IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 6 (May. - Jun. 2013), PP 59-65
www.iosrjournals.org

Social Networking Websites and Image Privacy

Abhilasha Singh Rathor, Pawan Kumar Mishra
Mtech Scholar Uttarakhand Technical University
Assistant Professor Uttarakhand Technical University

***Abstract**: Social Networking Sites (SNS) are being used for over a decade, and has exponentially grown in popularity in the recent few years. They are web based services that allow individuals to: (a) make a public or semipublic profile (b) share contents with many users (c) view and traverse other user list. SNS allow users to connect, share information and other comments, chat, play games, and even add comments.*

Social networking sites are very useful in sharing information, making friends and keeping in touch with old friends. It is an online service, platform, or site that focuses on facilitating the building of social networks and social elation among peoples for sharing interests, activities, backgrounds, or real-life connections. But with the increasing demand of social networking sites (SNS) privacy and security concern have also increased.

The focus of our study is to measure the amount of Privacy in SNS, and based on these current techniques and attack strategies I propose a model designed in PHP to handle the privacy and security issues of SNS's.

We propose a policy based infrastructure, with the help of a SNS designed in PHP, that allows:

1. *Users to express their privacy preferences with respect to who can access their data and for what purpose.*
2. *Data provider support to enforce user privacy preferences, and supporting additional access models.*
3. *Handling privacy issues and access of data in SNS.*

I. Introduction

SNS have become very popular since they have many attracting features for the users. Most social networking websites allow member to design their own profiles so that they can design their profile page in order to express themselves and to reflect their personality. Users can customize the profile layout, add applications and can upload photos and other type of information. SNS also contains Friends list, containing other users of SNS. Through SNSs users can keep in touch with friends and family, they can find old friends, contact friends of friends, and even can contact people they didn't previously known at all. Some SNSs also help users to find a job or establish business contacts, such as connecting with clients, partners and in finding out jobs and business opportunities [9].

Social networking sites are web based services that allow individual to [14]:

1. Construct a public or semi-public profile within a bounded system.
2. Articulate a list of other users with whom they share a connection.
3. View and traverse their list of connections and those made by others within the system.

Content sharing services have made social networking sites immensely popular. Users view their profiles on social networking sites as a form of self-expression, but these profiles also have commercial value. To allay fears of privacy violations, social networking sites provide users with access control settings to place restrictions on who may view their personal information.

Also it is possible to consider the fact that the web applications are built for various purposes. Or instance we have researchers web application, social networking web application, e-mail application, ecommerce application etc. Each web application is built with different requirements for performance, security mechanisms, internationalization and scalability to serve its customers.

A. Need For Social Networking

21st century, people are preoccupied with their busy wok life that they do not have time to spare for their near and dear ones. However social networking has given them platform to stay in touch with their near and dear ones.

Social networking is one of the major technological phenomenons of the Web, with hundreds of millions of attached users. Social network enables a form of self expression for the users and help them to socialize and share contents with others. Social networking sites are very useful in sharing information, making friends and keeping in touch with old friends. But with the increasing demand of social networking sites privacy concern is also increased.

With SNS, users engage with each other for various purposes, including business, entertainment and knowledge sharing. The commercial success of SNS depends on the number of users it attract, and by encouraging users to add more users to their network and to share data with others in SNS.

B. Need For Privacy

Since SNS are widely in demand of current scenarios, the risk of their usage has also increased. Due to the lack of awareness among user and presence of less privacy protection tools, huge amount of user's data, including user's personal information, pictures and videos, is at risk. They can be used by strangers,

Content sharing is one of the main features of SNSs, but they do not provide any mechanism for collective enforcement of privacy policies on shared data.

Privacy expectations in social networks are based on relationships. Typical social networks support friends and networks with privileged access.

Friends: Friendships are a defining characteristic of social networking sites, and friends receive access to personal data. Friendships require acceptance by both parties.

Networks: Social networks also support networks, where members have some access to each other. Bebo and Facebook associate access controls with school attendance. Alternately, self-defined regions can be considered a network, and privacy controls may be associated with the chosen location.

Public Visibility: Sites define some subset of a profile (such as the user's name and affiliation) visible by default for searching and identification. Most sites also allow users to relax or strengthen their definition of public information.

Past work demonstrates that users have strong expectations for privacy on social networking sites.

