Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):2477-2483

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

An analysis of internet accounts' security threats by mobile phone password protection

Yanni Li[1], Zhijuan Li[2], Zheng Lv[1] and Haopeng Sun[3]

[1]School of Foreign Languages, Changchun Institute of Technology, Jilin, China
[2]School of Foreign Languages, Changchun University, Jilin, China
[3]School of Software Engineering, Changchun Institute of Technology, Jilin, China

---

ABSTRACT

With the development of mobile communication network and the popularity of smart phones, mobile phones are not just simple communication tools, but a protection tool which is used to authenticate the login or other sensitive operations for the Internet accounts. (mobile phone password protection). But on the other hand, mobile phone password protection is gradually facing with a series of security threats which possibly threaten the security of Internet accounts. Based on other researches and related cases, this paper is trying to take Tencent QQ, mobile banking and Alipay as the examples to analyze every security threat of mobile phone password protection in detail. It aims at enhancing the security consciousness of users and offering some solutions as well.

Keywords: password protection, verification code, security, Internet account.

INTRODUCTION

The Internet account security problems have always been the hot topic for people. Whether for the general software accounts or other special financial accounts such as mobile banking and Alipay, safety and reliability are the prerequisite for people to use them. All of the users need safety password protection measures for their accounts.

It has been for several years that mobile phones could be used as a protection tool for Internet accounts. [1]Among all of the password protection measures, mobile phone password protection has been applied most widely because of its simple operation and convenience. But on the other hand, mobile phone password protection is gradually facing security challenges for various reasons. There are always stealing cases about Internet accounts caused by mobile phone repotted in recent years. According to the research of Netqin (NQ), the total amount about stealing cases of Internet accounts caused by mobile phone is over 10.000 in 2013. So what are the real reasons that mobile phone password protection causes such accidents on earth? And how to avoid those security threats from phone password protection? Such questions always become the focus among the users of mobile phone password protection.

It is necessary for the users to know and avoid the security threats of mobile phone password protection deeply.

EXPERIMENTAL SECTION

Mobile phone password protection is a new and dynamic account protection measure. It takes the dual factors' verification. The principle is that the user binds his mobile phone with the related account. And if it needs to authenticate the login or other sensitive operations of the account, the user needs not only to enter password but also to

enter the verification code which he receives from the mobile phone text message. In this way, the related account could get another protection except the only password.

But from the cases in reality, there are many security threats about the mobile phone password protection. The related Internet accounts' stealing cases have become troubles to the modern people gradually. [2]

The available range of mobile phone password protection

Mobile phone password protection can be used as a password protection tool of traditional Internet accounts such as Tencent QQ. Traditional Internet was born early, and all sorts of hacking technologies have also gone through a long time development. So the current Internet accounts based on Windows operation system are all directly facing Trojan and malicious virus' threats from the Internet. In this context, all kinds of the Internet companies have launched various account protection measures to ensure the account security of their products. And mobile phone also serves as a protection measure among them. On the one hand, because the verification information is independent of PC, mobile phone password protection has some advantages compared with other protection measures and the traditional Internet accounts could avoid the threats of Trojan and malicious virus effectively. But on the other hand, there are some security threats which may reveal the users' personal information. It is worth noticing that those threats are from both mobile phone password protection and the users themselves.

Mobile phone password protection can be used as a password protection tool of mobile Internet accounts such as mobile banking. The development of the mobile phone brings about the development of mobile Internet technology. Various Application（app) software based on phone operation systems are gradually turn public lives around. A great number of Internet companies also take mobile phones as a account protection tool. But different from traditional Internet, mobile phones are used as not only a protection tool but also the running platform for APP software at the same time. The threats from mobile devices, mobile operation systems and mobile Internet have become the main security threats to mobile Internet accounts.

The main security threats to traditional Internet accounts and mobile Internet accounts in detail

The security threats which traditional Internet accounts and mobile Internet accounts are faced with are different.

1. Security threats to traditional Internet accounts

The security threats of mobile phone password protection to traditional Internet accounts are mainly form the flaws of the products and the thin security consciousness of users. The paper would take Tencent QQ as the example to analyze them.

1) The threat of supreme authority

In fact, there are still other password protections except mobile phone password protection for traditional Internet accounts.

