Journal of Applied Science and Engineering Innovation, Vol.3 No.5, 2016, pp.161-164
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Research on Protection Strategy of Information Security of Intelligent Mobile Terminal

Xiaoxing Ma [1]

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

Abstract: Intelligent mobile terminal has penetrate into modern people's life, bring people great convenience, at the same time also has bring the security risks, how to protect user information security and guard against these threats, has become the focus of attention. This paper focuses on the analysis of the security features of the intelligent mobile terminal, and summarizes the various problems of the threat on information security, and finally puts forward some measures to prevent.

Keywords: Information security, Security risk, Mobile intelligent terminal

INTRODUCTION

With the continuous development of information technology, mobile equipments have become the electronic equipment most closely related to the people's life and work. Global network index (GWI) released the latest survey report shows that people have at least one smart phones accounted for the proportion of the global total number of nearly 80%, of which nearly half of the people have one tablet PC (Figure 1).

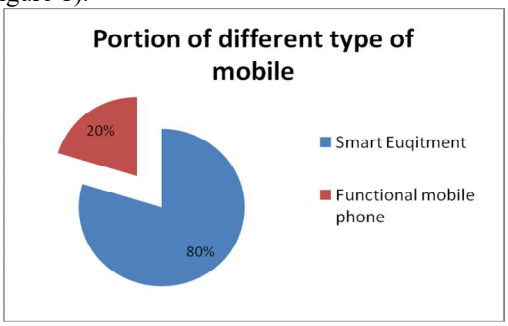

Figure 1. Portion of different type of mobile

From CNNIC (Chinese Internet Network Information Center) show that at the end of 2015, Chinese Internet users reached to 668 million, of which mobile phone users for 593570 million, accounted for 88.9%in the overall Internet users. From the original mobile phone, PDA, and now in the era of 3G smart phones, tablet PC, Kindle and navigation equipment, due to the popularity of mobile intelligent mobile terminal will continue be powerful and widespread in large areas, mobile intelligent mobile terminal has become indispensable to people's daily life activities. Due the character of openness and flexibility of the mobile intelligent mobile terminal, intelligent mobile terminal as well as a wide range of applications, caused a great threat to the security of information to mobile users. Mobile intelligent mobile terminal faced with all kinds of security problems: such as malicious software can control mobile intelligent mobile terminal background to send messages and background networking, resulting in the loss of telephone fare; malicious software can also monitoring the invocation, access to user location information, read and delete the user's personal data in the case of users without knowledge, resulting in leakage of user privacy.

SECURITY ARCHITECTURE OF MOBILE INTELLIGENT MOBILE TERMINAL

Mobile intelligent mobile terminal is mainly composed by two parts, which are hardware platform and software platform. Mobile intelligent mobile terminal security architecture is an open operating system as the core, which is an important feature of mobile intelligent mobile terminal. The security architecture of mobile intelligent mobile terminal consists of three layers: hardware layer, operating system layer and application software layer. The first of mobile intelligent mobile terminal security architecture is to ensure the safety of hardware, through secure hardware binding security operating system, security of operating system binding secure application software, through the binding layer by layer to achieve overall safety of the mobile intelligent mobile terminal. Mobile intelligent mobile terminals usually have ample peripheral interfaces, which enhance the user experience and increase the risk of virus transmission, some of the attackers will attack through the peripheral interface of mobile intelligent mobile terminal, and cause the threat to the safety of mobile intelligent mobile terminal, so we take the security of peripheral interfaces as a separate research content has important significance in the study of the security of mobile intelligent mobile terminal security. In addition, with the development of intelligent and storage space of mobile intelligent mobile terminal, many important data such as the

phonebook, SMS, agenda are stored in the mobile intelligent mobile terminal, once the privacy in the terminal was leaked, it will cause great harm to the user, so the user data protection is also a very important aspect of mobile intelligent mobile terminal security research.

Hardware security

The goal of mobile terminal hardware security is provides reliable hardware platform for the mobile terminal, to achieve the security policy on the mobile terminal chip level to ensure the safety of internal flash and baseband in the mobile communication terminal, ensure the chip system program, terminal parameter, and data not to be tampered with or illegal access.

The security of mobile terminal chip is mainly refers to the security of internal Flash chip and the baseband chip of mobile terminal. Flash chip is the recording of the mobile terminal system procedures, terminal parameters and user data chip. In order to protect the mobile terminal flash chip, should carry out security protection about the system boot program in the chip, communication protocol stack, mobile terminal IMEI number, user's private data and other chip configuration software. The baseband chip usually includes a digital signal processor for sound encoding/compression, balance, modulation and demodulation, and a control processor for processing the protocol stack and the user interface. Safety protection for baseband chip is mainly about the software program ROM, important safety parameters (such as uid, data authentication, access control list, keys) and logic design information of the chip and other important assets.

