Journal of Applied Science and Engineering Innovation, Vol.3 No.5, 2016, pp. 172-176
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Research on Condition Analysis of Information Security and Protection Strategy of Mobile Intelligent Equipment

Xiaoxing Ma [1]

[1] *Tianjin University of Finance & Economics, 25# Zhujiang Road, Hexi District, Tianjin, 300222, China.*

Abstract: Mobile intelligent terminal has penetrated into every aspect of people's lives, it can not only bring people great convenience, at the same time, it also exists some security risks, how to guard against these threats and protect user information security has become the focus of attention. In this paper, it analyzes the characteristics of the security architecture of intelligent terminal, which also summarizes the various types that can threaten information security, finally it puts forward some designs to prevent the problem.

Keywords Mobile intelligent terminal; Information security; Security architecture

INTRODUCTION

With the continuous development of information technology, mobile terminals have become the electronic equipment that can be most closely related to the people's life and work. The the latest survey report released by the global network index (GWI) has shows us that the number of people that have at least one smart mobile phone is nearly 80% the total number of the global people, among them, nearly half of the people own a tablet (see figure 1). Data from CNNIC (China Internet Network Information Center) has showed that, to the end of June, 2015, the size of China's Internet users has reached 668 million, the scale of mobile Internet users in China has reaches to 5.9357 billion, accounting for 88.9% of the overall Internet users. The function of mobile intelligent terminal has been stronger and stronger, from the original mobile phone, to PDA, to the smart phone, tablet, e-books and navigation equipment and so on in 3G era, the mobile intelligent terminal has become an indispensable daily necessities. Meanwhile, the open and flexible feature of mobile intelligent terminal itself, as well as the wide application of mobile intelligent terminal can bring a great threat to users as well as country in the field of information security, information security of mobile terminal will face various problems: such as malicious software can control the mobile intelligent terminal to send text messages as well as backstage network, which can result in the loss of calling fares; malicious software can also monitor user's communication and obtain user's location information without the user's awareness, read and delete the user's personal data, which can ultimately result in the leakage of user's privacy.

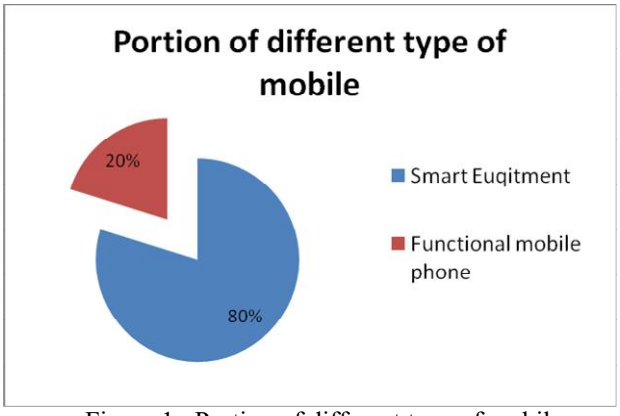

Figure 1. Portion of different type of mobile

SECURITY ARCHITECTURE OF MOBILE INTELLIGENT TERMINAL

The mobile intelligent terminal is mainly composed of two parts, which are hardware platform and software platform. The information security of mobile intelligent terminal is to ensure the safety of hardware in the first place, through the security hardware it can bind with safe operating system, then safe operating system can bind with safe application software, such layers of binding can achieve the

overall safety of mobile intelligent terminal. We can divide the security architecture of mobile intelligent terminal into three layers: hardware layer, operating system layer and application software layer. In addition, mobile intelligent terminals usually have rich peripheral interface, the interface can not only enhance the user experience, but also can increase the risk of spreading the virus, some attackers will attack the mobile intelligent terminal through the peripheral interface, which will threaten the security of mobile intelligent terminal, therefore, when it makes study on the security of mobile intelligent terminal, it is of great significance to take the peripheral interface as the separate content to study.

Hardware Security

The security goal of mobile terminal hardware is to provide reliable hardware platform for the mobile terminal, so as to realize chip level security policy for the mobile terminal and ensure the safety of interior Flash of the mobile communication terminal as well as the safety of baseband, which can ultimately ensure that procedures of chip system, terminal parameters, safety data, as well as user's data can not be tampered or illegal accessed.

