A Survey on Challenges of Privacy and Security Issues in Social Media

Rashmi Gupta
Dept. of Computer Science & Engineering
Amity University Haryana

Ruchi Kamra
Dept. of Computer Science & Engineering
Amity University Haryana

***Abstract :**Online social networks are becoming a major attraction of the internet, as individuals and organization desire to interact with one another, the ability of the internet to deliver this networking capabilities grows stronger. In this paper, the structure and components of the member profile and the challenges of privacy issues faced by individualsis discussed and governments that participate in social networking.*

***Keywords:** Social Network, Privacy and Security issues.*

1. Introduction

Social media is the platform that allow people to build a public or semi-public profile within a bounded system, articulate a list of other users usually called Friends with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site. Social networking by definition focuses on building and reflecting personal and social relations among people who share common interests, causes or goals. A social networking site is an on-line service that attracts a community of users and provides such users with a variety of tools for posting personal data and creating user-generated content directed to a given user's interest and personal life, and provides a means for users to socially interact over the internet, through e-mail, instant messaging or otherwise.

Recent years saw Facebook, Twitter, YouTube, LinkedIn, Skype, 9jabook and other social networking sites solidify their position at the heart of many users' daily internet activities, and saw these websites become a primary target for hackers .

2. Types of Social Networks

SNSs can be divided in a number of ways. We have chosen to follow, with some extension, the division developed by Digizen (2008), an organisation which promotes secure activities on the web.

2.1 Profile-based Social Networks

Profile-based services are largely organised around members' profile pages. Bebo (www.bebo.com), Facebook (www. facebook.com), Hi5 (www.hi5.com), MySpace (www.myspace.com) .

2.2 Content-based Social Networks

With these services, the user's profile is the most important way of organising connections. Though, they play a secondary role in the posting of content. Photo-sharing site Flickr (www.flickr.com) is a good example of this brand of service, one where groups and comments are based around pictures. Shelfari (www.shelfari.com) is one of the current brand of book-focused sites, with the members 'bookshelf' being a focal point of their profile and membership.

2.3 White-label Social Networks

These sites present members with the opportunity to create and join communities – this means that users can build their own 'mini-MySpace's', small scale, personalised social networking sites about whatever the initiator wants them to be about. Some interesting examples are WetPaint (www.wetpaint.com), Wikileaks (www. wikileaks.com) and Wikipedia (www. wikipedia.com) which uses social wikis as its format to enable social networking.

2.4 Multi-User Virtual Environments Gaming environments such as Runescape (www.runescape.com) and virtual world sites like Second Life (www. secondlife.com) allow users to interact with each other's avatars are a virtual representation of the user.

2.5 Mobile Social Networks

Many social networking sites are now offering mobile access to their services, allowing members to interact with their personal networks via their mobile phones.

2.6 Micro-blogging/Presence Updates

Many services let users post status updates i.e. short messages that can be updated to let people know what mood you are in or what you are doing. These types of networks enable users to be in constant touch with what their network is thinking, doing and talking about. Twitter (www.twitter.com), NairaLand (www. nairaland.com) and Wayn (www.wayn.com) are examples.

3. Structure of Member Profiles

The member profile represents how the individual chooses to present their identity at a specific time and with a particular understanding of one's audience (Wildbit, 2005). But some observations show that while the audience and the individual evolve over time, one's profile is usually stuck in time. Some profile information are common to all social networking sites, these include Names (First Name, Surname or Middle Name) and e-mail contacts. Table 1 shows the User profile information gathered by various social networking sites.

Table 1 Structure of Profile Information in some Social Networks. * means the field exist

Profile Information	Facebook	Twitter	LinkedIn	Orkut	freindster
Professional detail	*	*	*	*	
Gender	*	*	*	*	*
Age/date of Birth	*	*	*	*	*
Hobbies/Inte	*	*	*	*	*

rest					
Location	*	*	*	*	*
College/ University	*	*	*		*
Languages	*	*	*		
Religion	*	*	*	*	
Nationality	*	*	*	*	*

Suggestions or Advice to Users:

- The more profile information a user discloses or filled in his/her account, the more the user made public his/her private issues.
- Information which the user knows he/she uses as passwords or PIN (personal identification number) should remain blank. For example, some people use their date of birth or home town as passwords or PIN, in either case the field should be left black or made invisible.
- Users should also take full advantage of the feature that allows them to select which information in their profile will be visible to others.
- The closer potential connections between community members can be, the more information is the member willing to give about himself, beware!

4. The Privacy and security Issues

Attackers may use social networking services to spread malicious cryptogram, compromise users' computers, or access personal information concerning a user's identity, location, contact information, and personal or professional relationships. The user may also unintentionally reveal information to unofficial individuals by performing certain actions.

