Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 9 (4): 877-885, 2015
ISSN 1819-4311 / DOI: 10.3923/jse.2015.877.885

Study of Online Accounts Safety and Online Payments by Smart Phones

[1]Yanni Li, [2]Jiayin Li, [1]Zheng Lv, [3]Tianyu Li and [1]Yanling Tang
[1]School of Foreign Languages, Changchun Institute of Technology, 130012, Jilin, China
[2]School of Communication, Jilin Animation Institute, 130012, Jilin, China
[3]School of Software Engineering, Changchun Institute of Technology, Jilin, China

Corresponding Author: Yanling Tang, School of Foreign Languages, Changchun Institute of Technology, 130012, Jilin, China

ABSTRACT

The development of high-tech, smart phones are not only the tools for people to convey information but also a popular guard to protect one's accounts, especially through online payment. But the network of smart phones is not perfect for any operations which deal with money. As it is seen that there are more potential threats when logins or passwords are put into one's smart phone keyboard to get into his internet account. Based on the working procedure of smart phones as the payment tool, this study tries to analyze the security problems of smart phone password from the perspective of M-banking. The purpose is to raise the safety awareness of online banking users and offer some solutions to the banks as well.

Key words: Safety, online account, M-banking, smart phone, database

INTRODUCTION

The online account security problems have always been the critical issues for people and smart phones has been widely used as a protection tool for online accounts recently among all of the password protection measures, because of its simple operation and convenience. But on the other hand, mobile phone password protection is gradually facing security challenges for various reasons. Zhou (2013) identified the factors affecting user adoption of mobile purchase based on trust and flow theory. Park *et al.* (2007) conducted a survey of 221 Chinese nationals by SEM multi-group analysis which showed cultural background is also one of the reasons. While internet banking is coming around the world under big data era, risks are everywhere. A research from Australia tells convenience is the main motivator for consumers to bank on the internet and banks will be better if they can let the consumers understand the learning benefits from the process (Lichtenstein and Williamson, 2006). As all know that trust should be the first in this relationship (Vance *et al.*, 2008). Based on Porter's 5F Model, this study tries to analyze the whole working procedure of smart phones in M-banking which can show the threats coming from different areas, outside or inside the chain.

According to the research data of Netqin, the total amount about stealing cases of online accounts caused by smart phone is over ten thousand from 2013-2014. So it is quite important to explore the real reasons that cause such accidents by logging in the password through smart phones. While there is still increasing number of smart phone users joining in this group, this study analyzes the reasons from the perspective of self-efficacy and perceived credibility and puts forward some suggestions to avoid the risks under the internet era.

MATERIALS AND METHODS

In 2000, ICBC (Industrial and Commercial Bank of China) started its business services by M-banking based on SIM. Smart phone has been used as a password protection tool of online banking for several years. The development of smart phones brings about the development of mobile Internet technology. Various application (APP) software based on phone operation systems are gradually getting into public view. A great number of Internet companies also take smart phones as account protection tool. But different from traditional Internet, smart 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 problem to online accounts. But how do the smart phones work as a payment tool in M-banking system?

From Fig. 1, it is obviously seen that there are outside and inside routines in the whole procedure. The chain is connected by internet no matter it is the public zones or bank systems. So it can be seen that there are similarities and dissimilarities when password from smart phone is applied in two kind of online accounts.

Firstly, the protection process is similar, both for mobile online accounts and traditional online accounts. The users need to authenticate the login or other sensitive operations through verification code which receives from the smart phone text message.

While the platforms used are quite different for traditional online accounts such as Tencent software, the users receive verification code from smart phones and enter it into the computer (Akan *et al*., 2008). But for online accounts through smart phones, all of the operations are based on the phone systems, from which hackers could obtain the verification code through virus based on smart phone system. In other words, this will cause different safety problems between traditional online accounts and accounts from smart phones.

According to Porter's 5F Model, it is obviously seen that in bank network, traditional online account is the biggest competitive rivalry to traditional account in banks. While with the development of high-tech, smart phone becomes the substitute for PC in M-banking, because of its propensity from customers and their dependency upon the existing channels through the functions of smart phones which is shown in Fig. 2.

