Research on Situation and Key Issues of Smart Mobile Terminal Security

Hao-hao Song, Jun-bing Zhang, Lei Lu and Jian Gu

Abstract As information technology continues to develop, smart mobile terminal has become the electronic equipment most closely with people life and work. Meanwhile, the security threats are also increasing to smart mobile terminal when it conducts the business application. Based on the analysis security situation on smart mobile terminals, the key security issues of smart mobile terminals are analyzed detailed: program security analysis, data security protection and defect research. Finally, we point out the development direction on research of smart mobile terminals.

Keywords Dynamic analysis · Data security protection · Defect research · Smart mobile terminal · Security situation

1 Introduction

Currently, the ordinary mobile phones on the market can be classified as the ordinary mobile terminals, and the smart mobile phones are classified as the smart mobile terminals. The smart mobile terminals refers to the mobile terminals having the operating system platform with open (the flexible development, installation and

Research presented in this paper is sponsored by National Science and Technology Significant Project "Security Evaluation Technology Research on Smart Mobile Terminals" (No. 2012ZX03002011) and 2013 Annual Technical Standards Special Project of Science and Technology Commission of Shanghai Municipality "Research on key technical standards of testing on Information security product" (No. 13DZ0500501).

H. Song (✉) · J. Gu
The MPS Quality Supervision and Testing Center of Security Products for Computer Information System, The Third Research Institute of Ministry of Public Security, Shanghai, China
e-mail: haohaosong@gmail.com

J. Zhang · L. Lu
Network Security Protection Bureau of Ministry of Public Security, Beijing, China

E. Qi (ed.), *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation*,
DOI 10.2991/978-94-6239-145-1_2

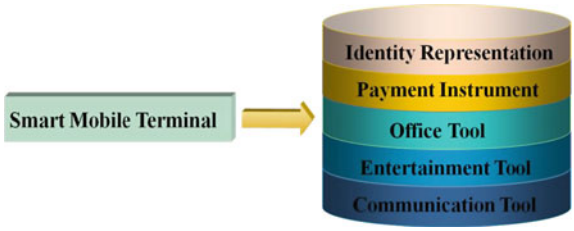

Fig. 1 Development trend of smart mobile terminals

operation in application programs), the PC-class processing power, the high-speed access capabilities and the rich interactive interface, including the smart mobile phones and the tablet computers. The mainstream operating system platforms include two categories—Android and iOS on the market.

With the development of encryption chip, secure communication protocols, authentication technologies, the future development trend of smart mobile terminals is the smart mobile terminal not only is as a communication tool, entertainment tool and office tool, but also is as a representative of payment instruments and identity. Using it, you can carry out the small amounts of payment or credit card shopping. The smart mobile terminal can also be the access card and the membership card. Figure 1 shows the development trend of smart mobile terminals.

2 Security Situation on Smart Mobile Terminals

With the development of 3G network and other wireless, smart mobile terminal is not just communications equipment that used to call and send SMS, the users that access the Internet through smart mobile terminals increase significantly [1]. Smart mobile terminal has become to the key strength to promote mobile internet business quickly develop. According to the 30th "China Internet Network Development Statistics Report" released by China Internet Network Information Center on July 2012 recently shows that at the end of June 2012, China's mobile phone users reached 388 million, increased by about 32.7 million compared with the end of 2011. The percent of mobile internet user increases from 69.3 to 72.2 % [2].

Meanwhile, with the development of technologies and applications, the terminal that stores private information and economic benefits become the primary attack target of the black chain. Both R&D capabilities such as Mobile malware, network attacks and misuse of resources and implementation of environmental already exist. Security issues that the mobile intelligent terminal and operating system facing, such as Android, IOS, Symbian, Windows Mobile and Rim, increasingly prominent.

In the end of December 2013, more than 6000 Mobile malwares were developed in Chinese mainland. As shown in the report of CNCERT, 6249 Mobile Internet

malicious programs were captured in 2011, increasing by more than twice as in 2010. The most is deductions malicious programs, with the amount of 1317, which is 21.08 %, following by spread malicious programs, information theft programs, Hooliganism programs and Remote control programs. From the view of Mobile platform, about 60.7 % of malicious programs aim at Symbian platform, which is lower as in 2010. About 7.12 million Mobile intelligent terminals were infected by malicious programs in Chinese mainland, which brings serious threat and damage to the Mobile intelligent terminals [3]

With the development of technology and application, smart mobile terminals will be confronted with many kinds of security threat in the industrial applications, such as virus, disclosure of confidential information, illegal tampering of code, malicious replace of key components, and so on.

