International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 7, July 2015 **ISSN 2319 - 4847**

Analysis of Information Security in Social Network Sites and their Solutions

ZHU Zhenfang

School of Information Science and Electric Engineering,Shandong Jiaotong University, 250357,Jinan,China

ABSTRACT

As a newly emerged application in the internet, the social network sites have developed very fast in recent years. Represented by Facebook, Youtube and Renren, the social network sites have millions of users now. It created a new way of communication. Meanwhile, it brought about new information security issues such as identity theft, privacy leak and junk information, etc. This paper starts with introducing the basic concept, features and functions of the social network sites; then it analyzes the cause of the threats to users' privacy, the relevant damages and their common attack means; at last, it proposes solutions to some typical security problems on social network sites.

Keywords: social network sites, information security, privacy protection

1. FOREWORD

The social network sites serve as a medium and platform for the people to communicate and exchange information, express and share their feelings. In recent years, the rapid development of the social network sites is quite impressive and the number of the users has been soaring up. According to the statistics, the page view of the American social network Facebook is second only to Google-the largest website in the world. While in China, born in 2009, Sina Microblog's registered users grew to over a hundred million over the past few years. From the above information, it is easy to see that the social network sites built a complete system for social activities and sharing information for their users in the virtual world. With the increase of the users and diversified functions on the websites, the social network sites are getting out of the restrictions of virtual internet and generate significant and wide influence on their users in the real world.

However, while we are enjoying the convenience and happiness brought by the social network sites, more and more negative impacts occur. As the number of users enlarges, the social network sites are prone to breeding cyber-crimes. The security reports of Microsoft issued from July 2010 to December 2010 indicated that the phishing scam in social network sites increased by 1200% in 2010. Phishing refers to the behavior utilizing malicious links with legal covers to induce the user to buy junk software or leak personal privacy. Such stunning statistics remind us: even in virtual internet, careless may harm our real life. When the users feel the convenience of the social network, more attention has to be paid to the information security. Because once a user fills in his personal information, the social network site recommends your friends in real life or you share your pictures, address and personal living habits in the friends' circle, the leak of this information will bring bigger harms. Hackers faking their identities with the users' information or spreading spams and malware to users, such cases happen frequently.

As for the users, actions like preventing worm attacks, carefully filling personal information, being cautious while adding friends can prevent the leak of personal information to some extent. However, the prevention from the users cannot guarantee the information is 100% safe because many social network sites are developed with security vulnerabilities.

For instance, some websites are attacked by worm virus due to adopting Ajax technology. They will automatically send links with virus to the user's friends. Other users will be attacked by the virus once they click the links. Some website use permanent valid cookie to keep the users online. Such improper behavior contains huge threat because once the hacker steals the cookie information; he/she can do anything in the user's identity. In order to prevent and solve the information security issues while the users are surfing the social network sites, it is necessary for us to understand the mechanism and functions of the social network sites and seek solutions on the basis of the analysis on the occurred threats.

2. GENERAL DESCRIPTION OF SOCIAL NETWORK

In order to solve the information security problems of the social network site, we have to learn about the basic concept and structure of the social network site and the associated social network. The SNS (Social Network Service) in internet area normally refers to: Social Network Service, Social Network Software and Social Network Site. Obviously, these three things are correlated with each other and indispensable; they are combined to make up the platform for users to communicate information and exchange feelings.

The social network theory is based on the famous Six Degrees of Separation which was put forward by an American luminary in Social Psychology Mr. Milgram in 1960s. The basic content is "Everyone is six or fewer steps away, which means, by way of introduction, from any other person in the world, any two people can be connected in maximum six steps".

As the time goes and the technology keeps renovating, the functions of the preliminary social network founded on simple communities are improving and going toward globalization. The current social network integrates the previous functions like contacting friends, sharing photos and blogging. In addition, it gives more attention to the openness of the platform and obtaining of the third party's application program. It is certain that the social network service we are using now has gone far beyond the basic concept "a friend of a friend" at the beginning; it becomes more real and multi-functional. This is why the crisis of personal information security we are facing becomes worse. The more open the platform is, the more dangerous our privacies are. Thus, we have to bear larger risks of information leak and the solutions will be more complicated.

3. SECURITY OF SOCIAL NETWORK

3.1 Brief on Security of Social Network Sites

When security vulnerabilities exist in the website itself, they can lead unimaginable damage to the security of the users' information. For example, most of the security vulnerabilities existed in the well-known Kaixin website are caused by loose website filtering which gives hackers opportunities to input malware through the security vulnerabilities so as to obtain the account information of the website administrator. With the account, the hackers can modify the web page and add malicious code via the back-stage of the website. When the users view the page, the viewing will be automatically redirected to other website or start download Trojan Virus. Meanwhile, as more and more users access to internet through mobile phones, the security issues become worse. A great number of users encounter phone communication being intercepted, message and information of contact persons being stolen, attacking by virus while downloading audio or video files.

