ISSN:0975-9646

Privacy Conflicts for Collaborative Data Sharing in Online Social Network

Sandip S. Shirgave, Prof. Subhash V. Pingale, Dr. K. J. Karande

Department Of Computer Engineering
SKN Sinhgad College of Engineering
Korti, Pandharpur, India-413 304

***Abstract*— Web based online social networks (WBOSN's) are online group of peoples where online user can establish relationship with each other and share information and resources across the web with other online and offline users. With the dramatic increase of online users on social network websites, the need to assist users to manage their large number of online contacts as well as providing privacy protection become more and more difficult. These social network users may share sensitive and personal information with large number of online known and unknown users. Providing the security to online shared personal and sensitive information is very hard. Current social networking sites not provide any mechanism to privacy concerns over data related to multiple users. This paper we have a tendency to going study regarding different methods used by different authors.**

Keywords- social, security model, Privacy Disclosure, Social Networks

INTRODUCTION

Social networks are of significant importance in various application domains such as marketing, psychology, and epidemiology and homeland security. Social networks often contain some private information about individuals as well as their sensitive relationships. We define an online social network to be a system where (a) users are first class entities with a semi-public profile, (b) users can create explicit web links to other users or content items, and (c) users can navigate the social network by browsing the links and profiles of other online social users.

Online social networks having a number of many purposes. First, online social networks are used to maintain and to make new social connections. The online social network sites allow online social users to communicating with other online users who are already a part of their extended social network. Second, online social networks are used by each online user to upload her own information and contents. The information shared often varies from social site to another social site, and sometimes is only the user's profile information itself. Third, online social networks are used to find old and new online users, interesting information and content by filtering the search criteria in the social network. Online Social Network provides each online user with a virtual space containing profile information, a list of the online user's friends, and Web Pages which are related to online users, such as orkut, where online users and friends can post content and send messages to other user. A online social network users profile having information with respect to the users birthday, gender, interests, education, and work history, mobile number, home address. In addition, online social users can not only upload content into their own or others spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space.

Online Social Networks currently provide simple access control mechanisms for users to control the information shared in the online space. For example, when a online user uploads a video and tags friends who appear in the video, the tagged online friends cannot modify the privacy setting because owner of video having full access over the uploaded content.

Following figure depicts an example of multiparty social network representation. It describes relationships of five online users, Sandip (A), Yogesh (B), Nitin (C), Aatish (D), and Jayant (E), along with their relations with data and their groups of interest. Note that two online users may be directly connected by more than one edge labelled with different relationship types in the relationship network. For example, in above Figure, Sandip (A) has a direct relationship of type colleague Of with Yogesh (B), whereas Yogesh (B) has a relationship of friend Of with Sandip (A). In addition, two online users may have transitive relationship, such as Friend Of friend, colleagues-of-colleagues and classmates-of-classmates (LOL) in this example. This example shows that some data items have multiple controllers. For instance, Relationship A has two controllers: the owner, Sandip (A), and a stakeholder, Nitin (C). Also, some users may be the controllers of multiple data items.

For example, Nitin (C) is a stakeholder of Relationship A as well as the contributor of Content E. Furthermore, we can notice there are two groups in this example that users can participate in: the Fashion group and the Hiking group, and some users, such as Yogesh (B) and Aatish (D), may join in multiple groups.

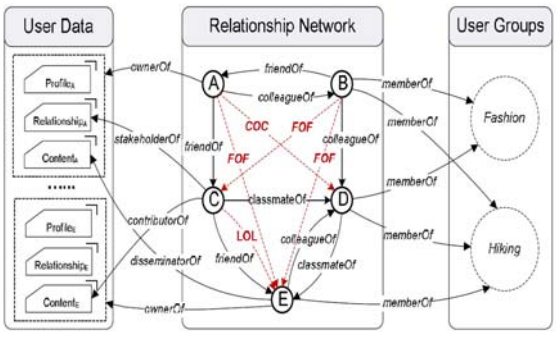


Figure 1:- An example of multiparty social network representation.

LITERATURE REVIEW

a. Identifying hidden social circles for advanced privacy configuration

With the dramatic increase of users on social network websites, the needs to assist users to manage their large number of contacts as well as providing privacy protection become more and more evident. Unfortunately, limited tools are available to address such needs and reduce users workload on managing their social relationships. To tackle this issue, author propose an approach to facilitate online social network users to group their contacts into social circles with common interests. Further ,author leverage the social group practice to automate the privacy setting process for users who add new contacts or upload new data items. Author evaluate his approach using real-world data collected through a user study. Author also includes an analysis of the properties that are most critical for privacy related decisions.