These security events show that attacks may occur in any part of the smart mobile terminal, while the ultimate goal is to get the value of the smart mobile terminal. If any security risk of the mobile intelligent terminal is used by an attacker, it will cause the loss of profits of developers, users and operators, and finally influences the development of smart mobile terminal industry.

We conclude that the threats to the smart mobile terminals can be categorized into the following five categories: 1. The hardware lacks protection measures, resulting from the physical user information stolen and destroyed; 2. The operating system has vulnerabilities, leading to malicious code infection and hacking; 3. The application software is easily hijacked, causing the user accounts and passwords stolen; 4. The communication processing lacks safeguards, call information is easily eavesdropped, leading to user privacy leaks; 5. The user data lacks protection, resulting in the leakage of user privacy. The threats to the smart mobile terminals are shown as Fig. 2.

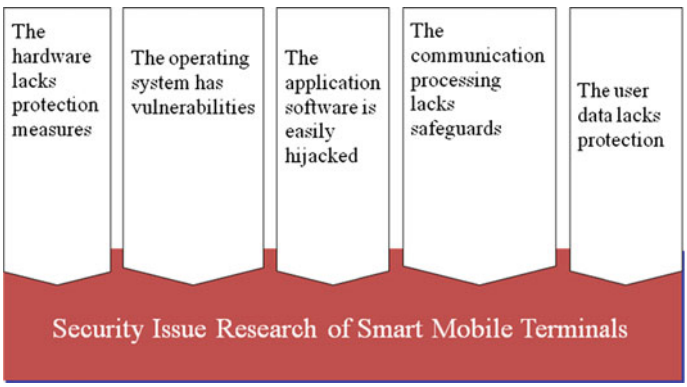

Fig. 2 The threats to the smart mobile terminals

3 Key Security Issue Research of Smart Mobile Terminals

At this stage, we consider that the security research on smart mobile terminal should be focused on three aspects: program security analysis, data security protection and defect research.

3.1 Program Security Analysis

In the application security analysis tools, the majority are the static analysis tools. The static analysis tools can quickly analyze the program features. However, the static analysis tools cannot make good use of information in runtime, so it cannot guarantee the accuracy of the analysis. Dynamic program analysis techniques can be very good to make up for the inadequacies of static analysis.

The current dynamic analysis tools on Android platform including its own Dalvik Debug Monitor Server (DDMS), as well as some of the dynamic monitoring system, such as DroidBox, TaintDroid and so on. However, the existing dynamic analysis tools on Android platform lack the fine-grained control, and lack the flexibility analysis strategy at the same time. In addition, for some heavyweight dynamic analysis (such as the instruction-level tracking), it not enough for the existing tools to complete efficiently.

Currently, the analysis for iOS system and its application is mainly the static analysis and testing. For some added confusion and hidden deep act, it is difficult to find only by a static method, they can be found only in a dynamic perform process. Therefore, the dynamic analysis techniques for iOS system can greatly compensate for the lack of existing detection methods. But it is difficult for the dynamic analysis techniques for iOS system to achieve, and requires the long-term studies.

3.2 Data Security Protection

For the current data security on Android system, there are many non-platform-related security issues (for example, the passwords and other sensitive data are transmitted on the non-encrypted text). In addition, there are also a lot of specific security issues on Android platform (e.g. Intent mechanism is imperfect). These issues are to be enhanced and addressed.

In addition, as a mobile operating system, Android system users and developers maybe are a large number of people with no clear concept of the operating system security, software security. That the users ignore security issues is likely to cause leakage of private data. For example, a considerable majority of Android users in the process of installation program does not care whether the authority applied for the program is necessary; they also do not care about whether their privacy data

stored in the phone has been protected. As developers, some developers have the unskilled development or insufficient attention to security issues, in the process of the programming, they may make some mistakes to give the opportunities for the attackers (for example, passwords do not be encrypted store, and important data stored on the SD card). Such applications into the market would cause great threats to user's privacy and security.