In order to help users protect their personal data, the SNSs architecture adopts a simple user centric policy management approach, where a privacy aware user is able to specify a policy that manages access to their posted profile objects. There have been numerous studies concerning the privacy in the online world. A number of conclusions were drawn from these studies:

1. There are varying level of privacy control, depending on the online site. For e.g.: Some sites make available user profile data on the Internet with no ability to restrict access, while other sites limit user profile viewing to a set of selected trusted friends [6].
2. The individuals lack appropriate information to make informed privacy decisions [6].

Due to lack of user awareness and proper privacy protection tools, huge quantities of user data, including personal information, pictures and videos are quickly falling into hands of authorities, strangers, recruiters and the public at large [9].

II. Problem Defination

In today's scenarios all the websites have privacy policies so have the Social Networking Sites. Social Networking Sites are one of the most visited sites but they are still vulnerable. Our research work is to provide some additional Privacy Policies that are used to enhance the existing Privacy Policies of Social Networking Sites. Examples of this type of network are LinkedIn, Black Planet and Good reads.

Most SNS provide only a binary relationship: *friend or not.* As a result there is no similarly between the real life social network and online social graph model and violates our security principle of keeping consistency between online and offline social networks [4]. To keep coordination between the two, we can extend relationship model as:

1. Types of relationships: This can be roughly categorized into bidirectional relationships such as friend or colleague, and one directional relationship such as fans of followers.

2. Trust Strength: This expresses how much a user trusts other users either with respect to a specific topic (topical trust) or in general (absolute trust).

3. Interaction Intensity: This measures the quality and quantity of interactions between users.

A fundamental feature of SNSs is the online social graph that connects users. It collects the core information on which all the socialization services provided by SNS are based, therefore it should be primarily protected.

It is easy for a malicious user to obtain multiple fake identities and pretend to be multiple distinct users in the SNS. If the SNS requires users to register with government issued identity cards, the barrier against launching node forging attacks becomes much higher. A more promising approach is to utilize the web of relationships embedded in a real life social network to establish and verify users identity. The basic idea is that people are who they connect with, communicate with, or affine to. Although it is not difficult to register under alias, it is extraordinary difficult to change one's friends and contacts.

III. Literature Survey

Millions of people join social networking sites, adding profiles that reveal personal information. The reputations of social networking sites has been diminished by a number of incidents publicized by the news media (Chiaramonte and Martinez, 2006, Hass, 2006, Mintz, 2005, Read, 2006). Is it possible to join a network of millions of people and be able to trust all of them? This does not seem realistic. Since people are obviously joining networks and revealing information, what role does trust play in the use of social networking sites?

Members use these sites for a number of purposes. The root motivation is communication and maintaining relationships. Popular activities include updating others on activities and whereabouts, sharing photos and archiving events, getting updates on activities by friends, displaying a large social network, presenting an idealized persona, sending messages privately, and posting public testimonials.

Extreme volume of content uploaded to social networks has triggered widespread concerns over security and privacy [6]. Personal data revealed on social networks has been used by employers for job screening and by local law enforcement for monitoring and implicating students. Criminals have also capitalized on the trust users place in social networks, exploiting users with phishing attacks and malicious downloads. The disparate, contrasting set of threats posed to users has resulted in a number of refinements to privacy controls. However, one aspect of privacy remains largely unresolved: friends. As photos, stories, and data are shared across the network, conflicting privacy requirements between friends can result in information being unintentionally exposed to the public, deteriorating personal privacy [5]. As social network content is made available to search engines and mined for information, personal privacy goes beyond what one user uploads about himself; it becomes an issue of what every member on the network says and shares.

A. Privacy Issues in existing SNS's

Facebook and other social network sites pose severe risks to their users' privacy. At the same time, they are extremely popular and seem to provide a high level of gratification to their users. Based on the literature and theories examined, the following conclusions were given [7]:

- SNSs users have a limited understanding of privacy settings in social network services and, therefore, will likely make little use of their privacy settings.
- Perceived benefits of SNSs outweigh the observed risks of disclosing personal data.
- SNSs users are more likely to perceive risks to others' privacy rather than to their own privacy.
- SNSs users were more likely to change privacy settings if they reported a *personal* invasion of privacy than if they reported an invasion of privacy to *others.*

Some key issues of privacy in Social Networking Sites are:

1. The SNS that are currently available does not make user aware of the dangers of divulging their personal information or they do not want to read the privacy policy of the SNS.
2. The privacy tools are not much user friendly, they are very complex to understand and use.
3. Users can control who can access what in their profile but cannot control what others reveal about them.

