Threats of Online Social Networks

Abdullah Al Hasib

Islamic University of Technology, Gazipur, Bangladesh

Summary
In the recent years, we have witnessed a dramatic rise in popularity of online social networking services, with several Social Network Sites (SNSs) such as Myspace, Facebook, Blogger, You Tube, Yahoo! Groups etc are now among the most visited websites globally. However, since such forums are relatively easy to access and the users are often not aware of the size and the nature of the audience accessing their profiles, they often reveal more information which is not appropriate to a public forum. As a result, such commercial and social site may often generate a number of privacy and security related threats for the members. This paper highlights the commercial and social benefits of safe and well-informed use of SNSs and emphasizes the most important threats to users of SNSs as well as illustrates the fundamental factors behind these threats. It also presents policy and technical recommendations to improve privacy and security without compromising the benefits of information sharing through SNSs.

Key words:
Online Social Network, Privacy, Profile squatting, Identity threat, Image Tagging and Crossprofiling.

1. Introduction

The advent of the Internet has given rise to many forms of online sociality, including e-mail, Usenet, instant messaging, blogging, and online dating services. Among these, the technological phenomenon that has acquired the greatest popularity in this 21st century is the Online Social Networks or Social Networking Sites (SNSs). For the past few years, the number of participants of such social networking services has been increasing at an incredible rate. These Online Social Networks are the network spaces where the individuals are allowed to share their thoughts, ideas and creativity, and also to form social communities. These online networks provide significant advantages both to the individuals and in business sectors. Some of the noteworthy benefits of online social networks are:

- Enable the people to stay connected with each other very conveniently and effectively, even on an international level. The connectedness and intimacy developed through this social networking might contribute to increased self-esteem and satisfaction might life for some students [1].
- Allow the like-minded individuals to discover and interact with each other.
- Provide a forum for new modes of online collaboration, education, experience-sharing and trust-formation, such as the collection and exchange of reputation for businesses and individuals.
- In the business sector, a well-tuned SNS can enhance the company's collective knowledge and engage a broad range of people in the company in the strategic planning process.

Since the success of an SNS depends on the number of users it attracts, there is pressure on SNS providers to encourage design and behavior which increase the number of users and their connections. However, the security and the access control mechanisms of SNSs are relatively weak by design as the security and privacy are not considered as the first priority in the development of SNSs [2]. As a result, along with the benefits, significant privacy and security risks have also emerged in online social networking [3] as well as the study of SNSs' security issues has now become an extensive area of research.

The aim of this paper is to provide a useful introduction to security issues in the area of Social Networking. In this paper, we have examined some of the most important threats associated with Social Networking Sites and figured out the primary reasons behind these threats and finally based on that, we have provided some recommendations for action and best practices to reduce the security risks to users.

The remainder of this paper is organized as follows. Section 2 summarizes the related works in the privacy and security of online social networks. Then some of the major threats in social network have been elaborated in terms of vulnerabilities and risks in Section 3. Section 4 represents discussion and several recommendations for enhancing the privacy and security of SNSs. And finally, the paper is ended with the conclusion at section 5.

Manuscript received November 5, 2009
Manuscript revised November 20, 2009

2. Related Works

The popularity of the concept of online social network has been increasing since 1997. As a result, in the recent years, social networking has gained intense media attention. Also the academic studies in different fields such as the ethnographic and sociological approaches to the study of online self-representation have started to appear [4, 5, 6].

In addition to that, there have been significant research works on the security issues of online social networking. Analyzing the privacy relevant behavior and privacy risks on popular online sites are of prime concern now. In article [7], the author has studied online social network users to determine the users' attitude towards the Social Networks (SN). The study has revealed the fact that the users normally tend to reveal a variety of information including their name, age, gender, address, photos etc using their profile and some of them tend to hide, fabricate such information as well. Figure 1 describes the types of information revealed by the users and the status of the revealed information.