It is said that smart phone is safer than other online payment methods, because only the reason is after the registration at banks with ID, bank cards and passwords can consumers start their M-banking. During the whole process, transactions are carried out in Data Encryption System

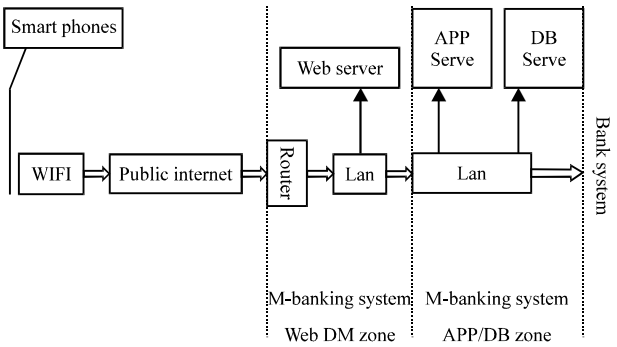

Fig. 1: Working procedure of smart phones as payment tool

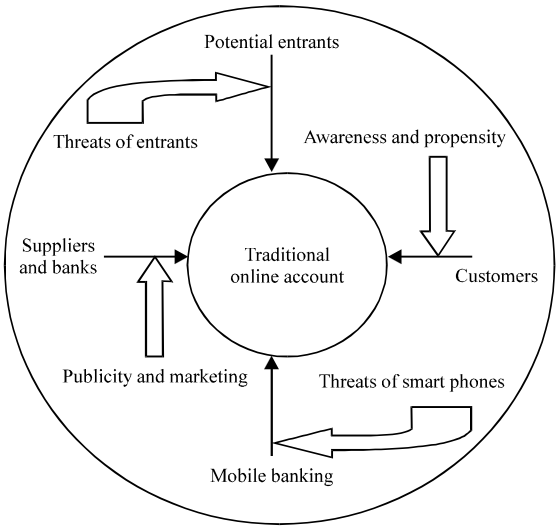

Fig. 2: Analysis of online banking system based on Porter's 5F model

(DES), even the mobile suppliers have no way to decrypt those messages. Besides it is in a very low cost which is 1/7 of the traditional transaction methods.

While it is undeniable that the technology used in this procedure is still developing in its early age, M-banking is running in the virtual environment which rely on internet too much. There are too many types of smart phones with different operation systems. It is hard for the banks to offer the same service to all the smart phones, especially the risks can occur in any steps, from the internet or the operation systems.

Traditional online accounts and mobile online accounts are involved mostly: The principle of 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 the truth is that it's very simple to be broken.

The hackers usually obtain the user's QQ account ID and password through Trojan, then this account will be tracked and monitored by them. When the user logs in the account, the system will prompt users to enter the three corresponding random double-digits in the coordinates and when the user enters the correct matrix digits, the Trojan will automatically record matrix coordinates and the corresponding matrix digits. Then the hacker will fail the transaction by the means of login timeout in order to make the user re-enter another three random double-digits. Over and over again in this way, the hacker could get all of the information of the password protection card. On the other hand, there is no limit about the times of error login at all which would make it easier for the hacker to steal the account.

Because of those flaws among these password protection measures, many Internet companies concentrate on smart phone password protection excessively. The result is that smart phone password protection has the supreme authority among all of the password protections. For example, before July of 2013, any kind of Tencent's three password protections (password protection card, security questions, smart phone password protection) parallels to each other, their authorities are

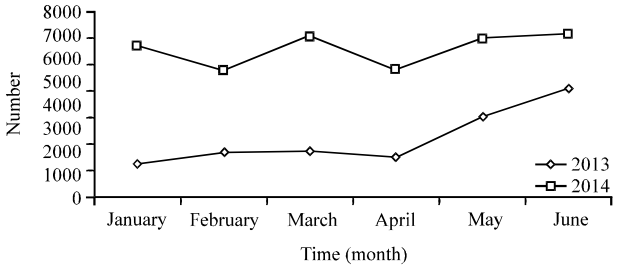

Fig. 3: APP problems shown in 2013 and 2014

the same. First, they can modify the password and authenticate the login and other sensitive operations of the account. Second, they can modify each other. But after July of 2013, Tencent company consciously improve the authority of smart phone password protection. The result is that smart phone password protection could modify the other two password protections but neither password protection card nor security questions could modify smart phone password protection in return. Even in March of 2014, Tencent closed the service of password protection card and suggest all of the users not to use security questions any more.