B. Privacy Threats and Attacks

User provides SNS with some basic information such as name and email address to create their profile. Registered users can invite their friends to join the SNS. In some SNS we have facility to send invitation to all the emails saved in address books. Once a profile is created then user can share his information with other users on SNS, which is the most important characteristics of SNS [3]. User can post public messages in various forms like text, photo etc. on their personal space provided by SNS.

Many organizations take advantage of SNS to advertise their products and services and at the same time to stay in touch with people. With respect to hundreds of millions of users of SNSs, and large amount of data shared by them, social networks are treasures of personal and corporate data [3].

Ideal SNS should fulfill the following privacy requirements [11]:

1. *End-to-end Confidentiality:* All interactions are needed to be confidential and only sender and receiver should have access to data.
2. *Privacy:* Personal information of a user should not be disclosed to any party apart from those explicitly mentioned by the user.
3. *Access Control:* Users should be able to manage access controls of their profiles as well as attributes of their profiles. Users should be also allowed to grant permission to another user or a group of users.
4. *Authentication:* For satisfying the previous requirements, a receiver of a message should be able to authenticate the sender of the message as well as the attribute message.
5. *Data Integrity:* For each exchanged message whether it is a response or a request, origin authentication and also modification detection are needed to be performed.
6. *Availability:* Public data has to be always available and all messages should be delivered at any time.

Access control methods of many of the current SNSs are very weak. There is challenge of making a trade-off between privacy and the following factors [19]:

1. *Social Network Searching:* It is unattainable to hide all the information of a user's profile but allow users to find it by social searching. Same case is for traversing friend's profile.
2. *Social Network Interaction:* There is a privacy breakage risk through common friends. Details of users, e.g. school name, interests etc, might be exposed through the profile of their friends.
3. *Data Mining:* SNS data may be studied for analyzing social behaviors which in that social network is considered as graphs and users are their vertexes and relationships are their edges. Removing private data on the other hand, reduces the accuracy of result.

IV. Proposed Policies And Inmplementaation

Since SNS are widely in demand of current scenarios, the risk of their usage has also increased. Due to the lack of awareness among user and presence of less privacy protection tools, huge amount of user's data, including user's personal information, pictures and videos, is at risk. They can be used by strangers, recruiters and even the public at large, in any way in which they want.

None of the previous research conducted so far solves all the privacy risks.

A. Level of Privacy Control

To protect user privacy, all existing SNSs provide some level of privacy control that allows users to control who sees what in their profile. They are:

a) Profile Privacy: It controls who can see the user's profile and his personal information.
b) Application Privacy: It controls what information is available to installed applications.
c) Search Privacy: It allows who can see for user and how he can be contacted.

B. Profile Viewers

The Privacy Settings are not sufficient enough to control the privacy of data. It is not sufficient which kind of data to be disclosed but it is also necessary which data to be disclosed to whom. Classification of people who can see user data is as follows:

a) Close Friends: They are the people whom user trusts enough to share almost each and every information. They are the best friends of the user's real life.
b) Friends: They can be user's family members, relatives or friends in real life.
c) Known: They are the people about whom the user knows a little. They can be people known online or met once or twice.
d) Visitors: They are the user's who are not in our friend list but visit the user profile to know about him.

C. Proposed policies and their implementation

The privacy tools in SNS are not flexible enough to protect user data. Most popular SNS, Facebook provide very detailed privacy setting, but current Facebook's privacy interface is too complex to understand by most normal users. Our target is Privacy settings to be simple, even understandable by the normal users.

Here we propose some privacy policies that serve as a resolution for the privacy issues identified in previous section. These policies when implemented can enhance as well as complement the privacy framework of existing SNS's.

To implement the policy proposed, we proposed a frame work in php and our implementation shows whether the given policies are applicable on a social networking site or not. Here in this paper we have shown the snap shot of only two webpages.

***a) Album Privacy Policy*: -** The user should be provided with an option to customize the access permission on the album and also on selected photographs of an album.

