

Survey on Threats in Social Networks

R.Ramana^{1#}, B.Bensujitha^{2#}

Department of Computer Science and Engineering[#]

Kalasalingam Academy of Research and Education[#]

rramanabtechcse.21@gmail.com¹, bensujitha@gmail.com²

Abstract:-The majority among the communication technology for many years is Online Social Networks (OSNs). Online Social Network makes the communication easier and instant reply. It has the ability to connect with other people, all over the world. The various Social Networks include Twitter, Facebook, LinkedIn, Google+, Youtube, Pinterest, Instagram and Tumblr. Amongst them very few are most popular to reach the attention of the people. However all are available public, they can be accessed by a common medium called Internet. When these are accessible through the Internet, the people may need different kinds of safety measures. In this paper, we discuss about various types of security issues and how they are used to protect the Online Social Networks.

Keywords: Online Social Network, Social Networking Sites, safety measures, hacking.

1. Introduction:

The Internet is not synonymous with World Wide Web. The Internet is a massive network of networks, a networking infrastructure [1]. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. There are many Social Networking Sites include Twitter, Facebook, LinkedIn, Google+, Youtube, Pinterest, Instagram and Tumblr. Users of online social networks must need an E-Mail address to create the profile to start the communication process with others. Most of the users make use of the mobile device to create their own profile.



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:

Facebook is the main network applications that are mostly used by the internet users. The users create their own user profile in OSN applications with and

existing E-Mail Id. Once, the user profile is created, the user can post their own activities, their real images and their own personal information. The users can tag their own present location by using Online Social Media. All the informations are publicly available in Online Social Networking applications.

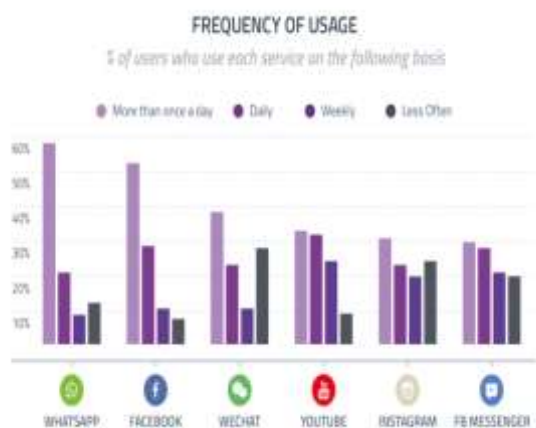


Figure 2 Online Social Network Users Age wise

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.

The users important information are available publicly so, then what are the security issues to be handled to keep these all users information to be secured[1]. Users can be aware of some security measures in which they can set up. This will help their users to restrict their own personal information from other users.

3. Security Issues:

3.1 USER'S ANONYMITY:

This enables to track users before they register with your site, that we can present personalized content to an anonymous user over multiple sessions. It persist information about a user's behavior, provided cookies are enabled on the user's browser. This feature can be parameterized to exclude those who spend less than a designated period of time on your site, avoiding the expense of storing data on irrelevant users. Finally, a tracked anonymous user

choose to register with your site, the data collected on that user is persisted in the account of the newly-registered user.

3.2 PROFILE AND PERSONAL INFORMATION

The users using the social network will provide their own personal information about their name, address, date of birth and their own location. This will help the hackers to get information about our own details. This will be present as public to all the social media users. Though the users will set their own private settings, the hackers will reach our information by performing various attacks. The hackers will use the third party application to access the personal information of particular user profile.

3.3 IMAGE TAGGING

The Online Social Network users can tag their images with their own profile. This will be viewed by their own friends, friends of friends, and even to public. Hence, this image tagging provides the hackers particular information about other users.

3.4 IMAGE HACKING

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]

Hackers can easily hack the real images of the particular user and those photos can be misused widely for nuisance activities.

3.5 DRAGGING THE IMAGE

The hackers can easily drag the images to the desired location and also can save the images for various purpose activities. No security measures are given.

3.6 SNIPPING TOOL IN WINDOWS OS

The snipping tool is the special feature in advanced OS. This tool is used to cut and store images. The hackers can use this tool to cut and store the images which are posted publicly on the social media.

3.7 PRINT SCREEN

The print screen is one of the important feature in the computing system[3]. Using this feature they can print our images on the place where they are going to use it for some activities. The right click option is mostly used for this option.

3.8 FAKE PROFILE

When the users information is available publicly, the hackers can provide the fake profile of one's social users. The images can be dragged and dropped to the particular location of where the hackers want.

3.9 SOCIAL PHISING

Social Phising, which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party[4]. 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.

3.10 E-MAIL SPAM ATTACK

The hackers will hack the E-mail address of the social users. The attacker can easily obtain the details easily from these features offered by the social networking sites.

3.11 MALWARE ATTACK

The hackers can form a hostile or intrusive software including computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs. Attackers can send this type to hack the social users personal information's.

3.12 TEMPORARYINTERNET FOLDER

Every computer system has a folder known as temporary internet folder[3]. When the same page

is loaded again the page is loaded from the temporary internet folder. 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.

3.13 GATHERING SOCIAL DATA

Based on the information gathered on the victim profile, the victim will get the marketing advertisement and shopping offers[5]. Here the user privacy is completely degraded.

3.14 DELETING THE USER ACCOUNT

The user can delete their own account or profile completely[5]. Though the account is deleted, the hackers having our own personal information can operate our account without knowing the social users.

4. Conclusion:

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.

5. 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] J. Flesher. How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. In The Internet Engineering Task Force, 2006.
- [4] A. Fuller. Employers snoop on Facebook. In The Stanford Daily, January 2006.

[5] 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.