Advanced techniques to overcome the privacy issues and SNS threats

C. Infant Louis Richards

Student, Dept. of CSE, Jeppiaar Engineering College, Chennai, India

richiemdu@gmail.com

Abstract

We have witnessed a dramatic rise in popularity of online social networking services such as MySpace, Facebook, orkut, twitter etc which are now among the most visited websites globally. However, since such websites 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, thereby improving the privacy in social sites.

Keywords – Social Networking, Privacy issues, Security

1.1 Introduction

Online service providers, such as Facebook and orkut, are beginning to collect various kinds of public and private data across the Web for the purposes of targeted marketing. A vast variety of data is collected about the user, and the current legal system has different legal standards for different kinds of data.

This is problematic because the privacy policies against government and third-party intrusions are complex and confusing to the end user. Furthermore, we are proposing an accountability infrastructure for protecting consumer’s online privacy. Currently, different kinds of data are protected under separate privacy policies and codes. The end user cannot predict how the data can be used by the government or third-parties, or how all their private information would be protected under the existing law.

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.

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.

2.1 Report 2011

The first decade of the 21st century saw a dramatic change in the nature of cybercrime. Once the province of teenage boys spreading graffiti for kicksnotoriety, hackers today are organized, financially motivated gangs. In the past, virus writers displayed offensive images and bragged about the malware they had written; now hackers target companies to steal intellectual property, build complex networks of compromised PCs and rob individuals of their identities. 2009 saw Facebook, Twitter 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. Because of this, social networks have become one of the most significant vectors for data loss and identity theft. New computing platforms also emerged last year, and shortly thereafter fell victim to cybercriminal activities. What was lost was once again found in 2010, as old hacking techniques re-emerged as means to penetrate data protection. By understanding the problems that have arisen in the past, perhaps internet users can craft themselves a better, safer future.

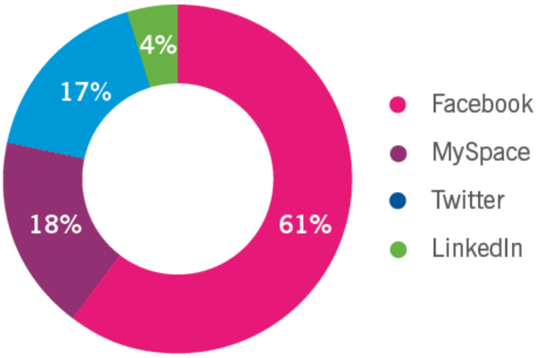


Fig.1 Social Network Analysis based on Risk (2011)

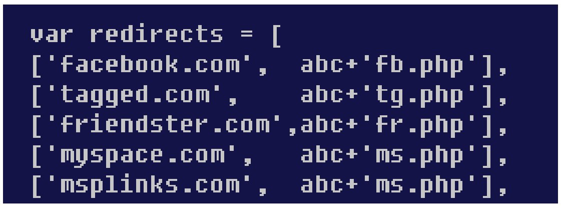
3.1 Known attacks

The following mentioned are the already known famous spam attacks that we come across in the social websites.

3.2 Koobface

Those worried about the dangers of social networking sites have a right to be concerned, as many malicious attacks, spammers and data harvesters take advantage of under cautious users. Most notably, the notorious Koobface worm family became more diverse and sophisticated in 2009. The sophistication of Koobface is such that it is capable of registering a Facebook account, activating the account by confirming an email sent to a Gmail address, befriending random strangers on the site, joining random Facebook groups, and posting messages on the walls of Facebook friends (often claiming to link to sexy videos laced with malware). Furthermore, it includes code to avoid drawing attention to itself by restricting how many new Facebook friends it makes each day.

Koobface's attack vectors broadened, targeting a wide range of sites other than the one that gave it its name (i.e., Facebook). Social networking sites, including MySpace and Bebo, were added to the worm's arsenal in 2008; Tagged and Friendster joined the roster in early 2009; and most recently the code was extended to include Twitter in a growing battery of attacks. It is likely we will see more malware following in the footsteps of Koobface, creating Web 2.0 botnets with the intention of stealing data, displaying fake anti-virus alerts and generating income for hacking gangs. Social networks have become a viable and lucrative platform for malware distribution.



```
var redirects = [
['facebook.com',  abc+'fb.php'],
['tagged.com',    abc+'tg.php'],
['friendster.com',abc+'fr.php'],
['myspace.com',   abc+'ms.php'],
['msplinks.com',  abc+'ms.php'],
```

