Achieving Non-Conflict OSN Model Using Online Social Graphs

[1]L.Venkateswara Reddy, [2]Vendoti Monica Reddy and [3]Lakshmi Paidimarri

[1]Professor, Dept of IT, Sree Vidyanikethan Engg. College,
E-mail: Lakkireddy.v@gmail.com
[2]Dept of CSE, Sree Vidyanikethan Engg. College,
E-mail: monicar564@gmail.com
[3] Dept of CSE, Sree Vidyanikethan Engg. College,
E-mail: lakshmipaidimarri@gmail.com

***Abstract* - Online social networks such as Facebook are among the most popular sites on the Web and continue to grow rapidly. They provide mechanisms to establish identities, share information, and create relationships. The resulting social graph provides a basis for communicating and distributing and locating content. Even if social networks are now widely used ,their security and privacy remain challenging because of the tension between sharing information and ensuring privacy. This workshop is intended to discuss the current security and privacy issues of social network and explore new ways to address them. Evaluating goals in context of usage of osns will give conflicts. By developing relationship and protecting social graphs conflicts may be reduced upto some extent.**

***Key words* – OSN Model, Social Networks, Web, Online.**

1. INTRODUCTION

online social networks (OSNs) [1, 2] such as Facebook, MySpace, and Twitter enable people to stay in touch with their contacts, reconnect with old acquaintances, and establish new relationships with other people based on shared features such as Communities, hobbies, interests, and overlaps in friendship circles. According to Boyd and Ellison [1] and Wikipedia [2], an OSN is characterized as follows

It provides a platform to:

Allow users to construct digital representations of themselves (usually known as user profiles) and articulate their social connections with other users (i.e., lists of contacts).Support the maintenance and enhancement epresenting iconic fictional characters: celebrities, f preexisting social connections among users in the concepts, and other such entities. hysical or virtual world.

Help forge new connections based on common interests, location, activities, and so on.

It is therefore not surprising that stories about privacy breaches by Facebook and MySpace appear repeatedly in mainstream media [3-4].

2. EARLY SOCIAL NETWORKS

Forums:

Online forums also played a large part in the evolution of the social web. These were really descendents of the BBSs popular in the 70s and 80s, but usually came with a more user-friendly interface, making them easier for non-technical visitors to use. Various forum platforms, including **vBulletin** and **phpBB**, were developed, many of which are still used for forums. Forums remain a popular part of online culture, and many have made strides to add more social networking-type features (like profiles).

3. MAJOR ADVANCES IN SOCIAL NETWORKING

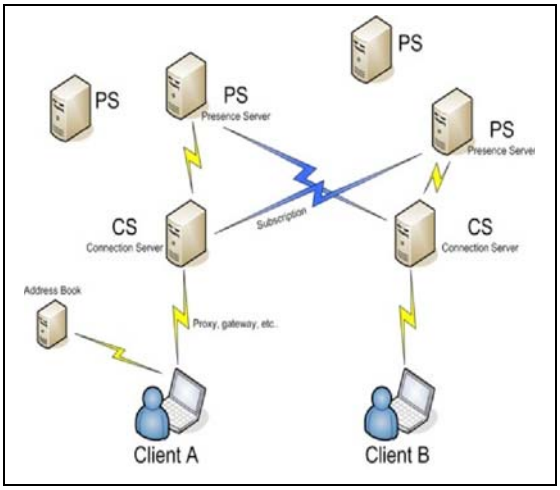
The early 2000s brought some huge developments in social networking and social media.

Friendster was really the first modern, general social network. Founded in 2002, Friendster is still a very active social network, with over 90 million registered users and 60+ million unique visitors each month. Most of Friendster's traffic comes from Asia (90% of it). The initial design of Friendster restricted users from viewing profiles of people who were more than four degrees away (friends-of-friends-of-friends-of-friends). In order to view additional profiles, users began adding acquaintances and interesting-looking strangers to expand their reach. Some began massively collecting Friends, an activity that was implicitly encouraged through a "most popular" feature. The ultimate collectors were fake profiles

4. CLIENT SERVER ARCHITECTURE AND PEER TO PEER FOR A THREE TIRE DESCRIPTION OF OSN

4.1 IN ONLINE SOCIAL NETWORK:

Let's say that the client **A** wants to contact the client **B**. The client a logs in a **CS**(**Connection Server**) through a persistent TCP connection (eventually using proxy,gateway..). Behind the CS there are the **PS** (**Presence Server**).Each person get always the same particular PS, which is where your personal status message, description of your user photo and similar things are stored



