intelligent mobile operating system and mobile data communication rate are also continuously improved, we are moving towards the Internet era marked by Android mobile. People can not only enjoy the traditional voice service, also can be convenient to complete the activities of browsing the web, mail processing, games, social networking and others through Android mobile phone. Android operating system is well ahead of other operating systems in Android mobile phone operating systems, playing a most important role. People can acquire applications through the official Google market and a large number of third-party Android markets. These applications can make people deal with their emails, information, images, social networking, etc. more conveniently, while Android mobile phone also stores people's text information, contacts, phone records, E-mail, etc. This information all belongs to the user's privacy information, and should be protected sufficiently. However, the personal data privacy is facing a huge security threats.

Therefore, it is the research focus of mobile phone manufacturers and scientific research institutions for enhancing the privacy security of Android system, and the research to enhance the security of Android system is also included in this paper.

Loopholes Existed in Android Mobile Phone Operating System

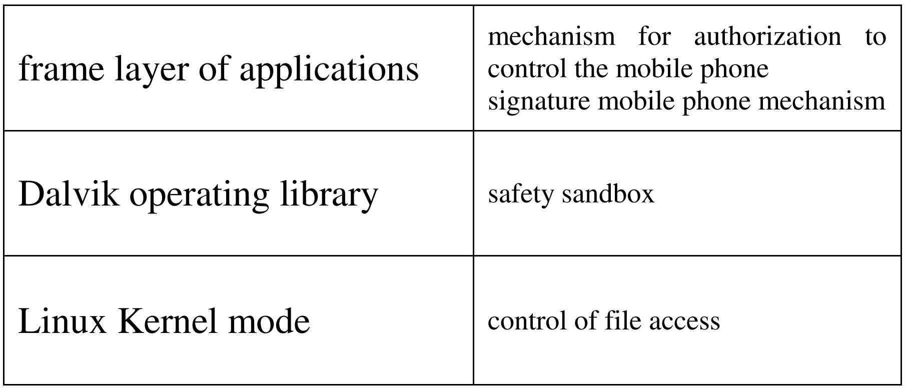
Android mobile operating system has the characteristics of openness, and it brings the security problems while facilitating the users. The system platform becomes the attacked targets of a large number of hackers. Against the vulnerabilities that exist in the Android mobile phone operating system, hackers develop a large number of tools that can enter into Android mobile phone, leading to the protection system shut down. These tools mainly use the malicious software that steals user's private information and commercial secrets, performs malicious deduction of user's mobile phone fee, and includes Trojan as the main tool. This kind of virus can connect with network automatically. They will be activated when the mobile phones are turned on of or the software starts to work, so as to make a series of destruction, and will harm the information stored in the phone after system boot, stealing a lot of information, to cause great economic losses to the user.

Android Mobile Phone System Lacks of Strict Supervision System for Software Installation. Due to its own insufficient basis, to a certain extent, Android phones increase and expand the safety problems, leading to its own imperfect validation mechanism and the foundation is weak. Only the integrity of software and quickness of installation can be ensured in the process of installation and download process, but the safety performance of mobile phone software can't be guaranteed. There are a lot of different third-party mobile download stores, leading to the safety performance being greatly reduced. And the regulatory is relatively weak and even the existence of bad commercial piracy cloning, increasing the risk of mobile security.

The Diversity of Wireless Access Modes Results in a Mass Invasion of Virus. Android phones have a large number of different ways to access to the network, resulting in a great discrepancy in access permissions. A lot of wireless local area network (LAN) does not need to undertake effective verification that can easily access, increasing security issues. There is a big risk of dotted lines local area network (LAN) for the access mode of wireless network. Most of Android mobile phone users are used to use security software to manage mobile phone, providing convenience for the user while bringing harm too. In the openness of wireless local area network environment, the attacker in the same network can effectively steal personal information, chart data of mobile phone users, bringing great harm to the user.

Android Security Mobile Phone Mechanism

Android system is an operating system implemented based on Linux Kernel, and Dalvik virtual phone operating layer, frame layer of applications are realized based on the condition above. The security mobile phone mechanism of Android has multi-layer security design against this kind of hierarchical design, as shown in Fig.1.



frame layer of applications	mechanism for authorization to control the mobile phone signature mobile phone mechanism
Dalvik operating library	safety sandbox
Linux Kernel mode	control of file access

Figure 1. Structure chart of safety mobile phone mechanism

In the Android kernel layer, the most basic Linux security mechanism is provided, including file access control, memory management, file access control mechanism. In Dalvik virtual phone operating layer, the security sandbox is provided. Let each application run in different sandbox, and ensure that the application and other applications does not affect each other at running time, to ensure the safety of their own resources and data. In the application framework layer, Android performs signature authentication mechanism for application APK package, to ensure the integrity and primitivism of their program. Access control mechanism limits the access for sensitive data, resources and system interface, and it is one of the most important Android security mechanisms.