Fig.2Koobface virus

3.3 The Mikeyy Mooney worms

In April 2009, the StalkDaily worm rampaged Twitter as heavily spammed messages pushing an infected site by more subtle attacks spread from tweeter to tweeter. The worm appeared to be the work of 17-year-old Mikeyy Mooney, whose name was referenced in a second wave of attacks appearing just hours after the initial StalkDaily incident. Shortly afterward, yet another worm that was crafted using cross-site scripting techniques to spread referenced Mikeyy. Further attacks in April brought more misery to Twitter users. The speed with which these attacks have appeared, spread and become major issues should send a strong message to the big Web 2.0 companies.

4.1 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. The top ten networking threats are given below.

- **Social networking worms:** Social networking worms include Koobface, which has become, according to researchers, "the largest Web 2.0 botnet." While a multi-faceted threat like Koobface challenges the definition of "worm," it is specifically designed to propagate across social networks (e.g., Facebook, MySpace, Twitter, hi5, Friendster and Bebo), enlist more machines into its botnet, and hijack more accounts to send more spam to enlist more machines. All the while making money with the usual botnet business, including scareware and Russian dating services.
- **Phishing bait:** Remember FBAction? The e-mail that lured you to sign into Facebook, hoping you don't pick up on the fbaction.net URL in the browser? Many Facebook users

had their accounts compromised, and although it was only a "tiny fraction of a percent," when you realize Facebook has over 350 million users, it's still a significant number. To its credit, Facebook acted quickly, working to blacklist that domain, but lots of copycat efforts ensued (e.g., fbstarter.com). Facebook has since gotten rather adept at Whack-A-Mole.

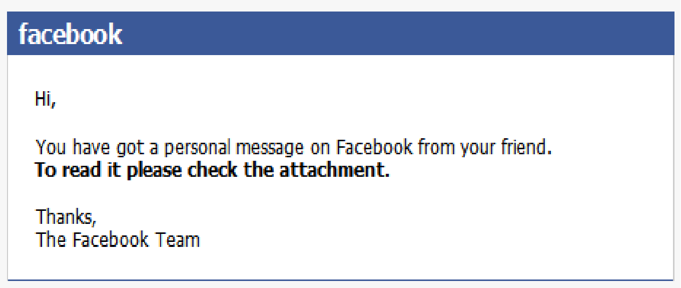
- **Trojans:** Social networks have become a great vector for trojans -- "click here" and you get:

* Zeus -- a potent and popular banking Trojan that has been given new life by social networks. There have been several recent high-profile thefts blamed on Zeus, notably the Duanesburg Central School district in New York State late in 2009.

* URL Zone -- is a similar banking Trojan, but even smarter, it can calculate the value of the victim's accounts to help decide the priority for the thief.

- **Data leaks:** Social networks are all about sharing. Unfortunately, many users share a bit too much about the organization -- projects, products, financials, organizational changes, scandals, or other sensitive information. Even spouses sometimes over-share how much their significant other is working late on top-secret project, and a few too many of the details associated with said project. The resulting issues include the embarrassing, the damaging and the legal.
- **Shortened links:** People use URL shortening services (e.g., bit.ly and tinyurl) to fit long URLs into tight spaces. They also do a nice job of obfuscating the link so it isn't immediately apparent to victims that they're clicking on a malware install, not a CNN video. These shortened links are easy to use and ubiquitous. Many of the Twitter clients will automatically shorten any link. And folks are used to seeing them.
- **Botnets**: Late last year, security researchers uncovered Twitter accounts being used as a command and control channel for a few botnets. The standard command and control channel is IRC, but some have used other applications -- P2P file sharing in the case of Storm -- and now, cleverly, twitter. Twitter is shutting these accounts down, but given the ease of access of infected machines to Twitter, this will continue. So Twitter will become expert at Whack-A-Mole too…
- **Advanced persistent threats:** One of the key elements of advanced persistent threats (APT) is the gathering of intelligence of persons of interest (e.g., executives, officers, high-net-worth individuals), for which social networks can be a treasure trove of data.