Chip level security mainly refers to two aspects, namely, the mobile terminal Flash chip and the security of the baseband chip. Flash chip refers to the clip that can record the procedures of mobile terminal system procedures, terminal parameters as well as the user's data. In order to protect the safety of mobile terminal Flash chip, it need to carry on the safety protection through the program of the system, communication protocol stack, IMEI mobile terminal number, user's privacy data, other configuration software of chip and so on. The baseband chip usually includes a digital signal processor for sound encoding / compression, balance, modulation and demodulation signal processor as well as a control processor for processing the protocol stack and the user's interface. As for the baseband chip, it need to carry on protection for software program in ROM, important safety parameters (such as UID, authentication data, access control list, key, etc.) the logical design information of chip and other important assets and so on.

The Security of Operating System

The operating system of intelligent terminal has developed rapidly from the situation of tripartite confrontation initially Palm, Symbian, BlackBerry to iOS and Android, which has occupied a major share of the market, in 2015, Chinese mobile phone went public, mobile phone system that is installed with Android can account for 82.02% of the attention ratio, which can occupy the vast mainstream; followed by Apple's iOS system, which can get 15.03% of the installation ratio; while the degree of concern of Windows Phone system is 2.01% (see figure 2).

The safety of operating system is designed to carry out scientific and reasonable configuration for the operating system through the sensitive call so as to achieve the goal of information security. The main method is through monitoring and protection as well as reminding for the system, so as to ensure the behavior of the system relates to the safety is always under controlled conditions, thus the user's behavior can not appear in the case without the awareness of the users to execute, or the execution of user's uncontrollable behavior. The information security of the operating system can be mainly divided into the security call control and the update of operation system.

1) Security call control. Due to the openness of operating system of mobile intelligent terminal, the middle layer of operating system can have a lot of application programming interface (API: Application Programming Interface) that can open to users to develop two times, which can bring a lot of risks. If API is not controlled, it is easy for the developer to achieve malicious behavior by reasonable combination of calls, which can threaten the security of user information. API needed for security control can be generally divided into communication class API and address application class API. Communication class API may cause the loss of tariff for the users, such as: calling, three-party calling, sending SMS, sending MMS, sending email, mobile network data connection and WLAN network connection, etc.. Address application class API may result in the leakage of user's privacy information, such as: locating, calling and recording, local recording, taking photo / video, the operation of the user's data and so on. The way of security control is to get the recognition of users when it calls these sensitive API, then the corresponding calling behavior can be implemented. Each calling should be recognized by the users is the safest approach, which may affect the user's experience, so in order not to affect the user's experience, for different application scenarios, users can choose other ways for confirmation. For example when the application software is used for the first time to confirm, once it is confirmed, the confirmation can be valid for a long period of time, or it can be re-confirmed when it restarts the software.

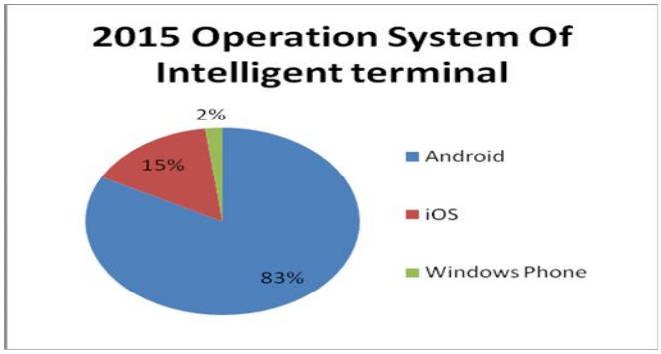

Figure 2 Operation System of Intelligent terminal

2) The update of operating system. In addition to strengthening security call control of the operating system, it also should ensure that the update of operating system itself is controllable. Due to the openness of operating system of the intelligent terminal, the mobile intelligent terminal can be carried out brush machine operation that is not officially authorized by the official. Through the brush machine operation to mobile intelligent terminal, it is possible to modify the mobile intelligent terminal protocol stack, which can implant malicious code to the mobile terminal, so as to bring a huge security threat to mobile intelligent terminal. So mobile intelligent terminal should be able to ensure that the official authorization can update the operating system, for non authorized update of operating system, it should give users the appropriate prompt, so as to ensure the safety of the operating system. As for the update that can not guarantee the safety of the operating system, manufacturers should tell users in the specification or other places that may bring security risks.

