ATLANTIS PRESS

Advances in Computer Science Research (ACSR), volume 73

7th International Conference on Education, Management, Information and Computer Science (ICEMC 2017)

Research on Security and Protection of Users' Privacy Information in Mobile Social Network

Wen He[1, a] and Tao Huang[1, b*]

[1]Chengdu medical college, Chengdu, Sichuan, 610500, China

[a]hewen41731@163.com, [b]1804280@qq.com

*The corresponding author

Keywords: Privacy Information; Security; Protection; Mobile Social Network

Abstract. With the rapid development of mobile network technology and the popularity of intelligent terminals, the scale of mobile social network users continue to increase, making personal information security and privacy protection as mobile social network users generally concerned. This paper gives a simple classification of the personal information of users in the mobile social network, analyzes the status and causes of personal information disclosure in mobile social networks, and puts forward some protection countermeasures and suggestions.

Introduction

With the rapid development of mobile Internet, the widespread use of mobile devices, the rapid rise of social applications, a variety of mobile social applications have emerged, to provide users with a variety of personalized services, for example, people can keep in touch with friends and family through social applications, at any time to share their feelings or life, find nearby friends, and playing games and entertaining with strangers, etc. With LBS, interest, address book and other functions, mobile social applications meet the needs of user communication, sharing, service and entertainment, and become an effective way for users to expand their circle of friends and meet new friends [1].

According to the China Internet Network Information Center (CNNIC) released the 38th China Internet Development Statistics report shows that as of June 2016, the size of Chinese Internet users reached 710 million, of which the scale of mobile phone users reached 656 million, accounting for 92.5% of the total number of Internet users, Internet users equipment further concentrated to the mobile terminal. At the same time, the number of users who use mobile phones, tablet PCs and other mobile devices for social activities is growing rapidly, and users of various types of social applications gradually increased, as of June 2016, WeChat friends circle, QQ space and microblog usage were 78.7%, 67.4%, 34%[2]. With the convenience and fast new experience, the reality and the virtual highly coincide, mobile social applications provide users with a wealth of personalized services. However, while users enjoy mobile social services, personal information security issues have become increasingly prominent. According to a survey of more than 13000 adults in 24 countries or regions conducted by the Symantec Norton Company in 2012 showed the new network crime are turning to social network or mobile device network[3]. The "Norton Cybersecurity Insights Report" released in 2015 [4] shows that about 594 million of the 17 countries surveyed have been attacked by the Internet in the past year. In emerging markets, China is one of the countries with the most serious attacks on cybercrime. In 2016, Tencent United Security Laboratory released "2016 Annual Cyber Security Report" [5] shows that the number of Trojan viruses in 2016 continued to rise, mobile phone infected users up to 500 million, a record high. Once the virus into the mobile phone or mobile terminal, it may steal the user's address book, SMS, social accounts, bank accounts and other important personal information, resulting in user privacy disclosure, to the user economic losses. The rapid development of mobile Internet has changed the way people live and communicate, to provide people with a lot of convenience, however, the risk of Internet users' information disclosure has also increased.

Mobile social network has the characteristics of mobile, localization and socialization [6], due to

the network can be provided to the user's many business, making mobile social network there are a variety of personal information, Such as the personally identifiable information that the user has filled in when registering the mobile social app; the location information generated by the user when using the LBS service; the personal financial information of the bank card, credit card, electronic wallet account and password involved in the use of mobile payment; user's social relation information in social network, etc. At all times, massive user data is aggregated in mobile social networks, and once user data is compromised, it can have serious consequences. So, how to effectively protect the user's personal information in mobile social networks is a valuable research topic.

This paper classifies the personal information in the mobile social network, which is divided into four categories: identity information, location information, personal financial information and social relations information, the concept and connotation of each type of information are briefly described. Based on the research reports provided by some authoritative security institutions both at home and abroad in recent years, this paper analyzes and summarizes the reasons for the disclosure of personal information in mobile social networks, and puts forward some protection countermeasures and suggestions, hoping to provide a reference for the protection of personal information in the mobile social network.