Although, this kind of action takes some unsafe factors of the two password protections into consideration, it over-raises the authority of smart phone password protection. Once the phone is lost or infected by malicious Trojan, the thieves or hackers can not only retrieve the QQ password through text message but also reset all of the password protections and even bind a new phone number with QQ account. If the users can not change the account numbers through customer service as soon as possible, they would lose the account forever. What's more, since 2013 the phone number bound to QQ account can be used as QQ ID. That means the thieves or hackers could just take phone number as the QQ ID and directly retrieve the password even without the ID information from the QQ client-side. In this way, supreme authority of smart phone password protection increases QQ account security risks.

Besides, smart phone password protection is regarded as the best password protection to all kind of traditional online accounts because of its dual factors' verification. When it needs to authenticate the login, the user will be required to enter both password and the verification code from text message to ensure the safety of the account. Even if ID or password is leaked out, dual factors' verification can block the infringement at any time.

But it is worth noticing that since compatibility problems come up, smart phone password protection couldn't cover all of the login locations. Dual factors' verification only exists in the PC client-side and all kinds of games client-sides but not in mobile client-side, iPad client-side or WAP pages. That is to say, if criminal gets user's QQ ID and password, he can avoid verification code from phone in PC client-side but log in the account through mobile client-side, iPad client-side and some WAP pages to obtain users' personal information. Such flaws are also happening in some online game companies.

Figure 3, research from 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 (Jakobsson, 2012).

Synthetical accounts are always the target of security threats: There are also some security threats from special service items of related products. Alipay can be the best example to explore and analyze the problems and risks in this field.

Security threat of the payment of QR code scanning: Alipay is the representative of the third-party payment platform and payment of QR code scanning is a kind of payment of Alipay. Quick Response (QR) code is just a network link in nature. Scanning the QR code is equivalent to opening a web page or APK download link. The QR code itself does not carry any virus but associated link of the QR codes was added the virus program by hackers. If users carry out the further operations after scanning a QR code with virus, their smart phones would have been infected. For example, the famous Trojan-Stealth thieves made the public cyber citizen suffer great loss in 2013. This Trojan spreads through QR code and it could identify phone numbers and intercept the verification codes from phone text message and send them to the hackers. The general process of its stealing is as followings: Firstly, the Trojan could disguise itself as a QR code and induce the user to download it. Secondly, it could run automatically in the background and send the phone number to the hacker. Then, it could obtain the ID card number though phone number or it could fake a web page and induce the user to enter the ID card number. Next, the hacker can control the victim's phone to retrieve log-in password of Alipay and intercept the verification code from phone text message. Besides, the hacker could retrieve payment password through "ID card number + verification code from phone text message. Finally, the hacker could steal the money from the Alipay account.

Except for Trojan, the QR code crime can occur through the way of fishing. If users open a fake Alipay fishing web page after scanning a QR code and enter some related account information, it also can lead to the loss. It's hard for the public to identify the normal QR code, besides it will open the download pages automatically after scanning a QR code. If the user clicks the download carelessly, the virus could be installed in the smart phone.

Safety problems of fast payment: Security threats of fast payment of Alipay are not from Internet. The criminal could obtain the money from Alipay account without hacking technology. Because of some vulnerability of communication operators, if only one gets the user's ID card number and phone number, he could use a fake ID card to renew the SIM card of the user successfully. The criminal could retrieve log-in password of Alipay through the verification code from phone text message, then retrieve payment password through "ID card number + verification code from phone text message." Finally, the criminal could steal the money from Alipay account.

In fact, the key problem of fast payment is that the phone number could be used as the log-in account. A great number of users take their emails as log-in accounts when they set up new accounts. But in order to make it more convenient, Alipay allows users to take phone numbers as log-in account. That means the criminal need not to spend time to get the user's account number but use the phone number to retrieve log-in password directly.

Security threats of authentication: Alipay belongs to third-party payments in nature. But for an ordinary user, it is more like a kind of online banking or mobile banking. The most obvious difference may be the authentication. If the user of online banking or mobile banking wants to modify or retrieve password, he has to hold his ID card and perform the operation over the banking counter. But there are such real counters in Alipay system, most transactions or other operations are achieved through the authentication of text messages as well as personal information. The security threat of authentication is that once the personal information leaks out and the phone is used maliciously, the criminal could modify log-in password and payment password.

RESULTS AND DISCUSSION

M-banking, as a new field is not studied by many researchers, especially from the angle of smart phones. According to the author's research, there are some articles written from the theory of consumers' attitude (Laforet and Li, 2005; Riquelme and Rios, 2010) or the factors which can influence the users acceptance on information technology (Legris *et al*., 2003; Amin, 2008). Their concerns are on the consumers' behavior and psychology. But this study emphasize the technological problems, especially the threats from different aspects when a user tries his m-banking by smart phones and this should be the key for the wide usage of M-banking in the future. Besides it is undeniable that the convenience and safety should be put into researchers' consideration, so some suggestions are put forward from the whole view of online account security.