In this paper, author proposed an approach which helps users in managing their social network contacts into relevant groups automatically, and also helps users set up their privacy policies automatically for their uploaded content. Organizing
contacts into groups helps users set privacy settings for newly added content or new contacts joining their social circles.

b. A Privacy Preservation Model for Facebook-Style Social Network Systems

Recent years have seen unprecedented growth in the popularity of social network systems, with Facebook being an archetypical example. The access control paradigm behind the privacy preservation mechanism of Facebook is distinctly different from such existing access control paradigms as Discretionary Access Control, Role-Based Access Control, Capability Systems, and Trust Management Systems.

Authors work takes a first step in deepening the understanding of this access control paradigm, by proposing an access control model that formalizes and generalizes the privacy preservation mechanism of Facebook. The model can be instantiated into a family of Facebook-style social network systems, each with a recognizably different access control mechanism, so that Facebook is but one instantiation of the
model.

Author also demonstrate that the model can be instantiated to express policies that are not currently supported by Facebook but possess rich and natural social significance. This work thus delineates the design space of privacy preservation mechanisms for Facebook-style social network systems, and lays out a formal framework for policy analysis in these systems. Author formalized the distinct access control paradigm behind the Facebook privacy preservation mechanism into an access control model, which delineates the design space of protection mechanisms under this paradigm of access control. Author also demonstrated how the model can be instantiated to express access control policies that possess rich and natural social significance.

PROPOSED WORK

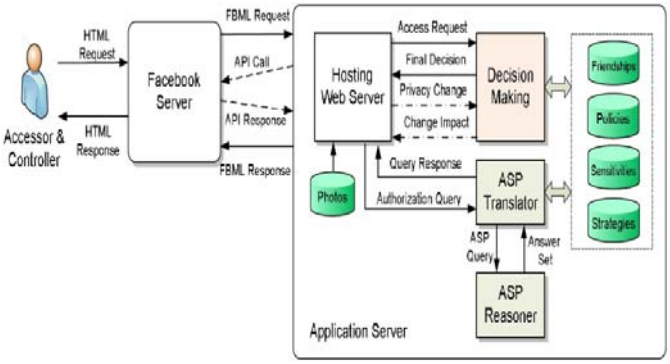


Figure 2:- Overall Architecture Of Socialcontroller Application

The architecture of Socialcontroller, which is divided into two major parts: social server and application server. Firstly the social server provides an entry point via the social web application page, and provides references to photos of online users, friendships between two online social users, and feed data through API calls. A social server takes inputs from online social users, and then gives the input to the application server.

The given application server is responsible for the input processing and collaborative management of shared online contents and users information. Information related to user data such as user identification, friend lists of online social user, user groups in the social network, and user contents are stored in the application database. When access requests are made to the decision-making portion in the application server, results are returned in the form of access to photos or proper information about access to photos.

In addition, when privacy changes are made, the decision making portion returns change-impact information to the interface to alert the user. Moreover, analysis services in Socialcontroller application are provided by implementing an ASP translator, which communicates with an ASP reasoner.

Users can analysis services to perform complicated authorization requests. The main component of Socialcontroller is the decision-making module, which takes the access requests and returns responses in the form of either permit or deny for the requests. To calculate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the controller.

Then, the decisions of all controllers are aggregated to yield a final decision as the response of the request. Multiparty privacy conflicts are resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for decision making.

Privacy setup on social networking sites

Social network sites work to strengthen privacy settings. Facebook, orkut, linked-in, twitter are limit privacy as part of their default settings. It's important for

users to go into their user settings to edit their privacy options.

These sites like Facebook, orkut, linked-in, twitter give online users the option to not display personal information such as home address, birth date, email, phone number, and employment status. For those who choose to include this material, Facebook allow users to restrict access to their profile to only allow those who they accept as "friends" to view their profile. But even this level of security cannot prevent one of those friends from saving a photo to their own computer and posting it elsewhere. However, still fewer social networking site users have limited their profiles.

For those who choose to include this contents, Facebook, linked-in, twitter allow users to restrict access to their profile to only allow those who they accept as "friends" to view their profile information and contents. But even this level of security cannot prevent one of those friends from saving a photo to their own computer and posting it elsewhere. However, still fewer social networking site users have limited their profiles.

It is vital that all social networking sites users restrict Access to their profiles, not post information of illegal or policy-violating actions to their profiles, and be cautious with
The information they make available.