In addition, the traditional Android platforms are mostly based password authentication mechanism, gestures password. This traditional authentication mechanism is simple, vulnerable to violence to crack. For the defect, the future research on authentication could focus on the recognition based on facial, fingerprint, hardware and other non-traditional way.

Current Android applications are vulnerable to attack by the reverse, tampering, and repackaging. Current mainstream Android application obfuscation tool Proguard is unable to meet the growing security needs in confusion intensity. Therefore, more advanced Android code obfuscation program need to be considered to research and develop.

3.3 Defect Research

Android system is based on the Linux Kernel; the common security threats for Linux (primarily security vulnerabilities) are capable to threaten Android system. At the same time, Android system supports the program execution based on the native codes (C language and C++ language) to, which left a hidden danger for the underlying security [4].

The top security system of Android is built based on the security sandbox of Linux Kernel and the checking mechanism of installation permission. Because of the vulnerability of Android kernel, in the event of root right of Android system is taken, the upper security will be completely lost.

The libraries layer in Android system is consist of a number of frequently used system functions, and due to the performance requirements, they is based on Native Code. This layer handles many important functions in Android system, such as database operations, SSL network transmission and so on. It is found based on research that the attack, caused by improper using of HTTPS/SSL in a large number of Android applications, may make the instant messaging content stored in online banking, social networking sites, email to be exposed to the danger. In addition, the system library is responsible for maintaining a variety of data storage and management on Android system (phone, SMS, email, GPS information, etc.). However, because data protection mechanisms as Android are not perfect, private information on the mobile phone cannot be well protected. Figure 3 shows the password is stored unencrypted in Android system.

There is the risk of data loss in Android system. For example, because Google account synchronization function is built on the Android, it will synchronize a lot of information on mobile phone, such as contact lists, system installation application,

Fig. 3 The password is stored unencrypted in Android system

schedule management, directly to Google's cloud platform. At the same time, in Android system customized by a third party, it is possible that there are other data will be synchronized to an external system.

4 Development Direction on Security Research of Smart Mobile Terminals

In the future, we believe that the security research on smart mobile terminals can be divided into three directions: research and development, testing and standards compilation. In the aspect of security research and development, the advanced code

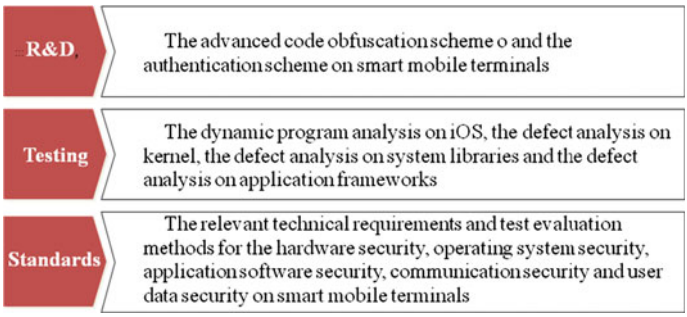

Fig. 4 Development direction on security research of smart mobile terminals

obfuscation scheme on smart mobile terminals, the authentication scheme on smart mobile terminals should be research as soon as possible. In the aspect of security testing, the dynamic program analysis on iOS, the defect analysis on kernel, the defect analysis on system libraries and the defect analysis on application frameworks should be strengthened. In the aspect of standards compilation, the relevant technical requirements and test evaluation methods for the hardware security, operating system security, application software security, communication security and user data security on smart mobile terminals should be accelerated to development. Development direction on security research of smart mobile terminals is presented as Fig. 4.

References

1. La Polla M, Martinelli F, Sgandurra D (2013) A survey on security for mobile devices. IEEE Commun Surv Tutor 15(1):446–471
2. China Internet Network Information Center (2012) The 30th China internet network development statistics report, July 2012
3. CNCERT (2013) 2012 China internet network security report
4. Ongtang M, McLaughlin S, Enck W, McDaniel P (2012) Semantically rich application-centric security in Android. Secur Commun Netw 6:658–673

http://www.springer.com/978-94-6239-144-4

Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation
Innovation and Practice of Industrial Engineering and Management (volume 2)
Qi, E. (Ed.)
2016, XVI, 1134 p. 406 illus., 156 illus. in color.,
Hardcover
ISBN: 978-94-6239-144-4
A product of Atlantis Press