ISSN 2278-3091
Volume 3, No.1, January – February 2014
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://warse.org/pdfs/2014/ijatcse02312014.pdf

CONTENT FILTERING ON SOCIAL NETWORKING SITES

Prof. G.N.Purohit (Dean, AIM &ACT), Banasthali University, Jaipur, Rajasthan, gn_purohitjaipur@yahoo.co.in

Dr. Priti Singh (HOD, ECE), Amity University, Gurgaon, Haryana, psingh@ggn.amity.edu

Mrs. Praveen Dangi (Ph.D*), Banasthali University, Jaipur, Rajasthan, praveenchoudhary09@gmail.com

ABSTRACT

A social networking service is a platform to build social networks or social relations among people. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Web-based social networking services make it possible to connect people who share interests and activities across political, economic, and geographic borders.
This paper presents the security risks of online social media networking system.

Key Words *:* Vulnerability, Social Networking Sites, Security, Privacy.

I. INTRODUCTION

The Social Networking Sites (SNS) are gaining a lot of popularity these days with almost all of the educated youth using one or the other such site.

These have played a crucial role in bridging boundaries and crossing the seas and enabling them to communicate on a common platform. Figure 1 shows Social Networking websites are often designed to fit a certain type of community such as the college community being mirrored by Facebook.com.

Figure 1. Social Networking Sites

There are also many potential threats to privacy associated with these SNS such as identity theft and disclosure of sensitive information. However, many users still are not aware of these threats and the privacy settings provided by SNS are not flexible enough to protect user's data. In addition, users do not have any control over what others reveal about them. Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information. In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Privacy on Social Networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes. Users also provide security for Image Filtering. When an image

is acquired by a camera or other imaging system, often the vision system for which it is intended is unable to use it directly. The image may be corrupted by random variations in intensity, variations in illumination, or poor contrast.
Filtering: transform pixel intensity values to reveal certain image characteristics
Enhancement: improves contrast
Smoothing: remove noises
Template matching: detects known patterns

For the Next generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information.

2. CHARACTERSTICS OF SOCIAL NETWORKING SITES

Social networking websites provide rich information about the person and his network, which can be utilized for various business purposes. Some of the main characteristics of social networking sites are:

- They act as a resource for advertisers to promote their brands through word-of-mouth to targeted customers.
- They promote the use of embedded advertisements in online videos.
- Users can play games, take fun quizzes, share photos and ideas with friends in social networking sites.

3. OBJECTIVE

The basic objective of this research is to study the vulnerability of social networking sites with respect to security for image filtering, emails and Web Browser.

4. SOCIAL NETWORKING SITES

4.1. Facebook

In Face book, the users can easily access links to either log out, access the home page, or alter their privacy settings. Thus, users are typically aware that privacy settings can be altered because the privacy settings link is highly visible. Once inside the privacy settings page, a user is given simple options in drop down menus that guide the user into choosing the desired privacy settings. A user must be part of a specific network (e.g. college, high school, city, organization, etc.) in order to browse / search the individuals that are a part of that network. Easy access to the privacy link, the straight forward ability to change one's privacy settings, and the limited ability to globally search are all positive aspects that help guard users' information from users in other networks. Facebook.com was launched in 2004 with the intent to connect U.S. college students, starting with Harvard College. In its first month, over half of the 19,500 students signed up. After gaining popularity, Face book opened its registration to non-college students, and in 2008, Face book surpassed MySpace as the leading social networking website.

4.2. Myspace.com

Myspace.com offers similar privacy setting restrictions as Facebook.com, the web site has a more ambiguous privacy settings link that is less obvious for users to access. As seen in the pictures to the left, there is no word 'privacy' anywhere on the homepage. The link 'account settings' sends the user to another page with the link "privacy settings." Myspace.com does allow users to change their settings, but it is not user friendly.

4.3. Frienster.com

Users can only alter the default privacy settings(Figure 2) of this online social networking by clicking the obscure 'settings' link in the top right hand corner of the website's home page. Moreover, only 10 percent of user profiles on friendster.com accessed during our study had altered the privacy settings to prevent us from contacting these users, thus supporting our conclusion that access of privacy settings is relatively unclear.

Figure 2. Vague Privacy Setting

Further, the default privacy settings are not very restricting, allowing third parties to message users and view their information in the absence of privacy awareness. It is also unclear as to which default settings should be altered in order to fully prevent this invasion of privacy to occur.

5. MINIMIZING VULNERABILITY OF SOCIAL NETWORKING SITES

Every user on a social networking site can choose to reveal their personal information using a range of attributes. We divide these attributes into two sets, individual and community attributes. Individual attributes (I-attributes) characterize individual user information, including personal information such as gender, birthdate, phone number, home address, group memberships, etc.