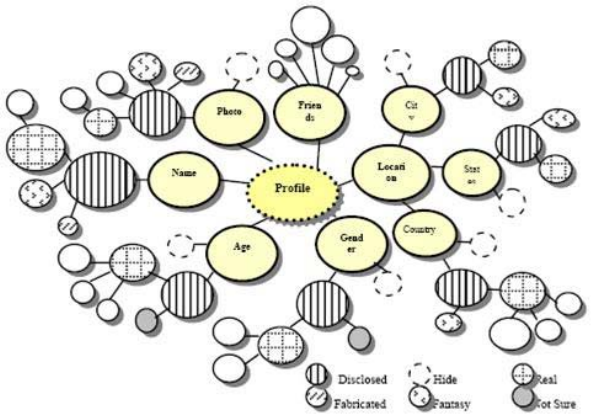

Figure 1: An overview of personal information disclosure [7]

The information that is available in the users' profile can be searched based upon different criteria and thus can also be accessed by the strangers. Most of the people tend to expose real identity information; thus it raises privacy and security issues. Unfortunately many users are not aware of this. The kinds of information users tend to reveal and corresponding percentage are also studied in the article [7] and the result is represented in Table 2:

- Almost half of the participants disclose all elements of their personal information.
- More than a quarter of users hide both their age and gender.
- People who hide some of their identity elements have fewer friends.
- Women are more likely to hide their location in comparison to men.
- People who fabricate their identity are less likely to use a fantasy location and they have the most friends.

Table 1: Combination of classified identity elements

Name	Age	Gender	City	State	Country	Friend	Total	%
D	D	A	D	D	D	159.1	6680	48.9
D	H	H	D	D	D	80.52	2251	16.4
D	H	H	H	H	H	32.55	58	0.42
D	D	M	H	H	D	127.5	740	5.42
D	D	F	H	H	D	101.1	842	6.16
Fb	D	A	R	R	R	182.6	168	1.23
Fb	D	A	Fn	Fn	Fn	40.06	6	0.04
D	A	D	A	H	U	114.6	227	1.66
D	A	D	A	H	O	124.1	3005	22.0

D=disclosed, H=hidden, R=real, Fb=fabricated, Fn=fantasy, A=all, M=male, F=female, U=USA, O=other countries

In a separate study of Facebook users done by Gross and Acquisty reveals that 71% of the Facebook users have the tendency to provide large amounts of sensitive personal information such as image, bithdate, in their profile that expose themselves to various kinds of security risks [8]. In a research on Human Computer Interaction (HCI), Wenday Mackay has shown that only a minimal percentage of users tend to change the default privacy preferences which are highly permeable [9].

Also a number of new methods and strategies have been proposed in different scientific studies to mitigate the risks associated with this information revelation. In [10], the authors have developed a novel face de-identification algorithm that can limit the ability of automatic face recognition software by removing identifying information while presenting other aspects of the face such as gender, ethnicity and expression. However, such methods have not been deployed to the social networks yet.

3. Threats of online social networking

The casual posting of personal information on a digital medium might create a permanent record of the users' indiscretions and failures of judgments that can be exploited by the third-party commentary to produce a number of threats to the users. The potential threats that the users might face can be broadly categorized in four groups: Privacy related threats, SNS variants of traditional network and information security threats, Identity related threats and Social threats. In the following subsections we have descried about these threats.

3.1 Privacy Related Threats

Digital Dossier of personal information:

Vulnerabilities: With the advancement of data mining technology and the reduction of cost of disk storage, the third party can create a digital dossier of personal data with the information revealed on the profiles of SNSs. A common vulnerability is that more private attributes which are directly accessible by profile browsing can be accessed via search (e.g. a person's name and profile image is accessible via search on MySpace, Facebook and others, unless default privacy settings are changed).
Risk: The information revealed on SNS can be exploited by an adversary to embarrass, to blackmail or even to damage the image of profile holder. For instance people are missing out their employment opportunities since the employer reviews the SNS profiles of the prospective candidates [11, 12]. In some cases people are threaten as well such as recently the Miss New Jersey, 2007 was threatened with publication TKK T-110.5190 Seminar on Internetworking 2008-04-28/29 of images taken from her SNS profile if she would not give up her crown [13].