Classification of Users' Personal Information in Mobile Social Networks

Identity Information. In the mobile social network, the identity information is the basis for the user to obtain the service. When the user registers the mobile social application, it needs to submit the relevant personal information such as the name, the mobile phone number, the mailbox, etc., the more realistic the more personal information can make Users get the more real social experience, but at the same time the greater the risk of user privacy disclosure.

Location Information. In recent years, location-based services (LBS) are widely used in mobile applications, which use mobile phone location technology to obtain the user's location to provide the appropriate services, such as: road navigation, online take-away, online rental car, etc. brought great convenience to life. In mobile social applications, location sharing, location based games (LBG), and nearby strangers dating and so on all need to use the user's location information, modern social life more and more inseparable from location-based services, more and more location information are provided to the service provider, if the user's location information is leaked, it may pose a threat to the user's personal and property security.

Personal Financial Information. Personal financial information mainly refers to the user in the social network using mobile devices to pay the relevant information, including bank accounts and passwords, electronic wallet accounts and passwords, payment records and so on. Most of the social applications have mobile payment function, when the user transfers money to a friend or interactive entertainment with friends will inevitably use this information, but once the user has scanned the two-dimensional code sent by a person who posing as a friend, the phone may be implanted Trojan virus program, so that the user's personal financial information theft and brings great economic losses to the user.

Social Relations Information. Social relationship information refers to the chain of relationships between users and users in mobile social networks. Mobile social network based on the user's real interpersonal relationships, through the virtualized social networking platform for communication, sharing and dissemination of information, in the process of interaction between users, criminals can infer the its social relationships through the logs posted by users on an open platform and other users' comments, once the user's social relations information disclosure, the criminals can pretend to students, friends, relatives, etc. to implement its precise fraud.

Analysis of Personal Information Disclosure of Mobile Social Network Users

According to the research reports provided by some authoritative security agencies both at home

and abroad in recent years and the research literature published by relevant authors, this paper analyzes and summarizes the reasons for the leakage of personal information in mobile social network from three aspects: service providers, users and the overall security environment of mobile networks.

Personal Information Leakage Caused by Service Providers. Through research show that the disclosure of personal information caused by service providers may be via the following two approaches:

(1) The application cross-border to access the personal information

Cross-border collection of personal information means that the application collects the personal information which the user is not authorized or beyond the functionality of the service [7]. Due to some important information of the user, the photos will often exist in the phone, if some applications cross-border to obtain the appropriate permissions, you can freely access the contacts, read the message, view the album, or even view the user's bank card password, etc., caused the user privacy disclosure. According to the "China Android Phone Privacy Security Report 2015" released by Data Center of China Internet(DCCI) shows that 11.9% of the Android mobile phone APP cross-border to get the privacy permissions, in which "read location information" and "access Contacts" to become the most cross-border access to the two major privacy permissions. In the social communication software, the cross-border of "send messages" permissions are the most serious, 7.0% of the social communication software did not have the send SMS related functions but called this permission. The permissions to send text messages are used illegally or maliciously, which may consume the user's telecommunications charges, resulting in economic losses [8]. The ecological environment of IOS system is relatively safe because of the closed system, but there are also have the phenomenon of mobile applications cross-border access the privacy data. Such as many mobile social applications read the user's mobile phone address book in the name of social, or read the user's photo album in the name of providing the picture download function, which results in the disclosure of the user's privacy information [6].

(2) Social platform data leakage

Users in the social platform for social activities, due to communication, sharing needs, will be registered to provide a lot of real-name information, such as name, phone number, picture, etc.. In order to enable users to get more personalized service and convenience fast and new experience, the social applications developed more and more additional features, such as: online shopping, mobile payment, social games, sports data management, users use these features need to authorize the social applications to obtain their own corresponding privacy information, such as location information, identity information, bank card account password information. With the increasingly powerful social software features, the use of social software more and more people, the social platform itself to master the user privacy data is also more and more, if the lack of reasonable supervision and effective management, there may occur the social platform to disclose the users' privacy situation[9]. In addition, social platforms may be due to technical vulnerabilities, hackers attack, causing the user information to be theft, resulting in disclosure of user privacy information.