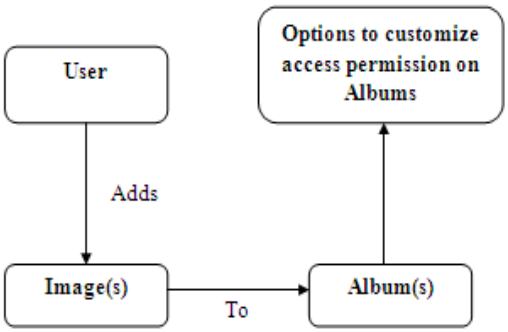

Fig 1. Album Privacy Policy

Album privacy policy is needed to maintain the privacy on specific album of the user. There are three level of privacy:

- Private
- Protected
- Public

Private Albums are visible to only user itself
Protected Album van be seen by only Closed Friends and Friends
Public Albums are visible to all.

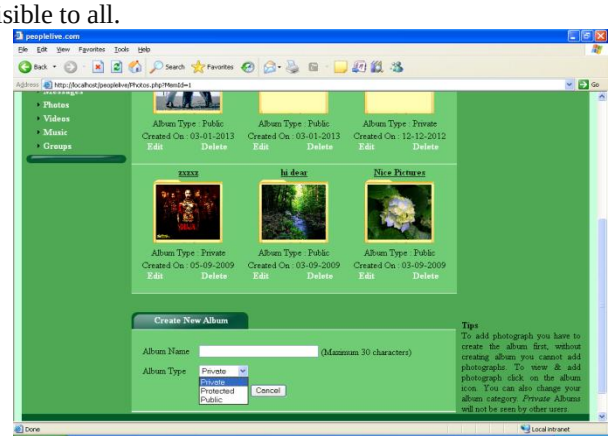

Fig 2. Album Type specification

Reason: Suppose a user adds an album on his profile, but he wants' different access permissions for different images or different albums then he cannot do this. So to provide user with this customization this policy is proposed.

***b) Image Protection Policy*:-** User can protect their images from being copied of downloaded by other users. By default Close Friends can see user's protected images while Friends, Known can see user's public images (user can change this access level also). But then also nobody can copy or download user's images. To download an image Close Friends, Friends and Known need to send a message to user. When user approves the message then only it can be downloaded.

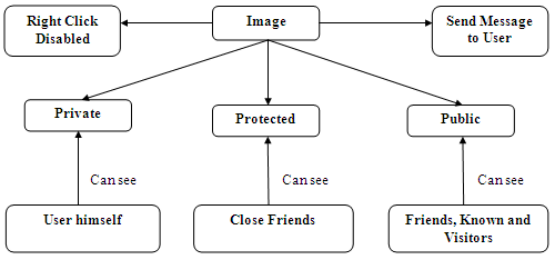

Fig 3. Image Protection Policy

Reason: Images privacy is of important concern. But without image being uploaded on SNS, SNS's charm will be reduced. So we provide privacy in images so that unauthorized user cannot download the image and edit it into something inappropriate to harm the user.

Image Protection Policy is needed to protect an individual image. In this when an image is added to a Private Album it is by default private. When image is added to Protected Album, it can be private or protected but not public. When image is added to Public Album, it can be private, public or protected.

Fig 4. Image Protection Policy

***c) Image Tagging Policy*: -** When a person tags a user, in Facebook user has option whether it will be displayed on his timeline or not, but we provide more customized option user will have option to accept or reject the tag. When user presses "yes" the tagged image appears on user's timeline, when he presses "no" his name is removed from tag. Once a user is tagged in an image he has option to delete that image also, if he finds it not appropriate. Only *Close Friends* or *Friends* can tag an image, *Known* and *Visitors* cannot do it.

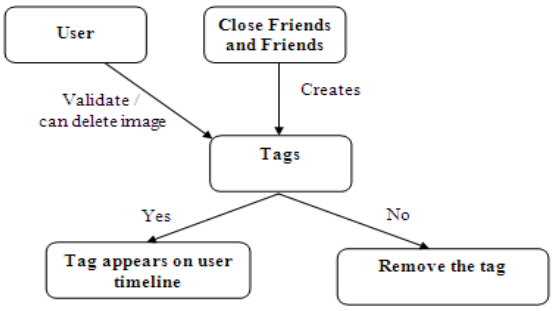

Fig 5. Image Tagging Policy

Reason: User's in SNS can control access to their profile but cannot control what others reveal about them. E.g.: A user can upload an embarrassing photo of friend and can directly tag it to friend's profile. So to solve this problem I propose this policy.