① Password Protection Card. Tencent's password protection card is a matrix card which takes the 8 x 10 structure. So there are 80 cases in the card and there is a double-digit in each case of the matrix. After the user binds the QQ account with the password protection card, Tencent's database will activate the matrix digits of the card. When the user wants to modify the password or make any sensitive operation or it needs to authenticate the login, he has to enter the three random double-digits according to the password protection card to complete the operation. The principle of the password protection card is one-time pad, which is a very safe design on the surface. Therefore, many computer game companies are also promoting and taking this kind of password protection card to ensure the safety of players' fictitious assets in the game. But in reality，it's very simple to break this kind of password protection card.

② Security questions. Security questions are used for password protection of all kinds of Internet accounts since the advent of the Internet. It is a primitive safeguard measure and it is still widely used in various of security systems of Internet accounts. so far, Security questions of most Internet generally are three preset questions and answers which are used to authenticate the identity of the users. Because they couldn't cope with the Trojan and malicious virus，their function is just to modify the password under safe environment but not to authenticate the login or other sensitive operations of the account. In this sense, Security questions are nearly useless to the account security.

2) The threat from flaws of dual factors' verification

Because of the dual factors' verification, mobile phone password protection is considered the best password protection to all kinds of traditional Internet accounts. When it needs to authenticate the login, the system will ask the user to enter both password and the verification code from phone text message to ensure the safety of the account. Even if the ID and password leaks out, dual factors' verification will also block those criminals' infringement.

3) The threat from flaws of Mobile-Token
Some Internet companies develop Mobile-tokens to assist mobile phone password protection. Mobile-token is a kind of APP based on smart phone client side, and it can simplify the process of operations of modifying passwords and authenticating login. But what some Mobile-token binds with is app serial number but not the SIM card, for example, QQ Mobile-token could work without the SIM card. That means if the user replaced the phone but not uninstall Mobile-Token, the criminals would make use of the abandoned phone to modify password or setting of QQ game logins and Q coins' consumption verification.

2. Security threats to mobile Internet account
The security threats of mobile phone password protection to mobile Internet accounts are mainly form the virus based on mobile phone operation systems and factors concerned with mobile phones themselves. The paper would take mobile banking as the example to analyze them.

As an extension and innovation of the traditional banks, the security threats of mobile banking present the complexity and diversity. For most commercial banks, verification code of phone text message (mobile phone password protection) is still the main verification method in the transaction of mobile banking service. But the openness and virtual of Internet as well as mobile device's defects will all bring some security threats to the mobile banking or to this kind of password protection. The variety and content of security problems have different forms.

1) The threat from malicious APP
In the first quarter of 2013, the mobile banking client-side of China Construction Bank was infected by a virus named a private email. The virus could embed itself in the mobile banking client-side by means of the second packaging. It could also download and install itself automatically without the user's permission. The point is that the virus could intercept the bank account, password and even the verification code of text message and then send the information to the hacker.

For the mobile banking client-sides, there appear a series of malicious APP to obtain the use's information at present. This kind of APP or the variant programs often spread in some unknown APP stores or mobile forums.