Face Recognition
Vulnerabilities: Users of the social network often tend to add images to their individual profiles that can be used for identifying the corresponding profile holders. Thus an stranger can use this data source for the correlating profiles across services using face recognition which is a part of the broader threat posed by so-called mashups.
Risk: Face recognition can be used for the linking of image instances (and the accompanying information) across services and websites which in turn enables connecting, for example, a pseudo-anonymous dating profile with an identified corporate website profile. As a result, an adversary can gather substantially more information about a user than intended.

Content-based Image Retrieval
Vulnerabilities: Most of the SNSs haven't employed any privacy controls over the images of the profiles to prevent the disclosure of information through the Content Based Image Retrieval (CBIR) yet. CBIR is an emerging technology which is able to match features, such as identifying aspects of a room (e.g. a painting) in very large databases of images and thus increases the possibilities of location the users [14, 15, 16].
Risk: CBIR opens up the possibility of deducing location data from apparently anonymous profiles containing images of users' homes. This can lead to stalking, unwanted marketing, blackmailing and all other threats associated with unwanted disclosure of location data.

Image Tagging and Cross-profiling
Vulnerabilities: The SNS user has the option to tag images with metadata such as the name of the person in the photo, a link to their SNS profile (even if they are not the owner/controller of that profile), or even their e-mail address.
Risk: An adversary can use this feature to slander some well-known personalities or brands and gain profit from their reputation.

Difficulty of Complete Account Deletion
Vulnerabilities: Users of SNS normally face more difficulty in deleting the secondary information than to delete their user accounts from any online social network. In some cases, such secondary information is almost impossible to remove. For instance the public comments a user has made on other accounts using their identity will remain online even after deleting his account.
Risk: The user may lose the control over his/her personal information. The information that can't be removed can be used as digital dossier.

3.2 SNS Variants of Traditional Network and Information Security Threats:

Spamming

Vulnerabilities: The enormous growth of social networking sites has encouraged the spammers to create the unsolicited messages known as Social Network (SN) Spams to produce traffic overload in the social networks.
Risk: SN Spam may cause the traffic overload, loss of trust or difficulty in using the underlying application as well as Phishing and diversion to pornographic sites.

Cross Site Scripting, Viruses and Worms
Vulnerabilities: SNSs are vulnerable to cross-site scripting (XSS) attacks and threats due to widgets produced by weakly verified third parties [17].
Risk: An adversary can use this vulnerability to compromise the account, to perform phishing attack and to spread the unsolicited content to the email and Instant Messaging (IM) traffic. Moreover, it can also be used for Denial of service and associated loss of reputation.

SNS Aggregators
Vulnerabilities: Some of the new applications such as Snag, ProfileLinker provide read/write access to several SNS accounts to integrate the data into a single web application. But such applications use weak authentication method and thus the vulnerability is increased.
Risk: The effects of this vulnerability are Identity theft, Zombification of SNS accounts, e.g. for XSS attacks or advertising, loss of privacy for other members of the SNS by allowing search across a broader base of data.

3.3 Identity Related Threats

Phishing
Vulnerabilities: A phisher can easily and effectively exploit the information available on social network to increase the success rate of a phishing attack. For instance, the email phishing attacks can be achieved 72% hit rate by using the information available in the social network [18]. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links.
Risk: Phishing can reveal the sensitive information, such as passwords and credit-card or bank account numbers and cause financial and reputation damage.

Information Leakage
Vulnerabilities: The privacy of online social networks is jeopardized since an adversary can easily become a friend of a member of any restricted group by dissembling his identity and then access to the private information that belongs to the members of only that group. Moreover, on many SNSs such as MySpace it is even possible to use scripts to invite friends.
Risks: Some of the potential risks associated with this threat are: Leakage of Private information, Phishing for information and conducting spamming and marketing campaigns.