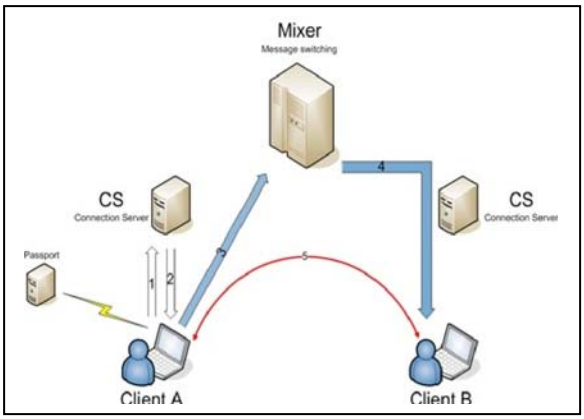
Another element of the architecture is the **Address Book**. The client A gets directly from the Address Book his list of contacts.

Then the client **A** tells to his **CS** who his friends are, the CS subscribes to his friend's **PS** to get the presence information that are sent up through the client server connection.

If the client **A** change his status to OffLine for example, the change goes up to the **CS** of A, then to the **PS** of A, then down to the **CS** of B through the subscription and then down to the client **B**.

CHAT

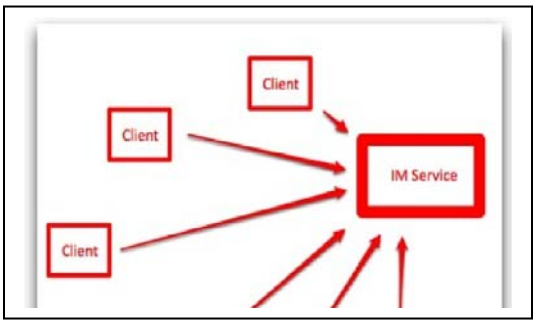
If the client **A** wants to chat, tells to his **CS** that wants to contact somebody, and the CS tells **A** to contact a **Mixer**, which sends IM traffic to a destination, for example to **B** (passing through the CS of B). Then A and B can communicate through the Mixer.

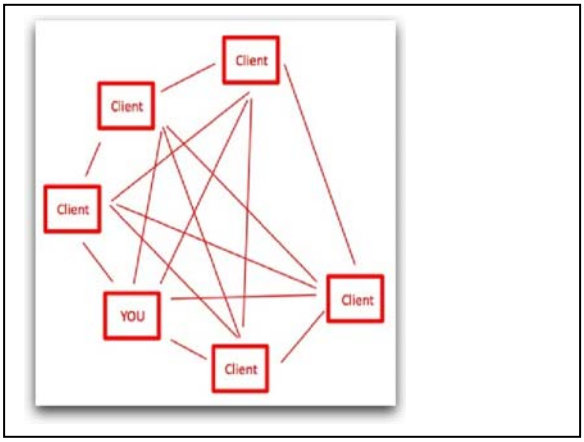


When the clients A and B wants to send larger pieces of data (big files, audio, video) then they use the **Peer-to-Peer[7-8]** technology. So A and B set up a **Session** through the Mixer. They need to know how to set up a direct connection, secure connection, IP addresses, protocols supported, NAT or firewall's information and so on. If the peer to peer connection fails A and B can always set up a connection through the Mixer.