Discretionary Access Control

Android operating system kernel uses Linux kernel for optimization, and its discretionary access control mechanism inherits from Linux system access control mechanism, containing the user and the file access control two basic elements.

User. Android user concept is based on Linux user name Uid, Gid group name, distinguished with the application for the user. When Android system installs an application, it will assign a unique Linux user ID, or UID for this application. For ordinary Android applications, the UID starts from 10000 and will be distributed by the Android system together, at the same time, Android will reserve the UID below 10000 for the system. For ordinary application, Android system assigns a GID that is equal to UID, so that each application has different GID, and both the kernel layer and application layer can distinguish each application by ID.

File Access Control. Android file access control is the same with Linux. Each file is relative to the user ID, user group ID and read/write/execution (RWX) ternary group permission. The file permission is given in the Linux kernel layer. Each application as a Linux user distinguishes with their corresponding files, and Android system files are owned by the system or the root user. Thus, it can guarantee the security of system files, and also ensure the data security of each application.

The Implementation of Android Private Information Control

Privacy information control module implements the protection of privacy information in the transfer process, including privacy information dye marker, communication audit between components and SD card storage three functional modules. For dye marker of privacy information data, it's realized through the transplant of existing open source project TaintDroid 4.1, providing privacy information judgment basis for inter-component communication audit and SD card storage audit.

Inter-Components Communication Audit. When the four basic components communicate, it will use the data carried by Intent. In order to prevent leakage of privacy information in the communication between components, the inter-components communication audit should be strengthened. Authority approval should be done before four basic components communication.

The communication way of Activity component carrying data is mainly to start another Activity. After the process to start adding privacy authority audit methods, the starting process is shown in Fig. 2.

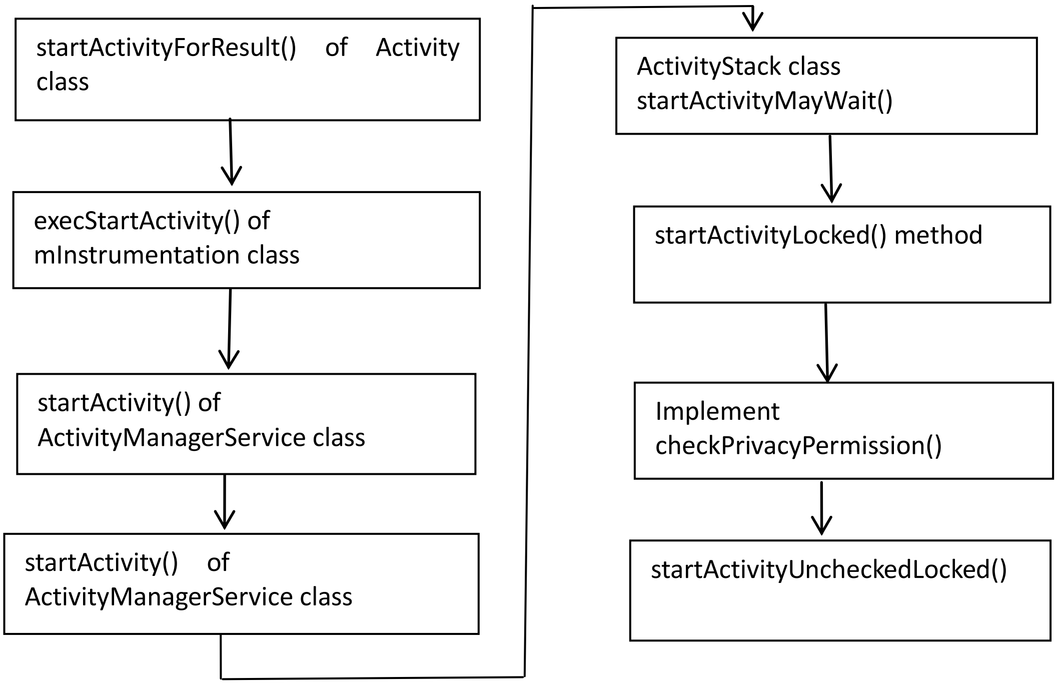

startActivityForResult() of Activity class
execStartActivity() of mInstrumentation class
startActivity() of ActivityManagerService class
startActivity() of ActivityManagerService class
ActivityStack class startActivityMayWait()
startActivityLocked() method
Implement checkPrivacyPermission()
startActivityUncheckedLocked()