The Personal Information Disclosure Caused by the User Own. Through the investigation and study found that the user's own lack of privacy protection awareness, unsafe mobile phone use habits and lack of the basic knowledge of information security are also the main reasons for the disclosure of personal information.

(1) The user lack awareness of privacy protection

The concept of mobile social is communication, sharing, display and discovery, compared to traditional social, mobile social will be incorporated the user's mobile phone real-name attributes, contact attributes and location attributes and other real information into it, for users to create a virtual social networking platform with a highly correspond of realistic social, greatly reducing the cost of trust between users, while mobile social break the constraints of time and space, so that users can publish log anytime, anywhere to share their photos, videos, location, mood, life status,

etc., to strengthen the contact between friends. Because of the convenient use, the "sharing and displaying" in the circle of friends has become one of the main activities of users on the mobile social platform. However, in the user's sharing and display, may contain a lot of privacy information, such as photos, video, personal information and the user's location information, etc., users share at the same time will be some of their own privacy information exposed. In addition, the comments between friends on the social platform are also easy to become the mining objects of people who have ulterior motives, which make it possible to understand the user's social relations information and some important information inadvertently leaked by other users in the comments.

Although the mobile social application provides users with some privacy control options, such as setting personal data access permission, spatial access permission, comments view permission, etc., due to lack of privacy awareness, some users ignore the privacy settings, so that the user data open to everyone, resulting in user privacy disclosure.

(2) User's mobile phone security habits

In some cases the user's information disclosure is also associated with their own mobile phone security habits, according to Tencent released the "2016 Mobile Security Report" shows that 38% of mobile phone users have multiple accounts share the same password situation, the other 20% of users use a simple combination of letters to set the password[10]. This password setting policy with security risks posed a great threat to the personal information security of the users, hackers can more easily to crack the user's password, steal the user's application account and then get its account and password in other applications. The user's social account are stolen with great harm, in addition to access to the user's many important personal privacy information, criminals can also log on the user's account to implement precision fraud to the user's friends.

In addition, studies have shown that a considerable number of users do not use the mobile terminal keyboard lock and password and other privacy control function, once the user's mobile terminal is lost, the user's personal information is easy to be leaked[11].

Open location positioning allows users to get geographically personalized services, and many users are accustomed to turning on location positioning, which poses a risk to the user's location information disclosure. The criminals can obtain the user's location information by continuously attacking the location server, once the user's location information can be obtained by the criminals at any time, they can infer the user's home address, workplace, hobbies, health status, etc., leading to some of the user's important privacy leaked.

(3) Users lack the knowledge of mobile phone information security protection

Users in the installation of mobile phone applications, some mobile applications will apply to the user to obtain the user's privacy privileges, such as: read contacts, read call records, read location information, open the camera and so on. Most of these privacy access permissions apply to a functional requirement for the application, but there are some applications that do not have the relevant functional requirements but cross-border to read the user's privacy information, because the user does not have the professional knowledge of mobile application authority management, and also unclear whether the privacy authority that the application obtained is necessary for the function, so it is directly authorized, leading to these applications cross-border to obtain the user's privacy information, resulting in personal information disclosure.

Public Wi-Fi With the development of mobile Internet has been gradually popular in people's daily lives, but many users do not understand the possible harm of accessing unsafe Wi-Fi [12]. Because public Wi-Fi networks are usually not password protected, this allows an attacker to access the mobile phone through any device on the network, intercepting data transmitted by the mobile phone over the network, thereby stealing the user's personal privacy information. According to Tencent released "2016 mobile phone security report" shows that 72% of users will use public free Wi-Fi on the phone, of which 64% of users connect to public Wi-Fi for web browsing, the use of social communication tools, 7.5% Of users will also pay online, which makes the user easy to disclose their personal information in the process of surfing online [10].

