Privacy issues in Online Social Networks

M.A. Devmane
P.V.P.P's college of Engineering
University of Mumbai
INDIA

N.K. Rana
Theem college of Engineering
University of Mumbai
INDIA

ABSTRACT
The popularity of online Social Networks (OSN) is increasing tremendously. OSN enable people to connect with their friends as well as share information about their personal life. While most of the leading social platforms have primitives for providing privacy in the platform and the applications they are insufficient. There are some serious privacy problems that need to be resolved in existing OSN. There has to be a method to protect user-provided data in the profile as well as user-generated data by the OSN providers. Similarly a fully flexible and dynamic access control mechanism should exist to protect private data against attackers and unauthorized users .The access control system should be efficient in managing the privacy policies of OSN users.

General Terms
Cyber Security, privacy, social network services.

Keywords
Online Social network, privacy, cyber security, revelation of information

1. INTRODUCTION
Literally, privacy means the right to be independent of every external interruption or interference and become free by oneself. It can also be referred as the right to prevent one's personal information from being exposed to others. The Online Social Network (OSN) has shown tremendous growth in a very short span which is clear from the thing that day by day the number of OSN users is increasing .The user base of facebook alone has crossed 800 million around the globe. Almost everyone is member of at least one of the Online Social Networks. The OSN user can easily find his friend by searching the OSN.

The digital presence of a user on the OSN is known as his profile .The OSN allow the user to create his profile as well as list of contacts .The OSN allows user to edit, update the profile based on his requirements. The profile contains photo, first name, last name, date of birth, E-mailID, Mobile Number, work place, home town, his current location etc [10].Most of the OSN publish the activities of user in his own account to all other people in his contacts list. So by this way there is a kind of communication. Communication in OSN can also be formed by placing images, messages or attachments on the wall of the relevant contact. The contacts on the OSN can be increased largely by being a member of a group so whatever discussion is taking place on the group is visible to each and every member as well as the member will get the E-mail from the Online Social Network.
New contacts can be added by the user by searching for his friend on the OSN .The OSN provides a search engine to search friends based on certain criteria like student of same school, college, belongs to same home town, having similar interest and so on. A friend request can be send to such person. Similarly the people who may be friends based on certain criteria are shown to the user so that the friend can be added if the person is a friend of the user.

2. DISCLOSURE (REVELATION) OF INFORMATION

The basic motivation to be a member of OSN is to establish connections with others, so it is necessary for the user to provide his information so that someone else can identify and communicate with him. Apart from the mandatory fields like name, date of birth ,E-mail etc. the user try to provide maximum information like photo, contact home town, work place ,mobile number etc.

Apart from the above fields the OSN provides flexibility to the user to add information about his school, college, other interests, activities and so many other things. By providing such information on the OSN it is easier to get more connections of people having same school, college as well as same interest, activities and so on. By revealing such maximum information the user is not only attracting his friends but strangers also. It is found that on facebook on an average every user is having 150 contacts / friends [2].

Other than the profile of user lot many other things are present on his webpage. The wall contains the posts written by his friends which sometimes may contain sensitive information. The webpage also contains photos uploaded / published by the user. It also contains the list of friends of the user by using which it is possible to access their webpages [4]. The messages section in Facebook contains short messages which are send to the user by his friends.

By making some sensitive/ private fields accessible to everyone there are chances of personal information leakage [4][5]. The absence of personal information privacy oversight leads to the personal information leakage. In addition or as an alternative to the deployment of privacy preserving techniques, one may consider methods of detecting or discouraging leaks of sensitive information [6]. It is observed that the OSN users are not that much careful about the privacy of their profile in this digital world of OSN. The privacy may be at risk in social networking sites, information is willingly provided. Different factors are likely to drive information revelation in Online Social Network [4].

Due to some of the inbuilt properties the OSN are more prone to security threats.

