International Journal of Computer Networks and Applications
Volume 1, Issue 1, November - December (2014)

SURVEY ARTICLE

A Survey of Various Security Issues in Online Social Networks

M. Milton Joe
Assistant Professor, Department of Computer Application,
St. Jerome's College, Nagercoil, Tamilnadu, India
m.miltonjoe@gmail.com

Dr. B. Ramakrishnan
Associate Professor, Department of Computer Science and Research Centre,
S.T. Hindu College, Nagercoil, Tamilnadu, India.
ramsthc@gmail.com

Abstract – The most emerging communication medium for the last decade of years is Online Social Networks (OSNs). Online Social Network makes the communication quicker and cheaper. Facebook, Twitter, Google Plus, MySpace, Orkut, etc are the various existing online social networks. Among all the online social networks very few could turn the attention of the people towards them. However, all these social networks are available on the publicly accessible communication medium called internet. When these social networks are available in the internet, it will lead to various types of security issues. This paper discusses the various security related issues persists in online social networks.

Index Terms – Online Social Network (OSN), Privacy, Security, Hacking, Malware, Hacking, Spam, Attack.

1. INTRODUCTION

The most unbeatable technology internet brings all the people together to exchange messages with one another [1]. Internet is the easiest way to stay connected with people and it is the cheapest communication medium for quickest communication [2]. The growth of internet technology found social networks to exchange ideas, thoughts, interests, activities and so on [1, 3, 4]. There are many social networking websites such as Facebook, Twitter, MySpace, Orkut, Google Plus exist but very few are mostly used by the people all over the world. Users of online social networks must need an E-Mail address to create the profile to start the communication process with others [2, 3]. Once the user profile is activated the users will be provided with the communication interface to start the communication with one another. The users active in online social networking media have crossed more than one billion [3, 5, 6]. Among the users of OSN platform most of the users make use of the mobile devices to access their user profile [2, 7]. The total number of users exist in each social networking platform are listed below [2, 8]:

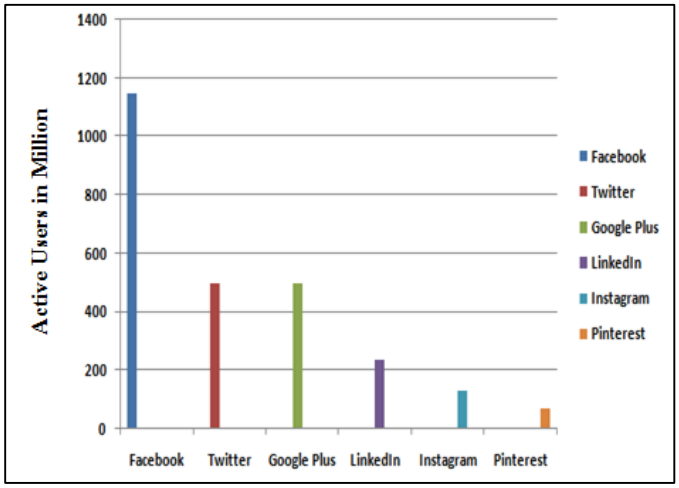

Figure 1 Total Number of Users in Various Social Networks

From the Figure 1 it can be identified that Facebook application has more number of users than the other social networking applications. Another interesting thing must be reviewed here is who are the users of social networking web applications. The most of the users of social networking web application are youngsters.

2. BEHIND ONLINE SOCIAL NETWORKS

The present social network applications are used by the young people of this generation. Facebook application is the one which is mostly used by the internet users. Users create user profile in OSN applications with and existing E-Mail id. Once the user profile is created, the users can post their real images, personal information such as E-Mail id, Phone numbers, and home address and so on. They can post their day to day activities, life style, what they like and don't like and even users are tagging their present location in online social media. This

SURVEY ARTICLE

shows very clearly that all the information about the people are most probably publicly available in online social networking applications.

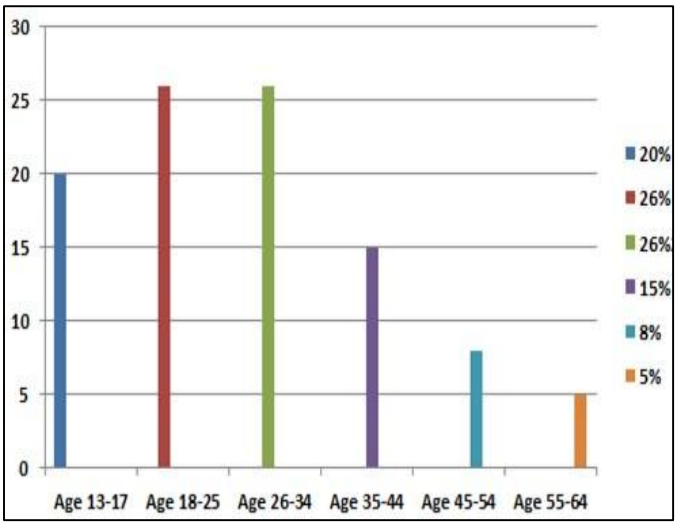

Figure 2 Online Social Network Users Age wise.