The Security Environment of the Mobile Network. According to the Cheetah Mobile Security

Laboratory released the "2016 Network Security Research Report" shows that Android mobile phone virus for four consecutive years of rapid growth, in four years Android malware increased by 16 times, mobile phone malware detection rate from 6% in 2013 to 2016 in 29%, nearly one-third of the new Android software was detected malicious behavior, While the proportion of phishing sites spread through social tools exceeded the search engine for the first time in 2016 [13],The security environment of mobile network is not optimistic. Criminals through mobile phone fraud, fishing links, etc. to trick users to install the mobile phone applications which contain Trojan horse program, once the user phone infected with the virus, it will spread to the circle of friends. Malicious software by controlling the user's mobile phone, steal the user's text messages, contacts, location, mobile banking and other privacy data, leading to the user's important privacy information disclosure, and even bring economic losses.

Countermeasures for Personal Information Security Protection of Mobile Social Network Users

Through the analysis of the causes of personal information disclosure in mobile social networks, this paper puts forward some protection countermeasures and suggestions from the government level, the service provider level and the user level:

The Government Level. Aim at the protection of personal information in mobile social network, this paper argues that the government level should improve the laws and regulations on the protection of personal information security of mobile social networks and make clear the responsibilities of service providers in collecting and utilizing personal information, to require the service provider to explain to user the use of information collection, scope and information utilization, etc. Through legal means to regulate the industry to collect and use the user's personal information behavior, make a clear definition of illegal acts of infringement to the user's personal information. For the illegal sale and use of personal information of enterprises and individuals to punish the law, so that the user's personal information security by a comprehensive legal protection.

In addition, this paper argues that the Government should establish a third-party security review authority, perform security audits for mobile applications, and evaluate the degree of privacy protection for mobile applications; only through the security authentication software can enter the app store. Through the mainstream media and a variety of information dissemination channels to guide users in the formal application store to download application software, cultivate the user's privacy awareness and the ability to identify the risk of privacy disclosure. Receive feedback and report of personal privacy information disclosure, monitor large-scale information leakage events, analyze the reasons for the investigation, and give guidance.

The Service Provider Level. The formulation and improvement of laws and regulations may lag behind the development of Internet technology. Therefore, this paper argues that an industry self-discipline association should be set up between mobile social service providers, which is responsible for the formulation of industry standards and standardizing the behavior of service providers, and members within the association should consciously abide by the provisions of industry associations and to accept supervision and evaluation. Rely on industry associations' self-discipline, should prompt service providers at least do the following aspects:

1) For user data collection, open and transparent, to protect the user's right to know and the right to choose, clearly inform the user what needs to be collected for social applications, what is the use, whether to provide to third parties, whether to agree to authorization, etc. [14], do not cross-border to collect user information, and do not use user information for other purposes other than social applications, add the user's personal information confidentiality clause to the user agreement.

2) Ensure the user's personal data security, using advanced data encryption technology to encrypt the user's account, password, identity information, bank card number, password and other important privacy data which stored in the server, to prevent hackers through the attack server to obtain the user's privacy information. Using the location protection technology to protect the user's location

information and prevent the attacker from obtaining the location or track information of the user through the attack location server.

3) Attach importance to the privacy protection settings of users on the social platform, allowing users to set a variety of levels of privacy access permissions, and on the social platform to popularize information security, fraud prevention and privacy authority management of the basic knowledge. Enhance the user's privacy awareness; improve the user's information security literacy.

4) Develop content review techniques and analyze filtering methods[15-16] to identify unsafe links and malicious programs on social platforms to prevent viruses or phishing links spreading on social platforms. For users in the social platform published some may involve sensitive privacy of the pictures or information, should promptly remind the possibility of information disclosure risk, prompting it to delete as soon as possible.

The User Level. At the user level, this paper argues that users should enhance the awareness of privacy protection and improve the user's information security literacy. In the use of mobile social networks, users should pay attention to the following aspects:

1) When using mobile applications, carefully read the user protocol for mobile applications, identify what user data will be collected and what is the purpose. Take the initiative to learn the knowledge of APP authority management, prohibit APP cross-border to access the user's privacy data.

2) Improve privacy protection awareness, when publishing logs on social platforms, pay attention to privacy protection, do not release your sensitive privacy information. Carefully turn on the mobile phone location positioning function, after using the location-based services, promptly closed positioning. Pay attention to setting privacy access permission, do not easily add strangers as friends.