- Very large and distributed user base.
- Group of users based on particular attribute like organization where he work, interest etc.
- The Online Social Networks allows user to post their own applications on the OSN which will be accessible by all others.

These features are used so many times to perform attack on the OSN [5][13].

Privacy is of paramount importance in the OSN since the illegal disclosure and improper use of the user's private data can cause undesirable or damaging consequences in people's lives. The visibility of users varies across the OSN [8].Generally the term Openness Level[OL] to measure how information in a social network could be accessed. E.g. "OL= Public" means accessible by everyone including crawlers .Social network in this category are best in visibility but worst in preserving privacy. "OL=Registration Required " preserves better privacy [9].The users of OSN believe that whatever messages they get in the OSN are trusted as it comes from their friend or acquaintances.

The fields in the profile are having some privacy settings which are to be set by the profile owner .e.g. name is having default setting as visible to everyone .The date of birth may be having privacy settings like everyone, friends, friend of friend, and custom .if it is set as friend of friend then it will be accessible to the people who are in the contact list as well as people who are in contact list of these people. In the custom setting the setting can be done by the user as per his preferences. Unfortunately current trend in OSN indirectly requires user to become system and policy administrators to protect their online contacts. This is further complicated the privacy of user due to rapid growth of OSN along with providing new services on OSN platform [10]. Apart from this the user doesn't know who may look at his private data he put online [11].

User's information disclosure can be helpful to other users, companies and third parties. Particularly, private information is very valuable when the information of many people is gathered on OSN. It provides data source for marketing and data mining. The recent surge in popularity of online social network applications raises serious concerns about the security and privacy of their users. Beyond usual vulnerabilities that threaten any distributed application over internet, online social networks raise specific privacy concerns due their inherent handling of personal data.

3. PRIVACY ISSUES IN OSN

The relation between privacy and a person's social network is multi-faceted.in certain cases we want to share the information with a few number of people whereas at some another time or occasion we may want to share the information with so many people in our real life [4] same thing is valid for OSN. Most of the users lack awareness of the privacy risks posed by sharing their personal information on the OSN [14].The privacy settings for most of the fields in the OSN are like accessible to everyone, friend, friend of friend, custom setting whereas the default setting is accessible to everyone. It is observed that at the time of registration with the OSN, user doesn't take these privacy settings seriously, so most of the data remains accessible to everyone. This leads to loss of privacy or personal information leakage. Malicious or curious users take advantage of such privacy settings and get access to the private data of the user and can use it for unethical purpose.

Existing research on web security and privacy falls short since most of the researchers prevent the user from providing information with which he is not comfortable. From the OSN point of view where it is necessary to provide at least the mandatory information to get accessible to outside world i.e. friends etc. [13].Most of the OSN are designed to make it easy for you to find and connect with others , for this reason the name and profile picture do not have privacy settings. The posts or photo uploading or status update it is possible to control exactly who can see it at the time you create it. This sharing can be controlled by clicking on the lock icon and selecting proper privacy settings. If certain fields are having privacy settings as "everyone" and one of the friend in the contact list connects with an application or website using the OSN platform, then the application or website will be able to access the content marked as accessible to everyone.

It is observed that so many OSN users simply accept friend request or send friend request though he does not know the person in real life or he may not be the same person as assumed by the user sending/accepting friend request. Such habits will lead to privacy breaches because whatever data / fields are accessible to the friends of profile owner will be used by such people and the private / sensitive information can be misused [14].

Even such simplest form of privacy breach can lead to havoc as 75,000 out of 2,50,000 facebook users accepted the friendship request which was actually generated by using automated script [14].which clearly indicate that the particular user can now get access to more than 75,000 user's data on facebook which can be utilized for any of the purpose.

Similarly some additional functionalities are added by the user by using some of the third party applications which can be used with the OSN. Though these third party applications are using the OSN as a platform they doesn't belong to the OSN and so they may not be trustworthy. Such applications mostly ask the user to grant permission to access some data from the profile t o run the application. Most of the time such applications do not specify exactly which data it will access. So once the user permits access to the profile data, the application can access any data and which may lead to loss of privacy of the user.