***d) Customizing Access on Tagged Images*: -** Access Customization by user on Tagged images. When user is tagged in an image every one can see him but user should have option to customize which friend can see which image.

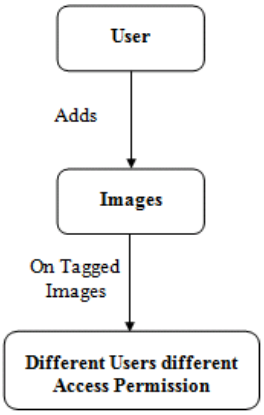

Fig 6. Customizing Access on Tagged Images

Reason: - By approving the tagged image we allow every friend of ours to view that image. However, there may be situations in which we would want to screen the viewers of that image. So that specified users can only view the tagged image of the user.

V. Conclusion And Future Work

This is a relatively new field and there is a tremendous potential for future research because of the recent increase in the number of users in SNSs. In this work we examined the existing privacy policies of some of the most common Social Networking Sites like Facebook, MySpace, and LinkedIn etc. While studying about the privacy policies we tried to keep in mind the requirements of Social Networking Sites users.

We studied the existing privacy policies and flaws in them for different Social Networking Sites. Keeping in mind the weakness of existing policies we suggested certain modifications in them.

In support to our proposed policies and to test their implementation feasibility, we have tried and implemented 4 of our policies. For this we designed our SNS in php which has the primary features of any Social Networking Site like Facebook. Then we implemented few of the proposed policies on it.

In future, we intend to extend our privacy policies that offer an easy and flexible way to user so that they can communicate with each other and the third party application without revealing much about them. We also aim at proposing a Privacy Policies Framework, which can easily be integrated with the existing one or even can be replaced.

References

[1] Vorakulpipat, C.; Marks, A.; Rezgui, Y.; Siwamogsatham, S.; , "Security and privacy issues in Social Networking sites from user's viewpoint," *Technology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET '11:* , vol., no., pp.1-4, July 31 2011-Aug. 4 2011

[2] Joshi, P.; Kuo, C.-C.J.; , "Security and privacy in online social networks: A survey," *Multimedia and Expo (ICME), 2011 IEEE International Conference on* , vol., no., pp.1-6, 11-15 July 2011

[3] SeyedHossein Mohtasebi and Ali Dehghantanha, "A Mitigation Approach to the and Malware Threats of Social Network Services ," *Multimedia Information Networking and Security, 2009. MINES '09. International Conference*, vol.1, no., pp.448-459, 2011

[4] Chi Zhang; Jinyuan Sun; Xiaoyan Zhu; Yuguang Fang; , "Privacy and security for online social networks: challenges and opportunities," *Network, IEEE* , vol.24, no.4, pp.13-18, July-August 2010

[5] Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, " State of the Art: Automated Black-Box Web Application Vulnerability Testing", *IEEE Symposium on Security and Privacy*, 2010, 1081-6011

[6] Anna C.Squicciarini, Mohamed Shehab, Joshua Wede, "Privacy policies for shared content in social network sites ", *The VLDB Journal(2010)* 19:777-796,DOI 10.1007/s00778-010-0193-7

[7] Debatin, B. et al., 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.

[8] Ai Ho; Maiga, A.; Aimeur, E.; , "Privacy protection issues in social networking sites," *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* , vol., no., pp.271-278, 10-13 May 2009

[9] Aimeur, E.; Gambs, S.; Ai Ho; , "UPP: User Privacy Policy for Social Networking Sites," *Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on* , vol., no., pp.267-272, 24-28 May 2009

[10] Xi Chen; Shuo Shi; , "A Literature Review of Privacy Research on Social Network Sites," *Multimedia Information Networking and Security, 2009. MINES '09. International Conference on* , vol.1, no., pp.93-97, 18-20 Nov. 2009.

[11] Cutillo, L.A., Molva, R., Strufe, T., "Privacy preserving social networking through decentralization, Wireless On-Demand Network Systems and Services", In: WONS 2009: *Sixth International Conference*, pp. 145-152 (2009).

[12] Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of AMCIS 2007, Keystone*, CO. Retrieved September 21, 2007

[13] Sophos security threat report 2011 (2011) *https://secure.sophos.com/securitywhitepapers/sophos-security-threat-report-2011-wpna*

[14] DotRights Social Networking Page, *www.dotights.og/social-netwoking*