From the research of NetQin shown in Fig. 4, it is obvious 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 because they are hidden deeply, it is very difficult to find them for users.

Besides, they are also infected through flash. Some users often take the method of flash to reinstall smart phone system so as to obtain the absolute control over smart 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 the 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 APPs which are provided by the third-party service to expand the function of the smart 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. Public are usually attracted by some special tittles such as "Latest" or "Crack" and they may take the risk to download the APP without security permission. 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 study.

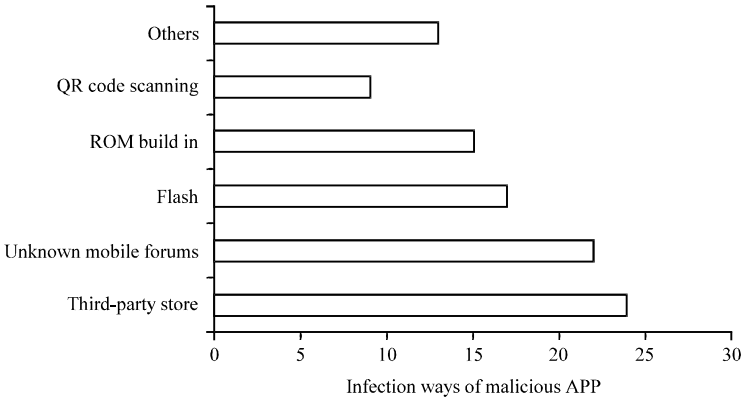

Fig. 4: Main infection ways of malicious APP

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 (Valcourt *et al*., 2005). Lacking of safety consciousness is an important reason why their smart 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 download is 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.

Solutions to the problems: It is well-seen that M-banking business by smart phones is prosperous in China, especially for its large population of smart phone users, so it is quite critical to set up a perfect banking system with the joint effort among the society, government, banks and mobile operators. But the following key points should be put in the first place.

Preventing strategies of false base station's fraud: Preventing strategies of false base station's fraud can be concluded as follows:

- Pay attention to the sudden disappearing signals of smart phones. When the phone can't receive the signals around the markets or banks, there may a false base station is running. The user should watch out for the text message received at that time. "Topics in Focus" of CCTV has reported that, due to the progress of technology, this kind of fraud text messages often copy banks' official ones. The content usually contains the words such as "Warm reminder", "Safety tips" which could reduce people's guard. Especially while receiving some messages which require replying account or personal information, the user must keep alert
- Install the security software. On the one hand, the public users should increase their security awareness, on the other hand, people should make the best use of security software to prevent the SMS fraud of false base station. For example, China Mobile Group Guangdong Company Limited has developed the first security software against the SMS fraud of false base station. The software can effectively identify and intercept illegal text messages
- Choose the safer phone. According to a research of false base station, it is not hard to find out that the majority of victims are the users of China Mobile and China Unicom. On the contrary, there is no related cases reported from Baidu that any user of China Telecom ever was the victim of the SMS fraud of false base station, this is a strange phenomenon. This is because the false base station cannot connect with the CDMA internet of China Telecom. The reason why users of China Telecom haven't been troubled by false base station is related to CDMA technique. So, the CDMA phones could avoid the SMS fraud of false base station more effectively

Solutions to the technology problems: For those important mobile online accounts, the companies which provide products should take some measures to assist the smart phone password protection as following: The study would take mobile banking as the example to analyze.