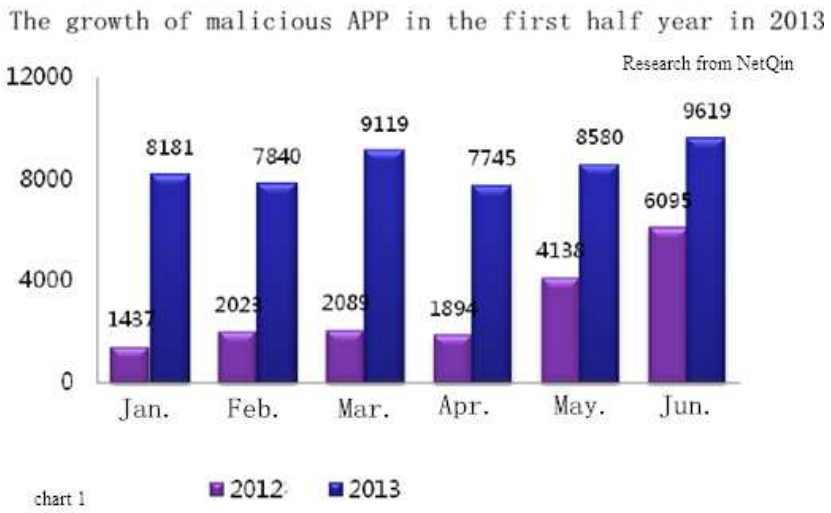


chart 1

There are three obvious characteristics as followings. First, disguise. This kind of APP can be disguised as a popular online APP such as Banks' client-side to mislead the user's operation. Second, update. the APP has a normal application but it will inject malicious code after the installation, and every once in a while it will automatically connect to the remote server and update the instruction of the hacker. Then steal. Once the APP installed in the mobile phone, the virus would intercept mobile phone number, the type of data connection, information of SIM card, bank account number and password, or even verification code of phone text message. The hacker could log in the account with another mobile phone and control the user's phone to do the transaction operations and then intercept verification code of phone text message through Trojan program. Therefore, the hacker could steal the money of user's bank account. In the future, the malicious APP could also use the same problems to threaten other accounts such as Alipay in the same way as mobile banking.

Research of NetQin shows that the amount of malicious APP is growing at a high speed, and it has been the main way for virus to spread. [3]

2) The SMS fraud of false base station
False base station is a kind of high-tech equipment. It generally consists of a host machine and a notebook computer. When false base station starts to run, it could interrupt and shield all the signals of communication operators. The shielding time could last 10-20 seconds and the false base station could get mobile phone cards' information at a certain radius during this time. Then it could disguise itself as communication operators' base station and then send fraud text message to the users' phone on behalf of the official phone number of banks. [4]

And different from general SMS fraud, this kind of false base station is very deceiving. The usual phone numbers which send the fraud text message are just similar to the real one, some alert users would see through that .But the sender numbers from false base station are totally the same as the real ones, so most users couldn't have the ability to see through them. Therefore the false base station could easily attract people to the phishing websites and obtain the bank account number, password and verification code of phone text message.

3) Lack of management for renewing SIM cards
After obtaining the bank account and password, the hacker could intercept the verification code of phone text message through not only using the virus but also stealing the personal information and renewing the SIM card. At present, part of the communication operators does not have the ability to identify fake ID card. If the information someone hold is the same as the information reserved, the clerk could renew the SIM card for him. The banks themselves and communication operators are both the participants in mobile banking service. But the banks will not do some relevant operation process of communication operators and make proper solutions or pre-arranged plans to deal with this security problems. The lack of joint security mechanism between banks and communication operators also become a kind of threat which couldn't be ignored.

4) The existing potential technology problems
① The disadvantage of root or jailbreak. In order to obtain the absolute control over mobile phone or make it convenient to use the pirate APP , most users would root (Android) or jailbreak （Ios）their phones, and According to the statistics, by the end of 2013 the total amount of this kind of users has increased to 47% among the smart phone users.

Both Android system and Ios system are taking the principle of Sandboxie to achieve the segregation and the control resource access among the software. But after root or jailbreak, the app software could break the Sandboxie and access API or resources. The point is the app software based on Android system and Ios system could be decompiled. [5]

The result is that although more free shanzhai or pirate third-party app software could be installed in this way, the trojan could be also mixed into the operating systems easier and brings security risks at the same time. The root or jailbreak of mobiles phones make the hacker obtain the verification code easier. So they could be a threat to mobile banking or other accounts.

② The defects of mobile phone systems. Mobile banking service is provided based on a system platform, which in fact is the mobile phone operation system. The main three mobile phone operating systems present are Android, Ios and Symbian. Most mobile banking client-sides are developed for those three operation systems. But just like personal computers, there are also vulnerabilities in the mobile phone systems.

For example, the certification permission vulnerability of authToken in Android system ever existed under Android version 2.3.3, the attack generally occurred in some wi-fi network. The attacker may be disguised as an open wi-fi point to guide users to the network connection, and then through the authToken, the attacker could get the user's personal privacy, as well as bank account number, password and verification code of phone text message.