3) The security of application. With more and more mobile intelligent terminal users, the corresponding application software also increased rapidly. However, due to the manufactures of operating system is lack of the audit mechanism for application software, the attacker is very easy to input the viruses, Trojans, worms, and other malicious codes into the application software, which can cause a certain harm to the mobile intelligent terminal users. The goal of application software security control is to determine the source of the application software, so as to control the sensitive behavior of the installed software.

Security Control of Application Software

The security control preventing technology of application software can be divided into two kinds: the authentication signature mechanism of application software and control technology of sensitive API.

1) The Authentication Signature Mechanism of Application Software. The authentication signature mechanism of application software is an effective means to manage the application software in the field. Android, Apple, Mobile Windows and other smart terminal manufacturers have adopted their own digital authentication signature mechanism, so as to call the specific API software for testing and certification, the software through the test can get digital signature. While the software without the authentication signature will not be able to call the sensitive API when it is installed and operated in the mobile intelligent terminal or it must remind the users of the safety when it calls. Through the authentication signature mechanism of application software, it can avoid the spread of the software effectively that may carry the malicious code or the illegal content.

2) Control Technology of Sensitive API. In addition to using the signature mechanism of the application software, it can also strengthen the management of sensitive API, so as to secure mobile intelligent terminal. API control technology of application software is similar to the security control technology in operating system that is mentioned above. The operating system of mobile intelligent terminal can provide the application of sensitive API control, so that users can provide with options to allow or prohibit the application of software to the call of sensitive API. By sensitive API control technology it can effectively prevent the application of malicious code to implement malicious behavior.

SECURITY MECHANISMS

System Protection Strategy

In order to ensure the safe operation of the system, the operating system of the intelligent terminal should provide the following mechanism:

1) Protecting password, including timeout setting, password length and password updating period;

2) Setting the security strategy of pushing email, if the user intelligent terminal is configured to access e-mail account, then email that is in accordance with the security strategy will be pushed to sync email directly on the terminal, which does not need to set by users;

3) Limiting the security strategy and restrictions on equipment through the XML file, VPN (Virtual

Private Network) configuration information, Wi-Fi settings, mail settings and so on;

4) Restricting the service of intelligent terminal can access, usually it can be including some network applications, such as Safari, YouTube, iTunes, Store and so on.

Data Protection Strategy

In order to protect confidential data of the intelligent terminals, the intelligent terminal manufacturers introduced a set of encrypted data protection mechanism to ensure that the system data can not be accessed directly when the mobile phone is locked or shut down. This kind of mechanism can be included:

1) The application of 256-bit AES (Advanced Encryption Standard) hardware encryption algorithm;

2) The support of remote information cleaning, if the user's mobile phone is lost or stolen, the owner or the administrator can trigger equipment remote information clear command, which can eliminate data on the device;

3) The elimination of local information, if the attempt of trying multiple password failed, the operating system can automatically start the local information elimination operation.

Security Strategy of Network Communication

In order to ensure the users can access to the remote with safety and do business with mobile office, the security strategy of intelligent terminal should provide VPN virtual private network, SSL/TLS communication encryption, WPA/WPA2 wireless access as well as the other aspects of the protection of communication.

PROTECTION STRATEGY

First of all, the users of intelligent terminal should improve the consciousness of self protection. To develop good habits of self protection can effectively prevent the leakage of information, such as not storing confidential information in the terminal, setting boot password, login password as well as SIM card password etc., as for the phone book, SMS, user documentation and other sensitive information, it should encrypt. If the terminal is lost, people can use the remote control program to destroy the user's private information, locking the terminal, so as to get the location information of the terminal and help to find out the lost terminal.