Operating system security

Intelligent mobile terminal operating system forms a tripod complexion from the original palm, Symbian, blackberry, now Android and IOS occupy a major share of the market. In 2015 82.02% of the proportion installed the Android system for mobile phone in Chinese intelligent mobile terminal market, occupies the absolute mainstream status, occupy the absolute mainstream. Followed is Apple iOS system, access to 15.03% of the proportion of the installation, Windows Phone system concerns 2.01% (see Figure 2).

The security of the operating system is designed to achieve the security y of the operating system by scientific and reasonable configuration. The primary means is to monitor, protect, and remind the system resource invocation, to ensure that the behavior of the system relates to the security is safe and always in a controlled state, make sure do not implementation of a certain behavior without user's knowledge, or the execution of user's uncontrollable behavior. Operating system security capability is mainly divided into secure invocation control and operating system update.

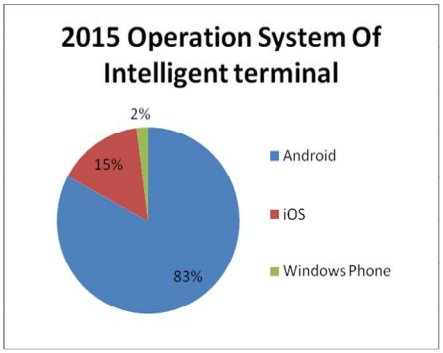

Figure 2

Due to the open of the mobile intelligent mobile terminal operating system, The middle layer of the operating system has a lot of application programming interface (API) to the user to carry out the secondary development. This brings a lot of risk. If the API is not controlled, it is easy for the developer to implement malicious behavior by a reasonable combination of calls. If the API is not under controlled, it is easy for the developer to implement malicious behavior by a reasonable combination of invoking, cause threat to the security of user information. API needs to be controlled for security including API that for communication and address application. API for communication may cause loss of user charges, such as: call, third party calls, send SMS, email, mobile network data connection, WLAN network connections. API for address application may result in the leakage of user privacy information, such as: home address, call recording, local recording, pictures and video, operation to the user data.

Security control is when the sensitive API execute corresponding invoke behavior must confirmed by the user. Each invocation is confirmed as the most secure approach, but it may affect the user experience, So user for can choose the different way of confirmation with different application scenarios, in order not to affect the user experience. User only have to confirm the security behavior at the first time to run the application software, confirmation will effective for a long-term, when the application software is reboot then need to re-confirm.

Besides strengthen the operating system security invoking control, but also to ensure that the self upgrade of operating system is controllable. Due to the openness of the intelligent mobile terminal operating system, a lot of mobile intelligent mobile terminal leave the factory can also install unofficial operating system, it is possible to modify the protocol stack of intelligent mobile terminal to implanted malicious code, which brings a huge security threat to the intelligent mobile terminal. So the intelligent mobile terminal should be able to ensure that the official authorization of the operating system update, give users the corresponding prompt for unofficial operating system updates, to ensure the security of the operating system, manufacturers should express risks for the security of the operating system cannot

be guaranteed for unofficial updates in the instructions.

Application software security

With the increasing number of intelligent mobile terminal users, the corresponding application software is also increasing rapidly. However, for the lack of audit mechanism that operating system vendors, attacker is easy to embed virus, Trojans, worms, and other malicious code into the application software, caused some harm to the users of intelligent mobile terminal. The goal of application software security control is to determine the source of the application software and control the sensitive behavior of the installed software.

1) Certification signature for application software:

Certification signature for application software mechanism is an effective means to manage the application software. Android, iOS, Windows Mobile and other smart terminal manufacturers have taken their own digital signature authentication mechanism, for testing and certification the specific API software through the test software for digital signature. Without the signature authentication the software in the installation and operation of intelligent mobile terminal, will not be able to invoke the sensitive API or will remind the user security issues may invoke. By applying authentication signature mechanism can effectively avoid the application software carry the malicious code or the illegal content.

2) Management and control technology for sensitive API:

In addition to the safety precautions of intelligent mobile terminal, we utilize the signature mechanism of the application software, also to strengthen the invoke management of sensitive API. Control technology for API is similar to the security control technology of operating system application software. Operating system of intelligent mobile terminal can provide the control for software application to invoke the sensitive API, to provide users with the option to allow or prohibit the application of software to invoke a sensitive API. By applying control technology for sensitive API can effectively prevent the behavior that application implement malicious code.

