Security and Online Social Networks

Javier Echaiz and Jorge Ardenghi

Laboratorio de Investigación de Sistemas Distribuidos (LISiDi),
Departamento de Ciencias e Ingeniería de la Computación
Teléfono: +54 291 4595135, Fax: +54 291 4595136
Universidad Nacional del Sur, Bahía Blanca (8000), Argentina
{je,jra}@cs.uns.edu.ar,
WWW home page: http://lisidi.cs.uns.edu.ar

Abstract. In the last few years we have witnessed a sustained rise in the popularity of online Social Network Sites (SNSs) such as Twitter, Facebook, Myspace, Flickr, LinkedIn, FriendFeed, Google Friend Connect, Yahoo! Groups, etc., which are some of the most visited websites worldwide. However, since they are are easy to use and the users are often not aware of the nature of the access of their profiles, they often reveal information which should be kept away from the public eyes. As a result, these social sites may originate security related threats for their members.
This paper highlights the benefits of safe use of SNSs and emphasizes the most important threats to members of SNSs. Moreover, we will show the main factors behind these threats. Finally we present policy and technical recommendations in order to improve security without compromising the benefits of information sharing through SNSs.
Keywords: Online Social Network, Privacy, Profile squatting, Identity threat, Image Tagging and Cross-profiling.

1 Introduction

The advent of the Internet has given rise to many forms of online sociality, from the old e-mail and Usenet services to the more recent instant messaging (IM), blogging, and online social services. Among these, the technological phenomenon that has acquired the greatest popularity in this 21st century is the latter, the 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:

– People can stay connected with peers very conveniently, no matter where they are. The connectedness developed through the social networking might contribute to increased self-esteem, specially for students [6].

– Like-minded individuals can discover and interact with each other.
– Create a virtual space 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, an 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, features and behavior able to increase the number of members and their connections. However, the security and the access control mechanisms of SNSs are relatively weak by design since security and privacy are not considered as the first priority in the development of SNSs [1]. As a result, along with the benefits, significant security risks have also emerged in online social networking [17] as well.

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.

2 Related Works

The popularity of the concept of online social networks has been increasing since 1997. As a result, in the recent years, social networking has gained intense media and academic attention. There are academic studies in different fields such as the ethnographic and sociological approaches to the study of online self-representation [2, 3, 5].

In addition to that, there have been significant research works on the security issues of online social networking. An- alyzing 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.

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]:

- 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.

A paper 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. This data expose themselves to various kinds of security risks [11]. In a research on Human Computer Interaction (HCI), Wenday Mackay has shown that only a minimal percentage of users tend to change the default and highly permissive privacy preferences [18].

Also a number of new methods and strategies have been proposed in different research papers 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-parties 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 will discuss these threats.

3.1 Privacy Related Threats

Digital File of Personal Information

Vulnerabilities: With the advancement of data mining technologies and the reduction of cost of disk storage, third parties can create a digital file of personal data from 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 an SNS can be exploited by an attacker to embarrass, to blackmail, to impersonate or even to damage the image of profile holder. For instance, people can miss out employment opportunities since the employer reviews the SNS profiles of the prospective candidates [8, 9]. Another example is Facebook Beacon, a marketing initiative that allows websites to publish a user's activities to their Facebook profile as "Social Ads" and promote products. When launching Beacon, Facebook stated "no personally identifiable information is shared with an advertiser in creating a Social Ad", and that "Facebook users will only see Social Ads to the extent their friends are sharing information with them".

Sadly data mining is still possible, the BBC "Click" technology program demonstrated that personal details of Facebook users and their friends could be stolen by submitting malicious applications.

Face Recognition

Vulnerabilities: Users of a 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 to correlate 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 attacker 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 [4][14][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 attacker can use this feature to slander some well-known personalities or brands and gain profit from their reputation. This information can be used to reveal links to relatives, friends, partners, co-workers, potentially leading to kidnappings.

Difficulty of Complete Account Deletion

Vulnerabilities: Members of SNS normally face more difficulty in deleting the secondary information than to delete their user accounts. 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 a digital personal file. For example, in 2008 Facebook allowed account to be deleted by the user, previously account "deactivation" was the only (partial and incomplete) solution.

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 and masive messages (spam) in order to produce traffic to their sites and better ranks at search engines, and at the same time overloading the social networks.

Risk: This spam may cause traffic overload, loss of trust or difficulty in using the underlying application as well as phishing and detours to inappropriate sites. In May 2009, Facebook users all over the world suffered a massive phishing campaign, launched by Russian hackers from servers in Latvia and China, that led to thousands of accounts being hijacked.

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 [12]. Every big SNS offer a well documented and easy API to programmers (in order to attract more users with new features), but they don't ensure security on the code produced.

Risk: An attacker 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, SocialMediaPop, NameBeeNameBee, ProfileLinker, TwitterFeed, etc. 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 data base.

3.3 Identity Related Threates

Phishing

Vulnerabilities: A phisher can easily and effectively exploit the information available on social networks to increase the success rate of a phishing attack. For instance, the email phishing attacks can achieve 72% hit rate by using the information available in the social network [13]. 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 sensitive information, such as passwords and credit-card or bank account numbers and it can cause financial and reputation damage.

Information Leakage

Vulnerabilities: The privacy of online social networks is jeopardized since an attacker 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 and Twitter, it is even possible to use scripts to invite friends (MySpace) or to follow members (Twitter).

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, e.g. users impersonating celebrities on Twitter. 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 done a significant damage to the reputation of a person or any brand which may in turn lead to financial and social problems.