Perpetrators of APTs use this information to further their threats -- placing more intelligence gathering (e.g., malware, trojans), and then gaining access to sensitive systems. So while not directly related to APTs, social networks are a data source. Less exotic, but no less important to individuals is the fact that information on your whereabouts and activities can give more run-of-the-mill criminals an opportunity.



facebook

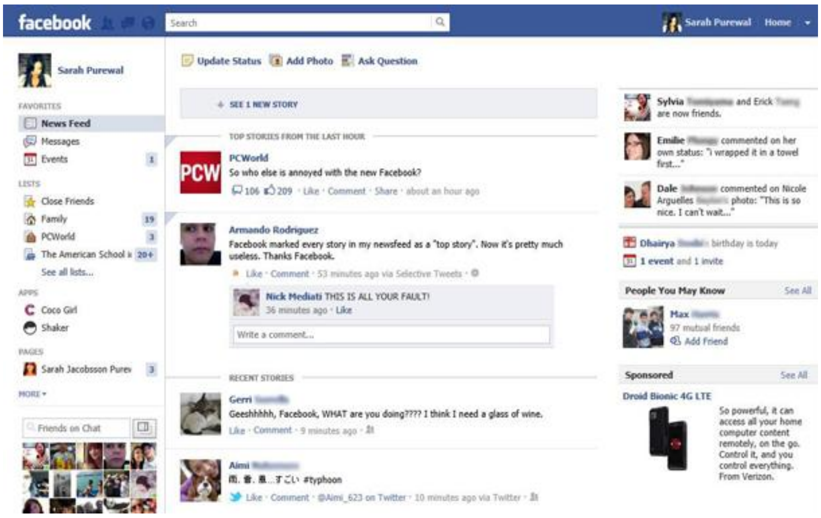
Hi,

You have got a personal message on Facebook from your friend.
To read it please check the attachment.

Thanks,
The Facebook Team

Fig.3 Facebook attacks

- **Cross-Site Request Forgery (CSRF):** While it isn't a specific kind of threat -- more like a technique used to spread a sophisticated social networking worm, CSRF attacks exploit the trust a social networking application has in a logged-in user's browser. So as long as the social network application isn't checking the referrer header, it's easy for an attack to "share" an image in a user's event stream that other users might click on to catch/spread the attack.
- **Impersonation:** The social network accounts of several prominent individuals with thousands of followers have been hacked (most recently, a handful of British politicians). Furthermore, several impersonators have gathered hundreds and thousands of followers on Twitter -- and then embarrassed the folks they impersonate (e.g., CNN, Jonathan Ive, Steve Wozniak, and the Dalai Lama), or worse. Twitter will now shut down impersonators attempting to smear their victims, but at Twitter's discretion. Admittedly, most of the impersonators aren't distributing malware, but some of the hacked accounts certainly have.
- **Trust:** The common thread across almost all of these threats is the tremendous amount of trust users have in these social applications. Like e-mail, when it hit the mainstream, or instant messaging when it became ubiquitous, people trust links, pictures, videos and executable when they come from "friends," until they get burned a few times. Social applications haven't burned enough people yet.



PCWorld
So who else is annoyed with the new Facebook?
106 209 · Like · Comment · Share · about an hour ago

Armando Rodriguez
Facebook marked every story in my newsfeed as a "top story". Now it's pretty much useless. Thanks Facebook.
Like · Comment · 53 minutes ago via Selective Tweets

Nick Mediati THIS IS ALL YOUR FAULT!
36 minutes ago · Like

Write a comment...

Gerri [redacted]
Geeshhhhh, Facebook, WHAT are you doing???? I think I need a glass of wine.
Like · Comment · 9 minutes ago

Aimi [redacted]
雨. 音. 風...すごい #typhoon
Like · Comment · @Aimi_623 on Twitter · 10 minutes ago via Twitter

Sylvia [redacted] and Erick [redacted] are now friends.

Emilie [redacted] commented on her own status: "i wrapped it in a towel first..."

Dale [redacted] commented on Nicole Arguelles [redacted] photo: "This is so nice. I can't wait..."

Dhairya [redacted] birthday is today
1 event and 1 invite

Max [redacted]
97 mutual friends
Add Friend

Droid Bionic 4G LTE
So powerful, it can access all your home computer content remotely, on the go. Control it, and you control everything. From Verizon.