There are several data mining techniques that are widely used on OSN .The process of gathering and managing personal information has been making a big step as the OSN comes up. In the age of web2.0, social network sites are really varied and colorful. More applications, videos, pictures are upload on the sites, which provides rich sources for data mining. Through data mining, fragments of user's information can be integrated. Somehow, a whole personal file will be leaking out. Data mining is the process of extracting hidden patterns from data. Comparing to data mining techniques, direct attacking techniques are the real dangers which users should protect them from.

3.1 Privacy features of Facebook

From the privacy point of view the OSN are taking due care and display their privacy policy on the website .here some of the privacy features of Facebook are discussed. As per the privacy policy user's name, profile picture, networks,

username and User ID are treated just like information the user choose to make public [15].Facebook may also receive information about the user from the games, applications, and websites the user uses, but only when you have given them permission.

Sometimes facebook get data from advertising partners, customers and other third parties that help to deliver ads, understand online activity, and generally make Facebook better.

Choosing to make user's information public also means that this information can be associated with him (i.e. name, profile picture, Facebook profile, User ID, etc.) can show up when someone does a search on Facebook or on a public search engine. It will be accessible to the games, applications, and websites the user and his friends use. It will be accessible to anyone who uses facebook APIs such as Graph API.

Sometimes the user will not be able to select an audience when he post something like writing on a someone's wall or comment on a news article that uses comments plugin. This is because some types of posts are always public posts. As a general rule, he should assume that if he does not see the sharing icon, the information will be publicly available. When others share information about the user, they can also choose to make it public. If the user does not want his information to be accessible through facebook APIs, he can turn off all Platform applications from his Privacy Settings. If he turns off Platform application he will no longer be able to use any games or other applications.

Deactivating facebook account puts the account on hold. Other users will no longer see the user's profile, but facebook do not delete any of the information. Deactivating an account is the same as the user telling facebook not to delete any information because he might want to reactivate the account at some point in the future[15].

When the user deletes an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. The user should only delete his account if he is sure he never want to reactivate it.

3.2 Google+ Privacy features

In order to use Google+, the user must have a public Google Profile visible to the world, which at a minimum includes the name he chose for the profile. That name will be used across Google services and in some cases it may replace another name the user has used when sharing content under his Google Account. Google+ may display user's Google+ Profile identity to people who has his emailID or other identifying information. The Google+ is having circles. Circles are groups of people with whom the user share content. The names of circles and who are added to them are visible only to the user, though he can set whether the list of people in all of his circles is visible in his public profile [16].

Posts and other content shared by or with the user - such as photos - may be visible on his profile to those with whom that content has been shared. He can use the profile editor to see how the profile appears to particular ndividuals. The user may choose to access Google+ through third-party applications (e.g. non-Google websites) by authorizing these applications to access all or part of his Google+ account via the Access Request page. The developer of the application may have access to his email address and to the other content such as the content friends have shared with him. The developer may also request additional information from the user, such as his location for mobile features of Google+. The user can revoke the developer's access to his Google+ Account at any time by doing changes in the settings.

On the basis of the study of information revelation, privacy and the countermeasures suggested thereon can be classified as shown in the figure 1.