- Strong password mechanism. Regardless of the computer or smart phone applications, the password mechanism is the most popular means of verification and it is often the first line of defense of the account security (Nathan, 2013). There is no doubt that the low intensity password would be easier cracked and brings the risks. Therefore, mobile banking client-sites should set up the strong password mechanism. The system should forbid the users to set the password as followings: Set the same numbers and letters as password, Set passwords the same as user's bankcard number, account number, ID number, telephone number or cell phone number, Set the user's birthday date including the year, month and day as password. The log-in password, inquiry password and transaction password should be separated in order to strengthen the first line of defense of the account security
- Multiple verification protections. The banks should add Multiple verification measures besides verification code of phone text message such as digital certificate, e-Banking Code Card, the reserved information verification, e-Password Device. At present there is only ICBC (Industrial and Commercial Bank of China) taking e-Password Device and e-Banking Code Card as another verification measures for mobile banking service. e-Password Device's and e-Banking Code Card's verification operations are off the smart phone and that keep the verification from the threat of Internet Trojans effectively
- Behavior analysis verification. Usually every user would have a regular behavior patterns. For example, most people often appear in a certain areas of the city. Even if the user travels on a business trip, it is impossible for him to be another place which is hundreds of kilometers from that certain area within just a few minutes (Tang, 2014). So with the consent of the users, the commercial banks may collect the information such as their smart phone models, smart phone numbers and locations of time periods, IP numbers and error times of password. In this way, each transaction verification will be analyzed be the back end system. Once there are abnormal operations, the back end system should immediately improve the verification level and even terminate the operations. Then the clerk of the bank could contact the user for confirmation. This kind of behavior analysis verification could keep the verification from the threat of Internet Trojans effectively

Improvement of the products: The analysis shows some security threats of smart phone password protection are caused by the products themselves such as the problems of Alipay's authentication and payment of QR code scanning, Tencent QQ's supreme authority and Mobile-Token. The criminals are likely to make use of these flaws to intercept verification code and let users' account in a dangerous condition. So for the Internet companies which provide products or services should pay attention their products' flaw and cut those unsafe factors in time.

Enhancement of security consciousness: For those threats that the present technology couldn't solve such the problems of flash, smart phone operation systems or for those threats that occurs for the flaws of the softwares themselves, the users should acquaint with those deep and keep alert and enhance their own security consciousness.

CONCLUSION

In this study security threats of smart phone password protection have been put forward clearly and analyzed the whole process that how threats work usually and the solutions or preventing strategies are listed at the end of the discussion. It is quite significant for the public users, because

awareness or alert should be arisen when they use their smart phone as the tool of payment while there are so many potential threats around them. Besides, Internet firms should improve their services on online products they offer to the users and avoid unsafe factors in the whole usage. While there are still other reasons which can cause the risks, like lack of management for renewing software and hardware led to the threats of mobile banking. So a joint management system from all the parties should be set up to dec7.

ACKNOWLEDGMENTS

The authors would like to give their thanks to Jilin Social Science Foundation (No. 2014wy23) and Jilin Education and Science Institute Program (GH14307) for their financial support.

REFERENCES

Akan, O.B., P. Frossard, Q. Zhang and N. Jayant, 2008. Special issue on wireless multimedia sensor networks. Comput. Networks, 52: 2529-2531.

Amin, H., 2008. Factors affecting the intentions of customers in Malaysia to use mobile phone credit cards. Manage. Res. News, 31: 493-503.

Jakobsson, M., 2012. The Death of the Internet. Higher Education Press, Canada, ISBN-13: 9781118312537, pp: 45-47.

Laforet, S. and X. Li, 2005. Consumers attitudes towards online and mobile banking in China. Int. J. Bank Market., 23: 362-380.

Legris, P., J. Ingham and P. Collerette, 2003. Why do people use information technology? A critical review of the technology acceptance model. Inform. Manage., 40: 191-204.

Lichtenstein, S. and K. Williamson, 2006. Understanding consumer adoption of internet banking: An interpretive study in the Australian banking context. J. Electron. Comm. Res., 7: 50-66.

Nathan, B., 2013. Wireless security. Comput. Electron., 1: 24-26.

Park, J.K., S.J. Yang and X.R. Lehto, 2007. Adoption of mobile technologies for Chinese consumers. J. Electronic Commerce Res., 8: 196-206.

Riquelme, H.E. and R.E. Rios, 2010. The moderating effect of gender in the adoption of mobile banking. Int. J. Bank Marketing, 28: 328-341.

Tang, D., 2014. Introduction to strategy development and strategy execution. Flevy Business Primer, October 21, 2014. http://flevy.com/blog/introduction-to-strategy-development-and-strategy-execution/.

Valcourt, E., J.M. Robert and F. Beaulieu, 2005. Investigating mobile payment: Supporting technologies, methods and use. Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications, Volume 4, August 22-24, 2005, Montreal, Canada, pp: 29-36.

Vance, A., C. Elie-Dit-Cosaque and D.W. Straub, 2008. Examining trust in information technology artifacts: The effects of system quality and culture. J. Manage. Inform. Syst., 24: 73-100.

Zhou, T., 2013. An empirical examination of the determinants of mobile purchase. Pers. Ubiquit. Comput., 17: 187-195.