Fig.4 News feed on Facebook

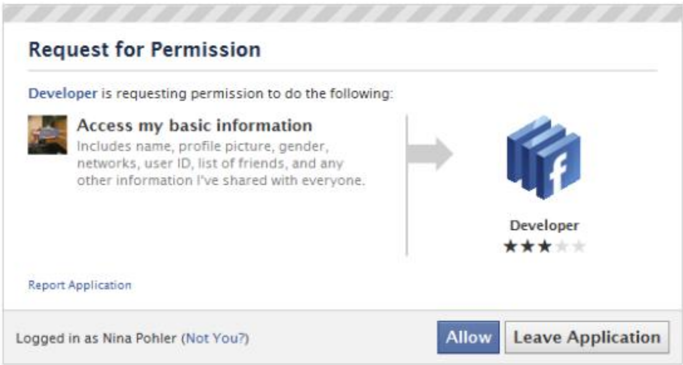
5.1 Reasons for increasing attacks

By analysing 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, Wall posts 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.



Request for Permission

Developer is requesting permission to do the following:

Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

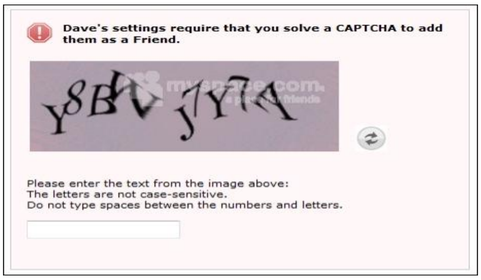
Logged in as Nina Pohler (Not You?)

Fig.5 Example of user agreeing third party agreement in Facebook

• 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.

6.1 Conclusion

The hack that bypassed security and harvested data from Twitter in July proves that social networking sites are just as vulnerable as any other software or web resource. Of course, the problem of data loss via social networks is fed by the willingness of users to share too much information with too many people. Many sites have woken up to the dangers they may present, with Facebook introducing a major new range of privacy settings in August. Sadly, in its announcement, Facebook recommended that users adopt a series of new privacy settings that would reveal their personal data to anyone on the internet forever.



Dave's settings require that you solve a CAPTCHA to add them as a Friend.

Please enter the text from the image above:
The letters are not case-sensitive.
Do not type spaces between the numbers and letters.

Fig.6 MySpace Captcha

Meanwhile, bit.ly, Twitter's favourite URL shortening service, responded to the common exploitation of such services to obfuscate malicious links, and teamed up with Sophos and other security providers to ensure its links are kept safe. The social networking boom shows no sign of stopping and businesses can no longer hide their heads in the sand. Social networking sites are now a vital part of many marketing and sales strategies. Therefore, they cannot be blocked—but they cannot be allowed to drain company resources or used as vectors for data loss or malware penetration. A unified approach providing sensible, granular access control, secure encryption and data monitoring, and comprehensive malware protection is mandatory for businesses to operate flexibly in the modern socially networked world.

References

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

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

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

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

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

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

[9] http://www.sophos.com/pressoffice/news/articles/2009/04/social-networking.html

[10] http://www.sophos.com/blogs/sophoslabs/v/post/5431

[11] http://www.sophos.com/blogs/gc/g/2009/04/12/stalkdaily-twitter-users-warn-attack/

[12] http://www.sophos.com/blogs/gc/g/2009/04/12/17yearold-claims-creator-stalkdaily-twitter-worm/

[13]http://www.sophos.com/blogs/gc/g/2009/04/12/mikeyy-attack-hits-twitter-users-bad-24-hours-web-20security/

[14]http://www.sophos.com/blogs/gc/g/2009/04/13/mikeyy-worm-madness-twitter/

[15]Rosenbush, S. (2005, July 19). News Corp.'s Place in MySpace. Retrieved November 10, 2007, from BusinessWeek.com:
http://www.businessweek.com/technology/content/jul2005/tc20050719_5427_tc119.htm

[16] Schmidt, T. S. (2006, September 6). Inside the Backlash Against Facebook. Retrieved November 18, 2007, from TIME.com:
http://www.time.com/time/nation/article/0,8599,1532225,00.html

[17] Second Life Economics Statistics Page. (2007, November 17). Retrieved November 17, 2007, from SecondLife Web site: http://secondlife.com/whatis/economy_stats.php

[18] Soltren, H. J. (2005). Facebook: Threats to Privacy. Cambridge, MA: MIT.

[19] The Gramm-Leach-Bliley Act. (2005, January).Retrieved November 18, 2007, from Electronic Privacy.

[20] M. Sutter, T. Müller,R. Stotzka et al. Inspector Computer.In German eScience Conference.