Profile squatting through Identity theft
Vulnerabilities: A malicious attacker can create a fake profile to impersonate a renowned person or a brand. Such profiles are usually created by the people who know the personal details of a user and create a profile to impersonate him or her and thereby causing all sorts of problems for the victim.
Risks: Profile squatting can do a significant damage to the reputation of a person or any brand which may in turn lead to the financial and social embarrassment. Recently an underage student at University of Missouri-Columbia was in trouble when college administrators found a picture of her duct-taped to a chair while another student poured beer in her mouth. This was a matter of considerable embarrassment as she had just been elected student body vice president.

3.4 Social Threats:

Stalking
Vulnerabilities: A participant can reveal his personal information including location, schedule, home address, phone number etc in his profile which can be used by an attacker for social stalking i.e. to threat the victim through physical proximity or phone calls or even e-mails, instant messengers or messaging on SNSs. Stalking using SNSs is increasing currently.
Risk: The impact of cyber stalking on the victim is well known and can range from mild intimidation and loss of privacy to serious physical harm and psychological damage.

Corporate Espionage
Vulnerabilities: Social engineering attacks using SNSs are a growing but often underrated risk to corporate IT infrastructure.
Risk: The main risk here is the loss of corporate intellectual property, but gaining access to insiders may also be a component in a broad range of other crimes, such as hacking corporate networks to cause damage, blackmailing of employees to reveal sensitive customer information and even to access physical assets.

4. Discussions and Recommendations

By analyzing the different kinds of threats associated with the Social Network Sites, I have found the following major factors that might be considered as the root of all threats:

- Most of the users (especially the teenagers) are not concerned with the importance of personal information disclosure and thus they are in the risk of over-disclosure and privacy invasions due to this underestimation of extent and activity of social networking. Especially, the major portion of threats are related with the friends list, posted pictures, Wallposts etc. in which users are relatively less conscious compare to the personal profile information.
- Users who are aware of the threats, often fails to properly manage the privacy preference due to the complexity and ambiguity of the interface and lack of user-friendly guidelines that would help the users to choose the appropriate privacy settings.
- The existing legislation and policy are not equipped to deal with many of the challenges that the social network currently presents including the legal position on image-tagging by third parties, the legal position on profile-squatting etc.
- Lack of appropriate authentication and access control mechanisms as well as other security related tools to handle different privacy and security issues of online social networks.

Recommendations:

Some of the recommended strategies for circumventing the threats associated with the online social networks are described below:

Building self awareness about the information disclosure: Users need to be more conscious about the information they reveal through their personal profiles in online social networks. They also have to accurately maintain their profiles through periodical review and necessary modification of the profile contents to ensure appropriate disclosure of information.

Encouraging awareness-raising and Educational Campaigns: Government should initiate different educational and awareness-raising campaigns to inform the users to make the rational usage of the Social Networking Sites as well as to encourage the providers to develop and practice security conscious corporate policies.

Reviewing and reinterpreting the regulatory framework: The existing legislation may need to be modified or extended due to the introduction of some issues like the legal position of image tagging by the third person which are not addressed by the current version. As a result, the regulatory framework governing SNSs should be reviewed and revised as it requires.

Promoting stronger authentication and access-control where appropriate: The strength of authentication method varies from SNS to SNS. However, in order to avoid fake and troublesome memberships, the authentication mechanism need to be further strengthen using additional authentication factors such as e-mail verification through Captchas.

Setting appropriate defaults: Since most of the users are not aware of the necessity for changing the default privacy preference [19], it is essential to set the default setting as safe as possible. The SNS service provider also needs to offer user-friendly guidelines that help the users to change the privacy settings successfully.

Providing suitable security tools: Providers also need to offer the following strategies for better user control on different privacy and security related issues:

- Tools that will allow the users to remove their accounts as well as edit their own posts on the other people's public notes or comment areas conveniently.
- Automated filtering tools for determining the legitimate contents.
- Tools for controlling the tagging of images depicting them.
- New privacy software such as visualization tools for increasing the utilization of privacy options by providing clear representations of social networks, friend proximity, and availability of profile features.