3) Pay attention to setting a higher security policy password, do not set the same password on multiple social platforms, regularly change passwords, and use mobile security software to scan the virus.

4) Form healthy online habits, do not access the unknown source or unknown security WIFI, in the case of uncertainty, do not easily click on the URL link or file, do not scan the source unknown two-dimensional code.

5) From the formal application store to download APP, to avoid downloading a malicious program with Trojan viruses, third party plugins or unsafe code, causing privacy leaks or economic losses to the user.

6) Use mobile phone security software to manage and protect the phone, regularly update the system and repair system vulnerabilities, regular security checks on the phone, killing the virus.

Summary

This paper discusses the classification of personal information in mobile social network, analyzes the reasons for the disclosure of personal information in mobile social networks from three aspects of service provider, user and mobile network security environment, and puts forward some suggestions on how to protect the personal information security of mobile social network users. Overall, the protection of personal information of mobile users at the present stage requires both the improvement of national laws and regulations and the collaborative cooperation of industry associations, service providers and users themselves. Only by converging all parties forces and making joint efforts can achieve the effective protection of the personal information of users, in order to promote the healthy and orderly development of mobile social industry.

Acknowledgement

This work is supported by Web Culture Project Sponsored by the Humanities and Social Science Research Base of the Sichuan Provincial Education Department (No.WLWH15-26).

References

[1] CNNIC. China Social Application User Behavior Research Report 2015 [EB/OL]. [2016-04-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/sqbg/201604/P020160722551429454480.pdf.
[2] CNNIC. The 38th China Internet Development Statistics Report [EB/OL]. [2016-08-03]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/P020160803367337470363.pdf.
[3] S.Y. Wang and N. Zhu. Research on the Privacy Protection of Mobile Social Media Users [J], Information Studies: Theory & Application, 2013, 36(7):36-40.
[4] Norton by Symantec. Norton Cybersecurity Insights Report 2015[EB/OL].[2015-11-24].https://us.norton.com/cyber-security-insights-2015.
[5] Tencent United Security Laboratory.2016 Annual Cyber Security Report [EB/OL]. [2017-1-20]. http://slab.qq.com/uploads/file/20170119/20170119095514_66827.pdf.
[6] X.L. Xu, The Research on the Problem and Protection of Mobile Social Network User's Privacy Security[D], (MS., Chongqing University, China 2014), p.6-20.
[7] X. Gong, The Security Research of the Personal Information Based on Mobile Internet [D], (MS., Huazhong University of Science & Technology, China 2013), p.25.
[8] DCCI. China Android mobile phone Privacy Security Report 2015[EB/OL]. [2016-1-20]. http://vdisk.weibo.com/s/sRCXj0VHA7O.
[9] T.Z. Qin, Suggestions on privacy protection for mobile social network users [J]. Computer Knowledge and Technology, 2016,12(27):36-38.
[10] Penguin Intelligence. Mobile phone security report 2016[EB/OL]. [2016-7-29]. http://tete.qq.com/a/20160729/004715.htm#p=1.
[11] N. Wang and D.C. Xu. The Investigation and Analysis of Personal Information Protection in the Mobile Social Network—from the Perspective of User Behavior Habits [J]. Journal of Intelligence, 2015,34(1):185-189,194.
[12] CNNIC. Investigation on Network Security Status of Chinese Mobile Phone Users 2015[EB/OL]. [2016-10-12]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/ydhlwbg/201610/P020161002016101249427.pdf.
[13] NYSE:CMCM. 2016 Network Security Research Report [EB/OL]. [2017-2-13]. http://cn.ccmc.com/news/security/2017-02-13/92.html.
[14] C. Qin. Privacy Protection in Big Internet Era [J]. Software Engineering, 2012,(5):10-12.
[15] J. Sun, X.Y. Zhu, M.M. Liu and P. Bi. On Security and Privacy in Social Network Service [J]. Network Security Technology & Application, 2011,(10):76-79.
[16] J.Y. Yang, X.X. Ye, S.C. Chen and J. Li. Security Problems in the Social Network Set and Their Solutions. Netinfo Security, 2014,(4):82-87.