SECURITY MECHANISM

System protection strategy

In order to ensure the safe operation of the system, the intelligent mobile terminal provides the following mechanism:

1) Password protection, including timeout settings, length and update cycle of the password;

2) Security policy setting, if the intelligent mobile terminal is configured to access the Exchange Microsoft account, then the corresponding policy like ActiveSync Exchange will be pushed directly to the device, user do not require to set;

3) Configuration to security policy and restrictions for VPN (Virtual Private Network) configuration, Wi-Fi settings, mail settings of the intelligent mobile terminal through the XML format file;

4) Restrict the service intelligent mobile terminal can access, usually including some network applications such as Safari, YouTube, iTunes Store.

Data protection strategy

In order to protect confidential data in intelligent mobile terminal, the operating system of the terminal is introduced into a set of cryptographic data protection mechanism to ensure that the data of operation system cannot be accessed directly when the terminal is locked or shut down. The mechanism includes:

1) Apply of 256 bit AES (Advanced Encryption Standard) hardware encryption algorithm;

2) Support clear information from remote for user. If the intelligent mobile terminal is lost or stolen, the owners can trigger clear up information from remote to eliminate the data on the terminal;

3) Elimination for local information, if password entering attempts fail repeatedly, the operation system starts to eliminate the local information automatically.

Network communication security policy

In order to ensure user access from remote and security mobile office, the operation system provides communication methods like VPN, communication encryption like WPA/WPA2 for access wireless.

RESULTS AND DISCUSSION

First of all, to improve self-protection awareness of user. Develop a good habit of self protection, can effectively prevent information leakage. For example, do not store confidential information in the intelligent mobile terminal, set the power-on password, login password and SIM card password, encrypt the phone book, SMS, user documents and other sensitive information. If the terminal is lost, user can use the remote control program to eliminate the user's private information, lock the phone, and access to the location of the phone information to help retrieve the lost terminal. Second, install the protective software through third-party antivirus software can provide real-time interception, prompting unsafe operation, killing the confirmed virus. Finally need to be reminded that do not breakout the intelligent mobile terminal. There are many security risks after the breakout of intelligent mobile terminal. The official said that, taking the mobile phone as an example, the breakout will cause the phone to frequent accidental crash; generate inaccurate location data, allow hackers to steal personal information, implant malicious software or virus; shorten the life of battery and other hazards.

CONCLUSION

The rapid development of mobile Internet, mobile intelligent terminal has become the main information carrier. However, consider storage and manage large number of sensitive information in the intelligent mobile terminal, its operation and usage related to and the economic interests of the users closely, so security problem of intelligent mobile terminal has attracted public attention. Compared with the traditional terminal, intelligent mobile terminal face broader security threats, security problems of terminal software have become increasingly severe, which requires with multi-level protection technology to deal with all kinds of security risks, to protect the interests of users is not compromised.

The leak of personal data such as contacts, SMS, calendar that user stored in the mobile intelligent terminal, will cause huge losses to the user. The security crisis of application store and application software has become increasingly serious, the accurate analysis and evaluation of security for intelligent terminal software is particularly important. Therefore, the mobile intelligent terminal should provide protection mechanism for user data protection.

The article analyze the security protection technology of mobile intelligent terminal based on current the security situation of mobile intelligent terminal. We should actively develop according to the technical standards for the security of all kinds of intelligent terminal software, to strengthen the research on safety assessment tools and methods of intelligent terminal software, carry out efficiency security assessment. At the same time, we should improve the quality and safety software from the source of software development, and implement compulsory safety measures in the whole life cycle in software development. Further, enhance the standards, management methods of mobile Internet network and information security, promote the security evaluate application of third party intelligent terminal software .

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

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

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

360 mobile guards security broadcast - 26, http://shouji.360.cn/securityReportlist/securityReport_26.html

Chen Shangyi, 2010 "Research on Internet security technology", Information security and communication security, 2010 vol.8, pp 16-20.

Chen Shangyi, 2013"Research on Internet security technology ". Information security and communication security, vol.8, pp 45-49.

David Barrera, 2010 “A methodology for empirical analysis of permission based security models and its application on to Android”. School of computer Science.

Feng Sha, Min Dong, 2010"Mobile internet security issues", Analysis of modern telecommunications technology, vol.4, pp 14-23.

Guo Chenfeng, Guo Jing,2014" China Mobile Internet application market analysis". Digital communication world, vol.8, pp 35-39.

Li Xia, 2014 “Research on the security mechanism of Android operating system”, Computer knowledge and technology: Academic Exchange, pp :1180-1188.

PATRICIAMM DONNA H, 2008 “Business risks and security assessment for mobile devices. Information Systems Control Journal, vol.21, pp :1-6.

Wang Qiang, Li Yaohua, Chen Lulin, Su Yanhua, 2010"The strategy of the development of mobile Internet in China". Modern telecommunications technology

Wei Liang, 2009, “Mobile Internet Security Framework”, ZTE technology, vol.2, pp 45-50.

Zhou Lan, 2009"Mobile Internet business innovation analysis", Modern telecommunications technology, vol.8, pp 32-40.