Community attributes (C-attributes) characterize information about friends of a user, including friends that are traceable from a user's profile (i.e., user's friend list), tagged pictures, wall interactions, etc. These attributes are always accessible to friends but may not to the other users. A user vulnerability depends on visibility and exposure of a user profile through not only attributes setting but also his friends.

5.1. Individual Attributes

Individual Attributes includes personal information or user information such as birth date, phone number or any other information. But if the user can use these information to secure their account then the vulnerable friend can easily hack their account, because these are very common things that vulnerable friend and any other person can easily know user birthday, phone number, address, so the user can use some discrete things so that no one can easily find out or hack other user account and that should be secure or minimizes vulnerability.

5.2. Community Attributes

Community Attributes characterize information about friend and also including those friends who are in user's friend list. They trace their information, pictures, and also wall interactions. Vulnerable friend can easily hack other people information. The information you post on the Internet is available to almost anyone who is clever enough to access it. Most thieves need just a few vital pieces of personal information to make your life a nightmare and if they successfully steal your identity. So to minimize this vulnerability, user and who are in user's friend list provide some security so that another people who are not user friend can't see or open their data.

6. CONCLUSION

Social networking websites is also one of the social media tools which can be used as a tool in education industry to generate on line traffic and a pipe line for new entrants. The use of these websites is growing rapidly, while others traditional online is on the decrease. There are vulnerable friends on social networking sites and it is important to find and unfriend vulnerable friends so that users can improve their privacy and security. Unfriending vulnerable friends from a user's social network can significantly decrease the user's social utility. In this paper, we study the novel problem of vulnerability reduction with social utility loss constraints.

7. FUTURE WORK

While the internet does introduce significant security risks, if policies and controls are designed appropriately, information security can be enhanced. Our long-term objective is to focus on various privacy barriers in SNS and suggest methods to overcome these barriers. The means for achieving this objective would be by developing an agile framework for privacy design that would combine the negotiations and conflict resolution strategies. This privacy framework will help in making the social networking sites more secure.

REFERENCES

[1].Ateeq Ahma.. **International Journal of Advanced Computer science and Applications**, Vol. 2, No.2, February 2011.

[2**].** P Gundecha, H Liu . **Minimizing user vulnerability of social networking sites, public.asu.edu**, .Dec 2012.

[3].Lenhart, A; & Madden. **privacy & online social network, http://www.danah.org/papers/JCMCIntro.pdf** ,2007.

[4]. Rosenblum, D., **The Privacy Risks of Social Networking Sites** , IEEE Security and Privacy, Vol. 5,Issue 3, pp. 40-49, May 2007.

[5]. Ellison, N.B; Steinfield, C; & Lampe, C. **The benefits of Face book "friends:" Social capital and college students' use of online social network site**, Journal of Computer-Mediated Communication.Vol 12, Issue 4.july 2007.

[6].Hak J. Kim. **Online Social Media Networking and Assessing Its Security Risks**, International Journal of Security and Its Applications Vol. 6, No. 3, July, 2012.

[7]. Rosenblum, D. **What Anyone Can Know: The Privacy Risks of Social Networking Sites**, IEEE Security and Privacy, Vol. 5,Issue 3, pp. 40-49, 2007.

[8]. Ellison, N.B; Steinfield, C; & Lampe, C. **The benefits of Face book "friends:" Social capital and college students' use of online social network sites**, Journal of Computer-Mediated Communication.Vol 12, Issue 4, 2007.

[9].Boyd, D; & Ellison, N. B. (2008). **Social network sites: Definition, history and scholarship. Journal of Computer--Mediated Communication**, Vol 13, Issue 1, pp. 210--230.

[10].E-Mediat**. Privacy, social media policy** ,http://www.bethkanter.org/privacy-security/

[11]. Aboulhamid, M; Sevillano, J. **Computer Systems and Applications**, IEEE/ACS International Conference on Computer Systems and Applications, Vol 4, Issue 2, 2009.

[12].Luo, W; Xie, Q; and Hengartner. **Facecloak, privacy technique for social networking sites** , IEEE International Conference on Privacy, Security, Risk and Trust. , pp.26-33, 2009.

[13]. Jones, S; O'Neill, E.**Feasibility of structural network clustering for group-based privacy control in social networks**, ACM, Vol 5, Issue 1, pp. 38-40, 2010.

[14].Leenes, R..**Sociality and Privacy in Online Social Network Sites,** Springer Boston, vol 320, pp. 48–65, 2010.