3.2 Analysis on the Security of Social Network Sites

The security issues of social network platforms not only associate with traditional computer network security, but also contain different features from the traditional computer network. Therefore, they face various threats in their actual applications. At present, the threats can be divided into two groups: traditional security threats and threats arisen from date mining techniques.

3.2.1 Traditional Security Threats

The traditional security threats can be classified as follows:

1) Communication of Spams

The traditional spams are normally communicated through emails, mainly including different kinds of commercial advertisements and malicious links. In Social Network Sites, through pushing to users' friends, such junk information are spread among wider scope and extended in a faster speed in the internet.

2) Third Party's Software and Plug-ins

Like other platforms, social network sites also provide free open interface to application programs. Any user can develop embedded program according to his needs. While providing convenience to users, such interfaces contain huge hidden risks.

3) Disrupt System Availability

Through increasing network load, redirecting user requirements and damaging network data, the hackers can affect the network property and system service so as to steal the user's information.

4) Steal User Name and Password

This is the most traditional attack which can also cause biggest damage. The theft of the user name and password means all the user's personal information in the social network site are exposed to the hacker. Thus, the hacker can do anything without being discovered in the user's identity.

3.2.2 Security Issues Arisen from Date Mining Technique

Data mining technique can be classified as follow:

1) Digital Files Collection

When the registered users' information on the social network sites are leaked, unlawful hackers may collect and settle a complete file for the full information of the users and sell it to seek benefits.

2) Operation Data Collection

Apart from the personal information filled by the user and publicized messages, the social network sites also include some network operation data, for example, the users' login and logout time, IP address, friend list information, chatting

record and shared information between the user and his/her friends .etc. All these information can be used to position the user's geolocation, identity characteristics or push other information to the user's friends.

3) Face Recognition

Many social network sites encourage or request the users to upload their real photos for identification while registering. If the hackers can easily cross access to the information and behaviors of the same user on different social network sites through face recognition system, obtaining more personal information and filing the complete data of the user will be much easier.

4) Tagging Image Data

Some social network sites provide with image tagging functions to the users. For instance, tag some location on the map, record when and why the user going to this location, or tag the third person on a group photo, record the name, identity or other information of the third person. The users may leak his personal information and put others' information in danger unconsciously.

4. TYPICAL PROBLEMS AND SOLUTIONS

In the following chapter, the author analyzes the security problems of social network sites and solutions with clickjacking as an example.

3.3 General Description of Clickjacking

Clickjacking technique, also referred to as UI redress attack, is a kind of web session attack for the purpose of cheating. The main attack idea is to utilize the users' lack of security technology knowledge and induce the users to a click malicious link without realizing it.

The attack principle of clickjacking is that the hackers use inframe as the carrier of the target web page while realizing the clickjacking vulnerability. Inframe is a tag of HTML standard which can create another web page inframe. The main function of inframe is to load target webpage during the application of clickjacking vulnerability. Hereafter are some examples to illustrate the principle of clickjacking:

1)The hacker creates a web page and use inframe to load it onto the target website (Twitter);
2)The hacker hiddens the target website to make it unable to be perceived by the users of the browser;
3)The hacker builds web page and tricks the users to click specific button;
4)The victim clicks on the button which will execute the order of Twitter web. Then the homepage of the user will publicize the malicious information carefully designed by the Hacker and send this information to the user's friends.

3.4 Harms of Clickjacking Technique

The harms of clickjacking mainly include:

1)Send spams: for example, using social network sites like microblogs to automatically send spams.
2)Information leak: such as leak of video chatting or phone chatting contents, documents stored online and emails .etc.
3)Malicious operation, such as automatically logging in the remote desktop and sending sensitive messages, buying junk goods and dialing other user's number on the phone. etc.
4)Set up network devices, for example, maliciously set up the parameters of network devices, modify or counterfeit the users' passwords, set up network firewall so as to break the security mechanism.

3.5 Analysis on the Defensive Approaches to Clickjacking

Defensing clickjacking vulnerability can be considered from the following two aspects: server end defense and customer end defense. Server end defense mainly involves the validation of users' identities, while the customer end defense concentrates on the security of the browsers.