Although Google has fixed this vulnerability and close the function of automatically finding and connecting network after version 2.3.4, there are still a great number of users under version 2.3.3 in China who haven't realized the threat at all. And as for IOS of Apple, it has been reported that a series of security accidents for IOS system of Apple have continually occurred since 2011, which are also worrying.

③ The threat from public Wi-Fi network. Because the Wi-Fi technology have been born for many years, and as technology advances, the security measures of Wi-Fi early version have been cracked. The hacker could intercept

verification code of phone text message of banks just through Wi-Fi signal analyzer. Most people would unconsciously connect the Wi-Fi network without password in public, even the kind of action has already been a lifestyle for modern people. But few of them know it is a dangerous action. [6]

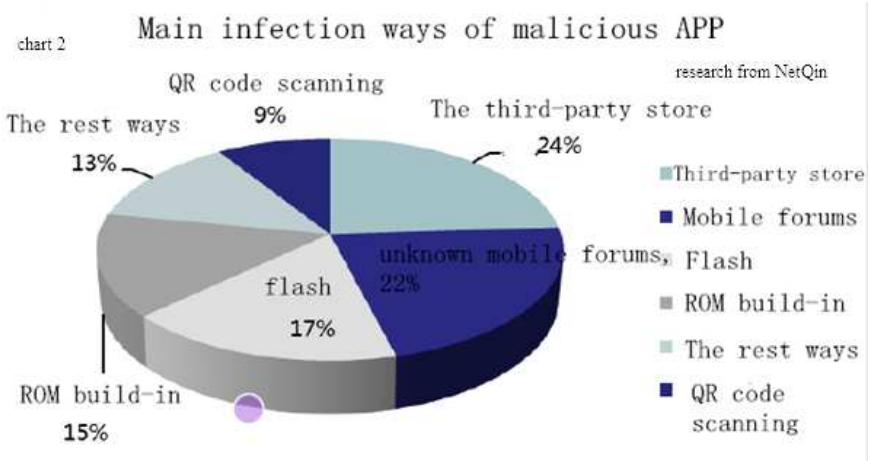
④ The outer attack and fraud. China is the main disaster area of mobile Internet virus all the time. By the end of 2013, the total amount of all kinds of known phishing sites released by CNNIC has reached to 100,000. Some famous virus such as Banker keylogger has stolen the money of mobile banking users and online banking users over ¥ ten millions. The varied fishing websites or web with trojans have become the main threat to the users of mobile banking service. The point is this Internet fraud has two obvious characteristics: Firstly, the fraud is becoming much trickier gradually than before. The hackers have learned how to induce the users to be deceived according to user's habits. Secondly, the fraud period lasts shorter than before .The average survival period of phishing websites in 2013 is less than 12 hours. That means it is usually too late when the user finds the fraud.

⑤ The threat from single verification protection. The traditional online banking have already developed a variety of verification measures after years of development such as digital certificate, E-Banking Code Card, the reserved information verification, verification code of phone text message, e-Password Device and so on. Most of the online banking of commercial banks are using dual verification mechanism, the basic security matures have been developed maturely. However, due to technical limitations of mobile banking, verification code of phone text message is still the only verification protection for most of commercial banks. The single verification protection creates significant security risk.

⑥ The Lack of security consciousness. Lack of security consciousness is the most serious problem in fact. Some users don’t know that a mobile phone, in modern life, is not just a simple communication tool but also the safeguard of Internet accounts, and There is no doubt it is equivalent to the ID card in people’s real lives, once a phone is lost or used maliciously by some people, the Internet accounts will be in the risks, the user’s personal data might also leak out. But most users don’t acquaint this very well and don’t keep their phones carefully. That sometimes would cause big trouble. So it is very important for us to improve our Safety consciousness and ensure the security of our mobile phone. Because the mobile banking service refers to many aspects of Internet security, mobile phone security and communications security, most users could not acquaint with them in detail. So the public should acquaint with the whole system to improve their public security consciousness.

RESULTS AND DISCUSSION

From the research of NetQin, it can been seen that the infection ways of malicious App are usually equipped with malicious software. In order to save money, some users are accustomed to buy the used phones, refurbished phones and shanzhai phones through the Internet or the other informal ways .But it is very possible for these phones to have been embedded the virus programs. And because they are hidden deeply, it is very difficult t find them for users.