4.2 IN OFFLINE SOCIAL NETWORK:

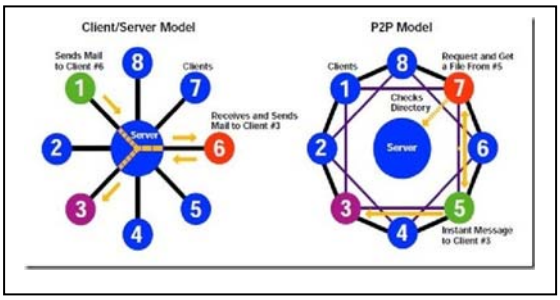
Client –server





Peer to peer

4.3 IN COMMUNICATION NETWORK:



5. PRIVACY AND SECURITY:

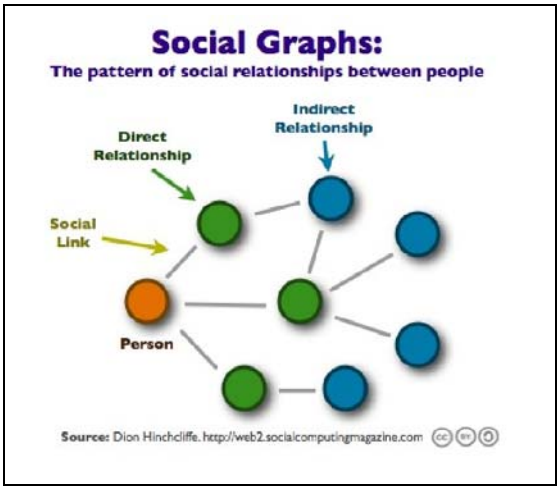
To sum up, a user's privacy requirement[6] is twofold First unauthorized entities (i.e., who are not granted access to the private data) must not learn the content of the private data which reveals identifying information of the data owner. Second, unauthorized entities must not be able to link multiple private data files to profile the owner, indicating that the stored or transmitted private data should appear random and leak no useful information. This private data can also fall nder the control of hackers. Given the reality of privacy breaches by centralized OSN providers, as exemplified by Facebook's beacon application [1, 4, 5], there is a motivation for giving control over data back to the users and not having one entity access all personal data of the users in the OSN.

Security requirements, including *availability* (i.e., data published by users has to be continuously available) and *accountability* (i.e., misbehavior of users should be traceable), must also be satisfied.

6. REDUCING CONFLICTS

6.1 USING ONLINE SOCIAL GRAPHS

The term "the social graph" usually refers to the connections between people who participate in social networking service, such as Facebook, LinkedIn. A fundamental feature of OSNs is the online social graph that connects users. It collect the core information on which all the socialization services provided by OSNs are based therefore, it should be primarily protected.



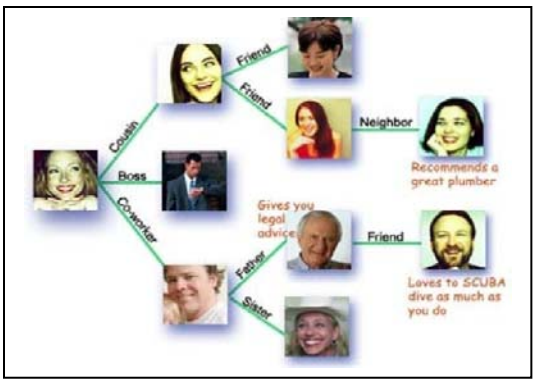
6.2 ENRICHED RELATIONSHIP MODEL

Relationship model includes:

a. Type of relationships

b. Trust strength

c. Interaction intensity



7. CONCLUSION

Social networking relates to audience research in that it is a new and very improved way of finding out exactly what consumers want. Whereas before, marketers could only look at consumers' buying patterns, behaviors and what surveys said, they can now go to the audience directly. Network users are publicizing their interests, wants and needs. Companies can then take this information and use it to better market their products and services to the target audience. Here it reduces conflicts by protecting online social graph.

REFERENCES

[1] d. m. boyd and N. B. Ellison, "Social network sites: Definition, history,and scholarship." Journal of Computer-Mediated Communication, vol.13(1), 2008.

[2] Wikipedia, “Social Network Service,” 2010; http://en.wikipedia.org/wiki/Social_network_service.

[3] S. B. Barnes, “A Privacy Paradox: Social Networking in the United States,”First Monday, vol. 11, no. 9, Sept. 2006

[4] R. Gross and A. Acquisti, “Information Revelation and Privacy in OnlineSocial Networks,” Proc. WPES ‘05, Alexandria, VA, Nov. 2005

[5] B. Krishnamurthy and C. E. Wills, “Characterizing Privacy in Online SocialNetworks,” Proc. WOSN ‘08, Seattle, WA, Aug. 2008.

[6] J. He and W. W. Chu, “Protecting Private Information in Online Social Networks,”in Intelligence and Security Informatics: Techniques and Applications,H. Chen and C. C. Yang, Eds., Springer, 2008

[7] S. Buchegger et al., “A Case for P2P Infrastructure for Social Networks —Opportunities and Challenges,” Proc. WONS ‘09, Snowbird, UT, Feb. 2009.

[8] S. Buchegger and A. Datta, “PeerSoN: P2P Social Networking — Early Experiences and Insights,” Proc. SocialNets ‘09, Nuernberg, Germany, Mar. 2009.