3.4 Social Threats

Stalking

Vulnerabilities: A participant can reveal his personal information including location, schedule, home address, phone number, real time location using a GPS, etc. in his profile, which can be used by an attacker for social stalking 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. For example, Twitter encourages members to post their mobile phone numbers in their profiles in order to "increase fun".

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 Discussion and Recommendation

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

- Most of the users (especially 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 their social network. Main threats are related to the friends list, posted pictures, wallposts, etc., where users are relatively less conscious to compare to the personal profile information.
- Users who are aware of the threats, often fail to properly manage their privacy preferences 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. Even slanderous allegations using digital media is unclear in most countries.

– 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.

Also there are privacy problems originated at the social networks itself. For example, in July 2009 it came to light that there are concerns by the Canadian Privacy Commission that Facebook is breaching several Canadian privacy laws by not deleting a user's information when their account is deactivated and by giving "confusing or incomplete" information to members. Facebook's Chief Privacy Officer was quoted as saying that "[Facebook] was working with the commission to resolve the issues". The CPC have given Facebook 30 days before they make a further review and recommendations. If Facebook don't comply with the Canadian statutes it's possible that the issue could be taken to the federal courts.

Privacy proponents have criticized Facebook's privacy agreement, which states: "We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile". Another clause that received criticism concerned Facebook's right to sell a user's data to private companies, stating: "We may share your information with third parties, including responsible companies with which we have a relationship".

The massive phishing campaign mentioned above originated strong criticism against Facebook for its late reaction to this issue and the fact that initially it merely tried to block the attack, rather than notifying users of the situation.

Other security fears regarding profile content itself are also present. For example in MySpace the embedding of videos inherently allows all of the format's abilities and functions to be used on a page. A prime example of this surfaced in December 2006, when embedded QuickTime videos were shown to contain hyperlinks to JavaScript files, which would be run simply by a user visiting a 'phished' profile page, or even in some cases by simply viewing a user's 'about me' elsewhere on the site. Users who entered their login information into a fake login bar that appeared would also become 'phished', and their account would be used to spam other members, thus spreading this security problem.

On January 26, 2008, over 567,000 private MySpace user pictures were downloaded from the site by using a bug published on YouTube and put on the Piratebay torrent site for download.

MySpace is often used as a venue for publicizing parties, sometimes with the host's knowledge and sometimes without. There have been some well-publicized incidents where MySpace parties have caused thousands of dollars damage to property.

4.1 Recommendations

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

Building self awareness about 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 how to make rational usage of 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 (not addressed by the current law) due to the introduction of some issues like the legal position of image tagging by third persons, etc. As a result, the regulatory framework governing SNSs should be reviewed and revisted.

Promoting stronger authentication and access-control where appropriate: The strength of authentication method varies from an SNS to another. 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 and security concerns. In this paper we have briefiy described some of the major features and benefits of social networking that have made this technology one of the most popular Internet technologies of today. We have also highlighted the crucial privacy and security threats that may arise due to "almost-anything-goes" ethics of social networking sites. Finally, we have stated some recommendations to enhance the security issues

of SNSs' to ensure that the users will get benefits from the social network sites rather than suffering its downsides. Insecure online social networks can make the perfect hearquarters for spammers, unscrupulous marketers, etc., people able to do serious harm to the uninformed users.

References

1. A. Acquisti and R. Gross. Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook. In *6th Workshop on Privacy Enhancing Technologies*, June 2006.
2. D. Boyd. Reflections on friendster, trust and intimacy. In *Intimate (Ubiquitous) Computing Workshop - Ubicomp*, Seattle, Washington, USA, October 2003.
3. D. Boyd. Friendster and publicly articulated social networking. In *Conference on Human Factors and Computing Systems (CHI 2004)*, Vienna, Austria, April 2004.
4. 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)*.
5. d. b. Donath, J. Public displays of connection. In *BT Technology Journal 22*, pages 71–82, 2004.
6. 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.
7. R. Feizy. Evaluation of Identity on Online Social Networking: Myspace. In *18th Conference on Hypertext and Hypermedia (HT '07)*, December 2007.
8. J. Flesher. How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. In *The Internet Engineering Task Force*, 2006.
9. A. Fuller. Employers snoop on Facebook. In *The Stanford Daily*, January 2006.
10. R. Gross and L. Sweeney. Towards real-world face deidentification. In *IEEE Conference on Biometrics: Theory, Applications and Systems*, 2007.
11. A. Gross R., Acquisti. Privacy and information revelation in online social networks. In *ACM Workshop on Privacy in the Electronic Society (WPES)*, 2005.
12. G. Hogben. Security Issues and Recommendations for Online Social Networks. Position paper, *ENISA, European Network and Information Security Agency*, October 2007.
13. T. Jagatic, N. Johnson, M. Jakobsson et. al. Social phishing. In *Communications of the ACM*, pages 94–100, 2007.
14. M. Sutter, T. Mller,R. Stotzka et al. Inspector Computer. In *German eScience Conference*.
15. E. Pilkington. Blackmail claim stirs fears over Facebook. In *The Guardian*, July 2007.
16. R. Datta, D. Joshi, J. Li, and J. Z. Wang. Image Retrieval: Ideas, Infiuences, and Trends of the New Age. In *ACM Computing Surveys*.
17. R. Gross and L. Sweeney. Towards real-world face deidentification. In *IEEE Conference on Biometrics: Theory, Applications and Systems*.
18. D. Rosenblum. What Anyone Can Know. In The Privacy Risks of Social Networking Sites, *IEEE Security and Privacy*, 2007.
19. W. Mackay. Triggers and barriers to customizing software. In *Proceedings of CHI'91, ACM Press*, pages 153–160, 1991.