4.1 Viruses

The fame of social networking services makes them a perfect target for attackers who want to have the heaviest blow with the least effort. By creating a virus and embedding it in a website or a third-party application, an invader can potentially infect millions of computers just by relying on users to share the malicious links with their associates or friends.

4.2 Tools

Attackers may use tricks that allow them to take control of a user's account. The attacker could then have the right to use the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also masquerade as that user and post malicious content.

4.3 Social Engineering Attacks

Attackers may send an email or post a statement that appears to originate from a trusted social networking service or user. The mail may contain a malicious URL or a demand for personal information. If you follow the instructions, you may reveal vital information or compromise the security of your system.

4.4 Identity Theft

Attackers may be able to collect enough personal information from social networking services to assume your identity or the identity of one of your friends. Even a few personal information may provide attackers with enough detail to guess answer to security or password reminder question for email, credit card, or bank accounts.

4.5 Third-party Applications

Some social networking services may let you to add third-party applications, including games and quizzes that provide additional functionality. Be cautious using these applications—even if an application does not contain malicious code, it might access information in your profile without your knowledge. This detail could then be used in a variety of ways, such as advertisements, performing market research, sending spam email, or accessing your contacts.

4.6 Business Data

Posting sensitive information intended only for internal company use on a social networking service can have serious consequences. Disclosing information about customers, intellectual property, human resource issues, mergers and acquisitions, or other company activities could result in liability or bad publicity, or could reveal information that is useful to competitors.

4.7 Professional Reputation

Inappropriate photos or content on a social networking service may threaten a user's educational and career prospects. Colleges and Universities may conduct online searches about potential students during the application process. Many companies also perform online searches of job candidates during the interview process. Information that suggests that a person might be unreliable, untrustworthy, or unprofessional could threaten the candidate's application. There have also been many instances of people losing their jobs for content posted to these services.

4.8 Personal Relationships

Because users can upload comments from any computer or smart phone that has internet access, they may impulsively post a comment that they later regret. According to a survey conducted by Retrevo, ―32 percent of people who post on a social networking site regret they shared information so openly. Even if comments and photos are retracted, it may be too late to undo the damage. Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache.

4.9 Personal Safety

The user may compromise personal security and safety by posting certain types of information on social networking services. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized.

5. Conclusion

Social networking is the current major trend in internet use. It is already heavily under attack and seems likely to continue to become more of a target as its popularity grows. Whether users eventually will be turned off by the rising tide of malware and spam may depend on how providers react and implement measures to ensure security and privacy. For those of us that still wonder how the dictator of Tunisia was overthrown in less than one month after being in power for almost two and a half decades. There is no question about how opponents of his regime were able to topple it. Two words describe it: Facebook, Twitter. These two social networking sites enabled protesters to take to the streets, organize the opposition, recruit new protesters, and prevail over the police force and the military. What happens to National Security? In conclusion, governments will have to play a major role in how secure social networks are, with much greater efforts required to crack down on current cybercriminals and discourage new blood from joining the dark side. These efforts must be implemented at both national and global level to ensure that crimes and criminals cannot be harbored and abetted by rogue nations ignoring global regulation. New laws must provide protection from criminals but also ensure secure behavior by those entrusted with sensitive data—who will doubtless continue to leak information in ever-greater amounts, as we have observed throughout the past decade.

References

[1]. Digizen (2008). Young People and Social Networking Services: A Childnet International Research Report [Online]. Available from http://www. digizen.org/downloads/fullReport.pdf

[2]. Esecurityplanet (2011), available at http://www.esecurityplanet.com/features /print.php/3874206.

[3]. Facebook(2011), "Facebook Factsheet", (http://www.facebook.com/press/info.ph p?factsheet) (accessed January 3, 2011)

[4]. LinkedIn (2011), "About Us", (http://press.linkedin.com/about) (accessed January 3, 2011)

[5]. MySpace(2011), "MySpace Fact Sheet", (http://www.myspace.com/pressroom/fa ct-sheet/) (accessed January 3, 2011).

[6]. Networld (2011), available at http://www.networkworld.com/news/20 09/012309-social-networking-sites-ahotbed.html.

[7]. PricewaterhouseCoopers (2010), "Security for social networking", Advisory Services Security, US.

[8]. Ralph Gross and Alessandro Acquisti (2005), "Information Revelation and Privacy in Online Social Networks (The Facebook case)", Pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES), Alexandria, Virginia, USA.

[9]. Sophos (2010), "Security Threat Report: 2010", available at http://www.sophos.com

[10] The Masked Walnut (2011), "Social networking sites & revolution: Organising revolt online". Available at http://southernnationalist.com/blog/auth or/the-masked-walnut/ Access date 14/03/2011 [11] Twitter (2011), "About Twitter", (http://twitter.com/about) (accessed January 3, 2011).

[12] Wildbit (2005), "Social Networks Research Report", available at http://www.wildbit.com last updated 07.25.05.