3.2.3 Defense Clickjacking at Server End

The defense against clickjacking vulnerability at server end shall combine with the security mechanism of the browsers. The main defense approaches includes:

1) **X-FRAME-OPTIONS Mechanism**

The new generation of browser Internet Explorer 8.0 issued by Microsoft proposed a brand new security mechanism X-FRAME-OPTIONS for the first time. This mechanism has two options: DENY and SEMEORIGIN. DENY means any web page could not use inframe to load web pages. While SEMEORIGIN means web pages comply with SOP (same origin policy) can be loaded through inflamed. While the browser is loading the website with such security mechanism, if any suspicious behavior is discovered, the browser will remind the users that the viewing webpage contains potential risks and advise the users to open the webpage in a new window in order to prevent the hackers hiding target webpage through Inframe.

2) **Frame Busting Code**
The precondition of clickjacking is to load the target website into malicious website. Using Inframe to load the webpage is the most efficient way. In accordance with the features of inframe, the researchers proposed Frame Busting code and using java script to prevent the malicious website loading web pages. If the webpage is found to be load by malicious web page, the system will execute automatic jumping function. However, if the users prohibited java script in the browser, the Frame Busting code will be useless. Therefore, this approach is unable to provide comprehensive security protection.

3) Validate Users with Verification Code
Clickjacking vulnerabilities make attacks through faked webpage. While the website developer can identify the user via verification code to confirm the click order is from the user himself, then execute the corresponding operation. The most effective way to identify the users is verification code. But the weakness of this method is quite obvious. The users think such operation is too complicated and most of the users dislike such kind of user interfaces. The target of the research on this approach is how to balance and unify the security and simple operability.

3.2.4 Defense Clickjacking at Customer End

The security mechanisms associated with the customer end can help prevent the clickjacking code executing at the customer end. Defense approaches at customer end mainly include:

1) Upgrade Browsers
The latest browsers offer many security mechanisms against clickjacking vulnerabilities. So far, the latest versions of all the browsers support the relevant clickjacking defense program. Thus, what the users need to do is to update the browser regularly and repair the vulnerabilities of the browser. In this way, the malicious attacks will be prevented effectively.

2) NoScript Extension
As for users of Firefox, using NoScript extension can detect and prevent clickjacking attacks to some extent. NoScript is a plug-in of Firefox browser. Its main function is to shield malicious scripts in the webpage and prevent the attacks from script virus and XXS code. Meanwhile, the clear-click software in NoScript is able to detect and warn the potential clickjacking attacks and automatically detect the unsafe webpages in the website. However, at the same time, the false rate is pretty high so that the users need to make judges while viewing on the browser.

3) Improve Security Awareness of the Users
The users shall not make random click and input important personal information on the unsafe and untrusted websites. Do not authorize third party software to login with the accounts of the social network sites. Remember to close the webpage in time after viewing.

5. CONCLUSION

This paper starts introducing the basic concept, features and functions of social network, then it further analyses the precondition of the popular security problems existed in social network sites; after that, it gradually explains the cause and impact of these security problems, it also gives a basic thought to solve the security problems of the social network sites and outlines the necessary basic properties for a sound social network site. At last, the paper introduces two kinds of typical defense approaches which are applied to the social network sites currently.

From the above contents, we can clearly feel the complexity and gravity of the security problems on social network sites. Certainly, the final solutions cannot be realized by a single area or approach. Apart from technical innovation and integrated development, the user itself also plays an essential role.

6. ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

Reference

[1] Wang liang. Current situation and trend of the SNS social networking [J]. Journal of modern telecommunication technology, 2009, (6): 9-13.
[2] Fogel J, Nehmad E. Internet social network communities : Risk taking, trust。 and privacy concerns J-J]. Computers in Human Behavior, 2009, 25(1) : 53.
[3] Valter F E, Battiston S, Schweitzer F. A model of a trust based recommendation system on a social network[J]. AutonomousAgents and Multi-Agent Systems, 2008, 16(1) : 57.
[4] Sun Jian, Zhu Xiaoyan, liu Momeng, etc. Privacy research to social network security [J]. Journal of network security technology and application, 2011, (10) : 76-79.

[5] Kim Youngae, Phalak Rasik. A trust prediction framework in rating-based experience sharing social networks without a Web of Trust[J]. Information Sciences, 2012, 191(5) : 128.
[6] Westerman D, Spence RP, Van Der Heide B. A social network as information : the effect of system generated reports of connectedness on credibility on Twitter[J]. Computers in Human Behavior, 2012. 28 : 199.
[7] Wu Huxin, Wu Bo, zhang Ming. Social networks risk's influence on the national information security [J]. Contemporary spread, 2010. (01) : 75-76.
[8] Zuo Shuguang, Lin Xi. Chinese SNS website development problems and countermeasures analysis [J]. Journal of southeast, 2009, (10) : 29-26.

AUTHOR

ZHU Zhenfang , PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc.. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year