Besides, they are also infected through flash. Some users often take the method of flash to reinstall mobile phone system so as to obtain the absolute control over mobile phone. But plenty of users just directly download the flash software in some informal forums. There is not any security permission for this kind of flash software. It could be uploaded by hackers, so those software might contain some Trojan or other malicious virus.

At the same time, APP downloading is also a common way to be infected. The main characteristic of smart phone is that the users could freely install the software, games and other APP, which are provided by the third-party service, to expand the function of the mobile phones. Therefore, many users are keen on downloading or upgrading the APP from the Internet regularly. But most of them are not accustomed to download or upgrade the APP in the official website but in some unknown mobile forums. And the public are usually attracted by some special tittles such as “the latest” or “the crack” and they may take the risk to download the APP without security permission. And finally their phones will be infected by virus.

Because smart phone makers do not have a unified technical standard, and the smart phone operating systems are various, there is not the sound security mechanism in current smart phone areas. As normal users, the public should keep alert all the time. In order to solve the problems, the following suggestions are given in this paper.

Firstly, users should improve their safety consciousness. A lot of virus infections are the results of the user's thin safe consciousness, even some malicious APP is installed by the users themselves. [7]The thin safety consciousness is an important reason why their mobile phones are infected with malicious APP, thus improving the safety consciousness is very important.

Secondly, users should download the APP from the safe and reliable websites. APP downloads are the most frequent action of smart phones, and that action has also become one of the ways of malicious APP infection. .So users should download the APP just from the safe and reliable platform or APP store.

Thirdly, users should carefully accept the permissions required by APP. When the users are installing a new APP, most of them don’t care the permissions required by APP and just click the “agree” option. In fact, most APP can still run normally without the permission required during the process of installing. And some viruses just need some permissions of the phone operating system to run. There is no doubt blindly “Agree” will help malicious APP build running environment and make the system be in danger.

Summary

The paper points out the security threats of mobile phone password protection and puts forward corresponding solutions or preventing strategies. And it has its significance in the following three aspects. For the public, they can acquaint with the security threats of mobile phone password protection in detail which would increase their security consciousness. For the Internet companies who provide products, they can improve the qualities their products and cut the unsafe factors.For the relevant organizations, the security threats of mobile phone password protection possibly are caused from many aspects. For example, The lack of management for renewing SIM cards brings the security threat to the mobile banking. For such special Internet accounts, management of communications operators, the defects of mobile devices, network products and mobile operation systems are all the reasons. So in order to avoid security threats of Internet account caused by mobile phone password protection, it is necessary to establish joint control mechanism. Companies which provide service, Internet security companies, communications operators, mobile phone equipment manufacturers should cooperate with each other. And the public should also improve their security consciousness and avoid the stealing cases of Internet account caused by mobile phones.

Acknowledgements

The authors would like to give their thanks to Jilin Social Science Foundation (NO.2014B278) and Changchun Institute of Technology for their financial support.

REFERENCES

[1] RK Nema, SN Meyyanathan; CS Sharma. A Practical Approach to Pharmaceutical Analysis, 1st Edition, CBS Publishers & Distributors, New Delhi, **2008**; 89-90.
[2]Bob. Wireless Security[EB/OL].Computing ＆ Electronic Books, **2013**
[3]Markus Jakobsson. The Death of the Internet [M]. Higher Education Press, **2012**
[4]NetQin. The Research of Mobile Phones’ Security in **2013**[EB/OL].
http://wenku.baidu.com/link?url=ju2wUj5eN-QOK
[5]Baidu Encyclopedia. The principle of false base station.[EB/LA]
http://baike.baidu.com/view/8940201.hem?fr=aladdin)
[6]Umeng. China Mobile Internet Market Insight Report Q3 **2012** [EB/OL].
http://wenku.baidu.com/link?url=1BIYJ5DK
[7]Valcout E,Robert Jean. Investigating Mobile payment [C]. IEEE International Conference on Wireless and Mobile computing, Network and Communications, **2005**

[8] Hexun . Marketing Research Report of Mobile banking in 2013［EB/OL]. http: / /bank. hexun. com/**2013** /sjbank / .**2013** [in Chinese]