The Figure 2 shows the users of online social network applications age wise. From the Figure 2 it can be identified that people between the ages 18 to 34 are mostly using the online social networks. In online social network applications all the people's sensitive information and their real images are publicly available. The question is: is it safe providing all the information in online social networking websites? What are the security issues behind the online social networks? Users those who are aware of security issues can set up various security parameters in social networking application. The fact is most of the users are unaware of security settings available in the OSN application and their unawareness makes their personal information available as public. That is, the users can restrict the viewers from looking their personal information. However, this privacy setting is not an ultimate solution because the hackers will hack the personal belongings in various ways.

3. SECURITY ISSUES

3.1. Users' Anonymity

Almost all the users of online social network applications make use their real name as the profile name. Hence, users' name is publicly available on social media and all the social media are indexed in the search engines [9]. People are losing the job opportunities since the employer the review the OSN profile of the particular candidate [10, 11]. When the attacker search victim name in the search engine, the attacker will lead to the particular user profile. Hacker can obtain all the possible information of the victim through the social networking websites [9].

3.2. Profile and Personal Information

Social network users almost provide their real name and sensitive information on their profile such as full name, contact information, date of birth, relationship status, education details, present and previous work locations [9]. These kind of sensitive information available on social network provides all the needed information to the hackers. These basic and sensitive information available as public to all the users of social networking web applications. Most of the users set their privacy settings as public. This unawareness of the privacy settings available in the user profile makes all the personal and sensitive information available to all the users. Though privacy setting is set as private still the details can be obtained by the hackers by employing various attacks [9]. Third party applications become popular among the users of online social networks. When the users make use of the third party application for ease of access to their social network profile, they have to agree to allow the third party application to access the personal information of the particular user profile [12]. In such a way the personal information of the user is transfer to another third party application domain [12].

3.3. Image Tagging

Users of online social network can tag the images with full name, E-Mail address and even they can provide the link to their OSN profile. This tagged image can be accessible to the friends of friends and even to public. Hence, this image tagging provides the information about the particular user to others users which can be used by the hackers for nuisance activities.

3.4. Image Hacking

Every day many real images are posted in each user's profile. Some of the photos are available as public because unawareness of the privacy settings. Most of the real images are viewable to the friends and friends of friends. These real images can be hacked in various ways as listed below:

- Dragging the image [2]
- Right Click and save as image [2]
- Snipping tool in windows OS [2]
- Print Preview and save [2]
- Combination of keys like Ctrl+A, Ctrl+S [2]
- Temporary Internet Folder [2]
- Print Screen [2]

Hence there is no security to the images posted on the social networking websites. Hackers can easily hack the real images of the particular user and those photos can be misused widely for nuisance activities.

3.4.1. Dragging the Image

Once an image is posted in online social media the image open to the hackers to drag and save the image. The attacker can

SURVEY ARTICLE

easily drag the image to the desired location to save the image. No security measures are applied to the images posted in social networks.

3.4.2. Right Click and Save as Image

When right click event is pressed on any image, the image will pop-up with the list of options. Among the list of displayed options on choice is right click and save as image. Using this option the attacker can save the photo to his/her computer without any difficulties. This right click option is open in all the social networking websites which shows that there is no security to the images posted on social network application.

3.4.3. Snipping Tool in Windows OS

The advanced version of windows OS has the special feature known as snipping tool. This tool can be used to cut and store any image which is visible on the screen of the system. Hence, this tool can be used to cut and store the images posted on the social media.

3.4.4. Print Preview and Save

When the image is visible on the social networking web applications the attacker can go for print preview option. When print preview option is activated, the print preview of the current web page is displayed. In the displayed preview page there is option known as save as pdf. Using this option the attacker can save the page as pdf and later the hacker can crop the image as he/she wishes.

3.4.5. Combination of Keys

The shortcut keys such as Ctrl+A is used to select the entire current webpage. Once the entire page is selected, the attacker can easily copy and paste the page to the desired location and the image alone then can be separated. Similarly the key combination Ctrl+S is used to save the web page to any location of the client machine. When the current page is saved, all the content of the page is available on the folder where it is saved. The hacker can easily take the image alone from the saved folder.

3.4.6. Temporary Internet Folder

Every computer system has a folder known as temporary internet folder. When a webpage is loaded for the first time the multimedia content of the page is stored in the temporary internet folder. When the same page is loaded again the page is loaded from the temporary internet folder. New content of the page is alone loaded to the client machine from the server. Actually this folder does not store the content temporarily. As long as the user deletes the content of this folder manually, all the contents are available inside the folder itself. All the images of the social network users are available inside temporary internet folder. Hackers can obtain the photo and it can be misused widely.

3.4.7. Print Screen

All the computing system has the feature known as print screen. Using this option the user can capture the present web application and store it in the desired location. Hence, the hacker can easily hack the images on the social networking sites using print screen option.

Hence, there is no security to the users' real images posted on the social networking websites.

3.5. Fake Profile

When the particular user's entire personal information as well as real image is available in social media, it is easily for the hackers to obtain those details. Once the sensitive information as well as photos are hacked the attacker will create the fake profile with those details. The name of the particular original user can be damaged completely the victim will be under trouble forever because of fake profile. Through this fake profile the attacker can add the friends of the victim to his/her circle and their personal information also can be hacked.