Secondly, installing protective software. Through anti-virus software from the third party, it can achieve real-time interception, the unsafe information sent to the terminal can be alarmed, so as to kill the confirmed virus as well as other operations. Finally what to be reminded is that the users of the terminal do not jailbreak the intelligent terminal, because a large number of intelligent terminal security problems and hidden danger will be existed after jailbreak. Only taking the mobile phone as an example, it is officially reported that the operation of jailbreak will cause the collapse of the mobile phone frequently; inaccurate positioning data; easy to steal personal information by hackers, adding malware or virus; shortening the battery life and other hazards.

CONCLUSIONS

With the rapid development of mobile Internet, mobile intelligent terminal has become the terminal that can carry information, however, because the intelligent terminal can store and manage a lot of sensitive information of the users, its operation and use can be closely related with the user's economic interests, so the safety problem of intelligent terminal has attracted public attention. The personal data that users stored in the mobile intelligent terminal (such as contacts, SMS, calendar, etc.) may be leaked out without the user's acknowledge, which will cause huge losses to the users. Compared with the traditional terminal, the security threat that is faced by intelligent terminal is more extensive, so it is particularly important to have accurate security analysis and evaluation on the behavior of intelligent terminal software.

In this paper, based on the current security situation of mobile intelligent terminal, it has analyzed security technology of mobile intelligent terminal, since the security problem of mobile intelligent terminal software is becoming more and more serious, which requires both manufacturers and industry associations to deal with all kinds of security risks with multi-level security protection technology, which also should strengthen the research of the intelligent terminal software security assessment tools and methods in the future so as to actively develop the safety of technical standards according to all kinds of intelligent terminal software;meanwhile, it also should improve software quality and safety standards from the source of software development, so as to implement the mandatory safety measures in the whole life cycle including software development, launching and operation. It also should further strengthen the network of mobile Internet and information security standards as well as management practices in all aspects, so as to promote the detection and evaluation of security of the intelligent terminal application software from the third party and ensure the information security of mobile intelligent terminal, which ultimately can protect the interests of users that are not compromised.

ACKNOWLEDGMENT

The authors wish to thank the helpful comments and suggestions from my colleagues in Department of information science and technology of TJUFE at Tianjin. This work is supported by the study fund of TJUFE at Tianjin (No. 201610070007).

REFERENCES

[1] David Barrera, A methodology for empirical analysis of permission based security models and its application on

to Android[J]. School of computer Science, 2010, 20(4):54-58.

[2] Li Xia, Research on the security mechanism of Android operating system[J]. Computer knowledge and technology: Academic Exchange, 2014, 2(3):1180-1188.

[3] PATRICIAMM DONNA H, Business risks and security assessment for mobile devices[J]. Information Systems Control Journal, 2008,Vol.21:1-6.

[4] Wei Liang, Mobile Internet Security Framework. ZTE technology, 2009, Vol2: 45-50.

[5] Feng Sha, Min Dong, Mobile internet security issues[J]. Analysis of modern telecommunications technology, 2010, Vol4:14-23.

[6] Chen Shangyi, Research on Internet security technology.Information security and communication security, 2010, Vol8:16-20.

[7] Zhou Lan, Mobile Internet business innovation analysis. Modern telecommunications technology, 2012, Vol 8:32-40.

[8] Wang Qiang, Li Yaohua, Chen Lulin, Su Yanhua, The strategy of the development of mobile Internet in China[M]. Modern telecommunications technology,2013.

[9] Chen Shangyi, "Research on Internet security technology[J]. Information security and communication security, 2013, Vol 8:45-49.

[10] 2015-2016 China smart phone Market Research Report[L].http://www.chinairn.com/report/20160428/104527882.html.

[11] 2015-2016 China Mobile / smart phone Market Research Annual Report[L]. http://mt.sohu.com/20160505/n447809847.shtml.

[12] 360 mobile guards security broadcast - 26[L].http://shouji.360.cn/securityReportlist/securityReport_26.html.

[13] Guo Chenfeng, Guo Jing, China Mobile Internet application market analysis[J]. Digital communication world, 2014, Vol.8:35-39.