Comparison between two existing OSN

	Facebook	Linked-in
Cryptosystem	Proxy encryption	PKC/ABE
Autonomy	Facebook managed by system manager; Proxy Encryption by application proxy	Linked-in managed by system manager; ABE managed by group creator
Independence	Yes	Yes
Collaboration	No	No
Anonymous authentication	No	No
Revocation	No	No
Integrity checking	Yes	Yes
Relationship transitive	No	No
Post message encryption	Yes	Yes

Security

Social network providers are the security issue of user's data. Users share personal data on social networks without being fully aware of the consequences. An individual's context in the social network can be used to extract sensitive information. Using the context to extract information can be achieved through social phishing. From the security perspective, a social network can be treated as a graph and it is manipulated in some ways to hide the information. Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.

Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.

Your online reputation can be a good thing: Recent research also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.

Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.

Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.

Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

Keep a clean machine: Having the latest security software, web browser, and operating system are the best defences against viruses, malware, and other online threats.

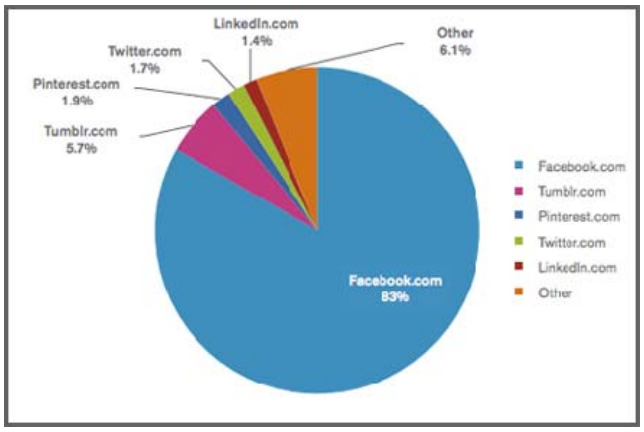
Own your online presence: When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how you share information.

Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.

Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.

When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Time Spent on Social Networking Site



Share of time spent

CONCLUSION

The importance of online social networks sites to human social development cannot be over emphasized, this is because online social networks sites allowed people to interact to each other freely, conduct businesses and above all serve as a medium of scholarly information seeking and dissemination as well, despite the issues of privacy and security conscious.

REFERENCES

[1] Pitkänen.O.Tuunainen, V.K, Hovi.M. 2009, Users' Awareness of Privacy on Online Social Networking sites – Case Facebook,https://domino.fov.unimb.si/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf

[2] Zhang.Ch, Sun. J,Zhu. X, Fang.Y. 2010 Privacy and Security for Online Social Networks: Challenges and Opportunities. Univ. of Florida, Gainesville, FL, Chi USA

[3] Dwyer .C., Hiltz R., and Passerini K. 2007 "Trust and Privacy concern within social networking sites: A comparison of Facebook and MySpace", in the Proceedings of AM. Conference on IS .

[4] Goettke R. and Christiana J. Nov, 2007, "Privacy and Online Social Networking Websites".

[5] Govani, T., and Pashley, H. Nov 2007," Student Awareness of the Privacy Implications while Using Facebook" Unpublished manuscript retrieved .

[6] Gross, R.and Acquisti. 2005"Information Revelation and Privacy in Online Social Networks (The Facebook case)", in the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

[7] Quan-Haase, A. (2007). University students' local and distant social ties: Using and integrating modes of communication on campus. Information, Communication & Society.

[8] Exacttarget(n.d.) 58% of Consumers Begin the Day With Email http://pages.exacttarget.com/etlpgen?v=153

[9] J. Domingo-Ferrer, "A public-key protocol for social networks with private relationships," in MDAI, ser. Lecture Notes in Computer Science, V. Torra, Y. Narukawa, and Y. Yoshida, Eds., vol. 4617. Springer,2007, pp. 373–379.

[10] J. Domingo-Ferrer, A. Viejo, F. Seb´e, and ´U. Gonz´alez-Nicol´as, "Privacy homomorphisms for social networks with private relationships," Computer Networks, vol. 52, no. 15, pp. 3007–3016, 2008.

[11] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Preserving confidentiality of security policies in data outsourcing," in WPES, 2008, pp. 75–84.

[12] K. B. Frikken and P. Srinnivas, "Key allocation schemes for private social networks," in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 11–20.

[13] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks," in OTM Workshops(2), ser. Lecture Notes in Computer Science, R. Meersman, Z. Tari, and P. Herrero, Eds., vol. 4278. Springer, 2006, pp. 1734–1744.

[14] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attributebased encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[15] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Secur., vol. 13, no. 1, 2009.

[16] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, 2009.