3.6. Social Phishing

Social Phishing is the way of attack used by the attackers to obtain the sensitive information of the victim. In this attack the hacker will provide a fake website which will look like a real website. Attacker will send the message to the victim that you have to authenticate your profile otherwise your profile will be deleted. When the victim visits the particular fake website it will prompt the user to enter the sensitive information and username and password of the victim. Most of the time the attacker is successful because of unawareness of the users.

3.7. E-Mail Spam Attack

In this attack the hacker will get the E-mail address of the victim and forward the spam mails to the users. Most of the users keep their E-Mail is available public in social media and the attacker can easily identify it. If the user keep their e-mail id as private the e-mail id can be guessed with the victim first and last name. Most of the social networking websites offer friend search through e-mail. The attacker can easily obtain the details easily from these features offered by the social networking sites.

3.8. Malware Attack

Malware attack become famous among social networking users. Attacker will send the malware injected code to the victim profile. Once the user click the malware URL false information will be posted on the victim wall. Other type of malware is, as soon as the victim click on the URL the user will be redirected to the fake website where the victim will be asked to enter his/her sensitive information. Similarly by clicking the malware the URL a client side code will be installed on the victim system to steal the information stored on the machine.

SURVEY ARTICLE

3.9. Sharing Day to Day activities

Users of online social networking have the habit of sharing their day to day activities among their friends. For instance consider the following post. “Hi I am moving the beauty parlor alone”. These kind of posting gives the clue to the kidnappers. Then the kidnapper is very well aware where the victim is going and who are all with the victim. These kind of sharing present ongoing activities online will lead to a security threat to the users especially to women.

3.10. Gathering Social Data

Monitoring the victim in social media the attacker can come to know, in which thing the victim is interested and what does the victim like. Based on the information gathered on the victim profile, the victim will get the marketing advertisement and shopping offers. Here the user privacy is completely degraded.

3.11. Deleting the User Account

When the user wants to delete his/her profile forever, he/she cannot delete the account completely. Though the account is deleted, the content posted by the user on another user’s profile will be available on social networking websites forever. User cannot delete his/her communication on the social media forever.

3.12. Physical Threat

An active user of online social network provides the sensitive information online such as E-Mail, Contact phone number, and home address. These kind of giving the physical identify to the attackers, they may ring up a call to the victim and send unwanted e-mails to the victim mail account. This will be a physical threat to the victim forever.

4. CONCLUSION

Online social networking applications are mostly used by all the people in and around the world. Most of the time of a day is spent in online social networking applications. However, the users of online social networks are unaware of the security issues do exist in OSN platform. There are various security issues which steals the sensitive and personal information of a user. This paper illustrates the various security issues available in online social networks. The future direction of the research will be modelling effective security algorithms to defend the security issues exist in online social networks.

REFERENCES

[1] M. Milton Joe, Dr. B. Ramakrishnan, Dr. R.S. Shaji “Prevention of Losing User Account by Enhancing Security Module: A Facebook Case”, Journal of Emerging Technologies in Web Intelligence, Vol. 5, No. 3, August 2013, Page No: 247-256.

[2] M. Milton Joe, Dr. B. Ramakrishnan, “Enhancing Security Module to Prevent Data Hacking in Online Social Networks”, Journal of Emerging Technologies in Web Intelligence, Vol. 6, No. 2, May 2014, Page No: 184-191.

[3] http://en.wikipedia.org/wiki/Social_networking_service

[4] Mohamed Shehab a, Anna Squicciarini b, Gail-Joon Ahn c, Irini Kokkinou “Access control for online social networks third party applications” Elsevier- Computers & Security 31 (2012) 897 911.

[5] Facebook, Facebook Statistics, March 2011. <http://www.Facebook.com/press>.

[6] Twitter, Twitter Numbers, March 2011. <http://blog.twitter.com/2011/03/numbers.html>.

[7] Facebook, http://en.wikipedia.org/wiki/Facebook

[8] www.socialnetworkingwatch.com/all_social_networking_statistics/

[9] Dolvara Gunatilaka,” A Survey of Privacy and Security Issues in Social Networks”, http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html.

[10] J. Flesher. How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. In The Internet Engineering Task Force, 2006.

[11] A. Fuller. Employers snoop on Facebook. In The Stanford Daily, January 2006.

[12] Balachander Krishnamurthy and Craig E. Wills, “Characterizing Privacy in Online Social Networks,” WOSN '08 Proceedings of the first workshop on online social networks, 2008, pp. 37-42.

Authors

Mr. M. Milton Joe received his B.Sc Computer Science degree from St. Joseph’s College affiliated Bharathidasan University, India and MCA degree from Anna University, India. Presently he is working as Assistant Professor in department of Computer Applications at St. Jerome’s College in Nagercoil, India. He has three years of research experience and authored eleven research papers in reputed international journals. His research interests include Web Security, Web Communication, Vehicular Network and Social Network Security.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 26 years. He has twelve years of research experience and published more than twenty five international journals. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.