Figure 2. Flow of starting Activity

When starting an Activity, whether using StartActivity () or StartActivityForResult (), eventually StartActivityForResult () in Activity class will be called. The methos is to call execStartActivity() of mInstrumentation class in startActivityForResult() method. MInstrumentation class is responsible for monitoring the interbehavior of applications and system, calling ActivityManagerNative.getDefault() in execStartActivity() method to get ActivityManagerProxy port, then calling the startActivity() method in ActivityManagerProxy port class. startActivity() method of ActivityManagerService class is started through Binder drive program. startActivityMayWait() of ActivityStack is called. This method performs Intent analysis and generating target project by calling startActivityLocked() method.

After the completion of analysis, add implementation method checkPrivacyPermission (). This method is used to judge if the transitive Intent contains private data, if yes, a target object is determined whether can access the privacy information.

Conclusion

With the all-round development of science and technology, smartphones represented by Android begin to become an important part in people's lives gradually. They bring the security problems while facilitating the users. Currently, Android smartphone system becomes a platform with the most malware. Theft of individual privacy has become the main means of attack. So, it has become the focus of Android security research and discussion for how to guarantee the users' privacy information in the Android platform.

In this paper, the protection and deficiency of user privacy information in Android system is analyzed. The framework of Android system is introduced and the transition of privacy information between application components is described. Then Android multi-level security phone mechanism is analyzed in detail, and the deficiency of current safety phone mechanism is discussed too. Focusing on the deficiency of current phone security mechanisms, combining with the existing Android security phone mechanism improvement, a privacy protection system model under double user mode is designed.

References

[1] Savola R M, Vaisanen T, Evesti A, et al. Toward risk-driven security measurement for Android smartphone platforms[C]// Information Security for South Africa. IEEE, 2013:1-8.

[2] Robson Y, Blackford S, Roberts D. 'MelApp' and the 'iPhone': smartphone application technology in the risk analysis of a pigmented skin lesion being a malignant melanoma[C]// Meeting of the British-Association-Of-Dermatologists. 2012:93-93.

[3] Savola R M, Väisänen T, Evesti A, et al. Toward risk-driven security measurement for Android smartphone platforms[J]. 2013:1-8.

[4] Moon J H. Smartphone use is a risk factor for pediatric dry eye disease according to region and age: a case control study[J]. Bmc Ophthalmology, 2016, 16(1):188.

[5] Guimarães, V, Ribeiro D, Rosado, L, et al. A smartphone-based fall risk assessment tool: Testing Ankle Flexibility, Gait and Voluntary Stepping[C]// IEEE International Symposium on Medical Measurements and Applications. IEEE, 2014:1-6.

[6] Shao Z P, Lu S D, Chen M. Risk Analysis of Smart Terminals in Mobile Application of Power System and the Protection Solution Design[J]. Applied Mechanics & Materials, 2012, 260-261:397-401.

[7] Busuttil T B, Warren M J. CIIP-RAM- A Security Risk Analysis Methodology for Critical Information Infrastructure Protection[M]// Information Security Management, Education and Privacy. Springer US, 2011:33-49.

[8] Aabo Y, Guin R, Lundqvist B. Risk analysis-a new aspect on protection and local control design[C]// Developments in Power System Protection, 2001, Seventh International Conference on. IEEE Xplore, 2001:347-350.

[9] Si-Wei L I, Zhong S U, Lai J R. Security Risk Analysis and Protection Policy for Information Networks [J]. Computer Security, 2010.

[10] Kwok L F, Longley D. Security Modelling for Risk Analysis[C]// Proc. International Information Security Conference, SEC 2004, 22-27 August. OAI, 2004:29-45.

[11] Neto R M S, Lucrédio D, Bossonaro A A, et al. Component-Based Software Development Environment (CBDE).[C]// Information Security for South Africa (ISSA), 2014. IEEE, 2004:338-343.

[12] Fortat F, Laurent M, Simatic M. Games based on active NFC objects: Model and security requirements[C]// International Workshop on Network and Systems Support for Games. IEEE, 2015:1-3.