International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.3, May-June. 2013 pp-1343-1345 ISSN: 2249-6645

An Access Control Model for Online Social Networks

Sasikala Marla, [1] P.V.R. Raj Varma[2]
[1]*M.Tech, Sri Sunflower College of Engineering & Technology, Lankapalli*
[2]*Asst.Professor, Dept.of CSE, Sri Sunflower College of Engineering & Technology, Lankapalli*

Abstract: *Over the last decade online social networking sites have increased in popularity. This popularity has brought many users together, increasing their ability to share information. While the general information sharing is desirable, some users might be concerned with the privacy implications of disclosing so much personal information online. Currently users have two main options- They can either refuse to enter the information they are uncomfortable disclosing, or they may limit access to the information via privacy controls provided by the social networking site. It is important to note, however, that in the second case the information is stored remotely, and thus the control of the data is lost to the user. This paper presents an access control model for online social networks.*

Keywords: *Access control, OSN, Privacy.*

I. INTRODUCTION

Since its creation, the Internet has spawned many information sharing networks, the most well known of which is the World Wide Web. Recently, a new class of information networks called "Online Social Networks (OSN)" has exploded in popularity and now rival the traditional Web in terms of usage [1]. Social networking sites such as MySpace, Facebook, Orkut, and LinkedIn are the examples of wildly popular networks used to find and organize contacts. Other social networks such as Flickr, YouTube, and Google Video, are used to share the multimedia content, and others such as LiveJournal and BlogSpot are used to share blogs.

Unlike the traditional Web, which is largely organized by content, the online social networks embody users as first-class entities. Users join a network, publish their own content, and then create links to other users in the network called "friends". This basic user-to-user link structure facilitates online interaction by providing a mechanism for organizing both the real-world and virtual contacts, for finding other users with similar interests, and for locating content and knowledge that has been contributed or endorsed by "friends". The extreme popularity and the rapid growth of these online social networks represents a unique opportunity to study, understand, and leverage their properties. Not only can an in-depth understanding of online social network structure and growth aid in designing and evaluating current systems, it can lead to better designs of the future online social network based systems and to a deeper understanding of the impact of online social networks on the Internet. OSNs also offer many useful properties that can be leveraged to enhance information systems, such as enhancements to controlling information propagation, new directions for information search and retrieval, and new ways of reasoning about trust.

Users increasingly share content, recommendations, opinions, and ratings using the online social networks. However, the growing number of users and the increasing variety and volume of shared information on these sites aggravates two fundamental problems in information sharing- privacy and relevance. Since users are often sharing personal information, privacy and access control is critical. In particular, almost all privacy mechanisms available to users today are based on access control- users can specify which other users are able to view the content or information they upload.

II. NEED OF ACCESS CONTROL IN OSNS

OSNs have attracted a large amount of users to regularly connect, interact and share information with each other for different purposes. Users share a tremendous amount of content with other users in OSNs using various services available. The explosive growth of the sensitive or private user data that are readily available in OSNs has raised an urgent expectation for effective access control that can protect these data from unauthorized users in OSNs. Access control in the OSNs is typically based on the relationships among users in the social graph. That is, granting access to an accessing user is subject to the existence of either direct or indirect relationship of certain types between the accessing user and the controlling users of the target. Many existing OSN systems enforce a rudimentary and limited relationship-based access control mechanism, offering users the ability to choose from a pre-defined policy vocabulary, such as "private", "publlic", "friend" or "friend of friend". Google+[2] and Facebook [3] recently introduced customized relationships, namely "circle" and "friend list", providing users richer options to differentiate distinctly privileged user groups.

In OSNs, users are provided to create profiles, add content onto their pages (e.g., photos, videos, blogs, status updates and tweets), and share these resource objects with other peers. OSNs offer their users various types of user interaction services, including chatting, private messaging, poking and social games. As OSN systems mature, various types of resources need to be protected, such as user sessions, relationships among users and resources, access control policies and the events of users. As shown in Figure 1, users can launch access requests against both resources (e.g., view a photo or create an access control policy) and users (e.g., invite another user to a game or poke another user).