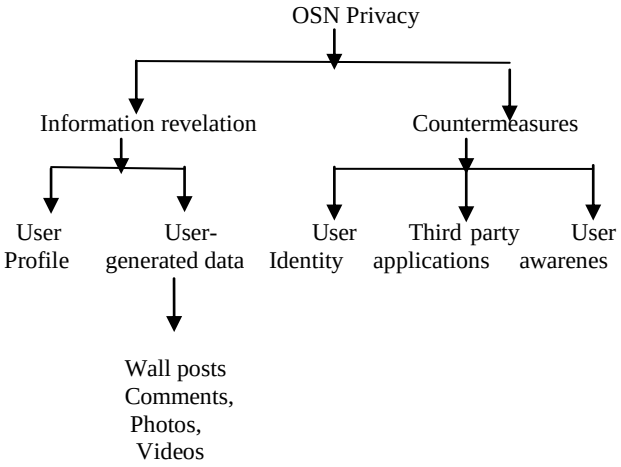

Fig. 1 OSN Privacy

4. CONCLUSION

Current risks of privacy on OSN, privacy policies and some protection methods status quo are summarized and reviewed in the paper. Information acquisition can be done directly accessing the profile by using an attack technique and data mining techniques. To overcome most of the privacy issues it is necessary to have the user education about importance of privacy of his personal data. The user should only provide the information he is perfectly comfortable with .The user should add only the people whom he knows or trust. He shouldn't blindly add anyone in the contacts as the friend may be having access to maximum information of the user which can be misused. To avoid fraudulent accounts the OSN should ask for some mandatory fields like PAN, Driving License No. etc. and it should be crosschecked with the government database and then only the account should be enabled. Further research on the new topics and privacy protection problems will accelerate the development of OSN as well as the applications designed for it.

5. REFERENCES

[1] Chi zhang , jinyuan sun,xiaoyan zhu , yuguang fang , " privacy and security for online social networks : challenges and opportunities " , IEEE Network July / August 2010 PP 13-18 .

[2] Na li , nan zhang , sajal das , " preserving relation privacy in online social network data" , IEEE Internet computing MAY / JUNE 2011 PP 35-42

[3] Ralph gross , alessandro acquisti , "Information revelation and privacy in online social networks " , ACM workshop in the electronic society WPES 2005 .

[4] Danesh Irane, steve webb, calton pu , " Modeling unintended personal information leakage from multiple online social networks " ,IEEE Internet computing May / June 2011 PP 13-19 .

[5] Andreas makridakis , elias athanasopaulos , spiras antonmatos , demetres antoniades et. Al. , " Understanding the behavior of malicious applications in social networks " , IEEE Network September / October 2010 PP 14-19 .

[6] Phillippe golle , frank Mcsherry , ilya miporonov , " Data collection with self-enforcing privacy " , ACM transactions on Information system security Vol. 12, No. 2,Article 9 Dec 2008 PP 9.1 – 9.24 .

[7] Mohamad badra , samer Ei-sawda , Ibrahim hajjeh , " Phishing attacks and solutions ", 3rd international conference on mobile multimedia ,Greece August 2007

[8] Justin Zhan , " Secure collaborative social networks ",IEEE transactions on systems , man, and cybernetics-part Capplication and reviews VOL 40, No. 6 NOV. 2010 PP 682-689 .

[9] Bo luo , dongwon lee , " On protecting information in social networks : A proposal ".

[10] Gail joon nahn ,Mohamed shehab , anna squicciarini , " security and privacy in social networks " , IEEE Internet computing MAY / JUNE 2011 PP 10-12.

[11] Marc donner , " Privacy and the system life cycle " ,IEEE Security and Privacy March/ April 2011 PP 3

[12] Amin Tootoonchian, Stefan serolu , yashar ganjali , alec wolman " Lockr : better privacy for social networks " , ACM CoNEXT ,Itali Dec2009 PP 169 – 180 .

[13] Weimin Luo, jingbo liu , jing lui , chengyu fan , " An analysis of security in social network " Eighth IEEE international conference on dependable , automatic and secure computing , IEEE 2009 PP 648 – 651 .

[14] Hongyu Gao , Jun hu , tuo Huang , Jingnan wang , Yan chen , " The status quo of online social network security : a survey " ,IEEE 2011 PP 1- 6 .

[15] www.facebook.com/full_data_user_policy accessed in DEC 2011.

[16] www.google.com/intl/en/+/policy accessed in DEC 2011.