5. Conclusion

Online social networks offer exciting new opportunities for interaction and communication, but also raise new privacy concerns. In this paper, we have briefly described of some major features and benefits of social networking that have made this technology as one of the most popular internet technologies at this moment. We have also highlighted the crucial privacy and security threats that may arise due to 'almost-anything-goes' ethos of social networking sites. Finally, we have stated few recommendations to enhance the security issues of SNSs' to ensure that the users will get benefits from the social network sites rather than sufferings of its downsides. If online social networks are not carefully used then instead of bringing the blessings to the users, it will be appeared as a dangerously powerful tool for spammers, unscrupulous marketers and others who may do the serious harms to the users.

References

[1] Ellison, N. B., Steinfield, C., and Lampe, C. . The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. In Journal of Computer-Mediated Communication, volume 12, 2007.

[2] A. Acquisti and R. Gross. Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook, . In 6th Workshop on Privacy Enhancing Technologies, June 2006. Available at: www.careerjournal.com/jobhunting/usingnet/20060112-flesher.html.

[3] R. Gross and L. Sweeney. Towards real-world face deidentification. In IEEE Conference on Biometrics: Theory, Applications and Systems.

[4] D. Boyd. Reflections on friendster, trust and intimacy. In Intimate (Ubiquitous) Computing Workshop - Ubicomp,Seattle, Washington, USA, October 2003.

[5] D. Boyd. Friendster and publicly articulated social networking. In Conference on Human Factors and Computing Systems (CHI 2004), Vienna, Austria, April 2004.

[6] D. B. Donath, J. Public displays of connection. In BT Technology Journal 22, pages 71 – 82, 2004.

[7] R. Feizy. Evaluation of Identity on Online Social Networking: Myspace. In 18th Conference on Hypertext and Hypermedia (HT '07), December 2007.

[8] A. Gross R., Acquisti. Privacy and information revelation in online social networks. In ACM Workshop on Privacy in the Electronic Society (WPES), 2005.

[9] D. Rosenblum. What Anyone Can Know. In The Privacy Risks of Social Networking Sites, IEEE Security and Privacy, 2007.

[10] R. Gross and L. Sweeney. Towards real-world face deidentification. In IEEE Conference on Biometrics: Theory, Applications and Systems, 2007.

[11] J. Flesher. How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. In The Internet Engineering Task Force, 2006. Available at: http://www.careerjournal.com/jobhunting/usingnet/20060112-flesher.html
[12] A. Fuller. Employers snoop on Facebook. In The Stanford Daily, January 2006. Available at: http://daily.stanford.edu/article/2006/1/20/employersSnoopOnFacebook.
[13] E. Pilkington. Blackmail claim stirs fears over Facebook. In The Guardian, July 2007. Available at http://www.guardian.co.uk/international/story/0,,2127084,00.html.
[14] Chen, Y., Roussev, V., Richard, G. III, Gao, Y. Content-based image retrieval for digital forensics. In Proceedings of the First International Conference on Digital Forensics (IFIP).
[15] M. Sutter, T. Müller,R. Stotzka et al. Inspector Computer. In German eScience Conference.
[16] R. Datta, D. Joshi, J. Li, and J. Z. Wang. Image Retrieval: Ideas, Influences, and Trends of the New Age. In ACM Computing Surveys.
[17] J. N. J. M. M. F. Jagatic, T. Social phishing. In Communications of the ACM Forthcoming, 2006. www.indiana.edu/\~phishing/social-network-experiment/phishing-preprint.pdf.
[18] G. Hogben. Security Issues and Recommendations for Online Social Networks. Position paper, ENISA, European Network and Information Security Agency, October 2007. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.
[19] W. Mackay. Triggers and barriers to customizing software. In proceedings of CHI'91, ACM Press, pages 153–160, 1991.

Abdullah Al Hasib received joint M.Sc. degree in Mobile Computing and Security from Helsinki University of Technology (Finland) and Royal Institute of Technology (Sweden) in 2009 and B.Sc. degree from Islamic University of Technology (Bangladesh) in 2005. He has been working as a lecturer in CIT department, Islamic University of Technology since 2005. His current research interest includes cryptographic protocols, wireless network security and mobility management.