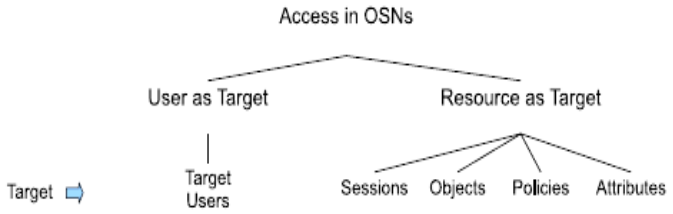

Figure 1: Taxonomy based on target

As shown in Figure 2, in OSN, a user can access other users (user as a target) or resources (resource as a target). By means of U2U(user to user), U2R(user to resource) and R2R(resource to resource) relationships, an accessing user and a target user can have a direct relationship or indirect relationships with user(s) in between, resource(s) in between or user(s) and resource(s) in between.

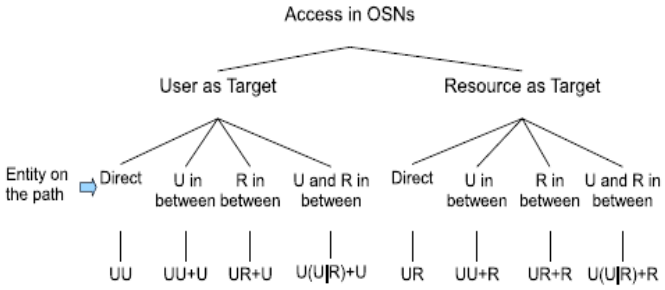

Figure 2: Access in OSNs

Likewise, an accessing user and the target resource can also be characterized in terms of the entities on the relating path. In the first two cases of accessing the target user, there is no resource involved. An accessing user should either have a particular direct U2U relationship (shown as UU) or a particular sequence of U2U relationships with the target user. Examples of such access to a target user are that Alice's direct friends can poke her, and Bob's friends of friends can request a friendship invitation to him. Similarly, a user may access a resource that directly relates to her (shown as UR), or may find a resource through one or more users in the network.

III. EXISTING WORK

Several access control models for OSNs have been introduced [4] [5]. Early access control solutions for OSNs introduced the trust-based access control inspired by the developments of trust and reputation computation in OSNs. The D-FOAF system [6] is primarily a Friend of a Friend (FOAF) ontology-based distributed identity management system for OSNs, where relationships are associated with a trust level, which indicates the level of friendship between the users participating in a given relationship. In [4], the authors introduced a conceptually-similar but more comprehensive trust-based access control model. This model allows the specification of access rules for the online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs.

In [7], the authors proposed an access control model that formalizes and generalizes the access control mechanism implemented in Facebook, admitting arbitrary policy vocabularies that are based on theoretical graph properties. In [12], the authors described relationship-based access control as one of new security paradigms that addresses unique requirements of Web 2.0. In [8], the authors proposed a semantic web based access control framework for social networks. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work [9]. Other related work includes general conflict resolution mechanisms for access control [10] and learn-based generation of privacy policies for OSNs [11].

IV. PROPOSED WORK

In our proposed work, we present an application called MController for supporting collaborative management of shared data. It enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. Consider the online social network "Facebook". Facebook server accepts inputs from the users, then forwards them to the application server. The application server is responsible for the input processing and collaborative management of the shared data. Information related to the user data such as user identifiers, friend lists, user groups, and user contents are stored in the MySQL database. Once the user installs MController in her/his Facebook space, MController can access user's basic information and contents. In particular, MController can retrieve and list all the photos, which are owned or uploaded by the user, or where the user was tagged. Then, the user can select any photo to specify the privacy preference. If the user is not the owner of the selected photo, he can only edit the privacy setting and sensitivity setting of the photo. Otherwise, if the user is an owner of the photo, then he can further configure the conflict resolution mechanism for the shared photo.

The core component of MController is the decision making module, which processes access requests and returns responses (either permit or deny) for the requests. Figure 3 depicts a system architecture of the decision making module in MController. To evaluate an access request, the policies of each controller of the targeted content are enforced first to generate a decision for the Mcontroller. Then, the decisions of all of the controllers are aggregated to yield a final decision as the response of the request. During the procedure of decision making, policy conflicts are resolved when evaluating the controllers' policies by adopting a strategy chain pre-defined by the controllers.

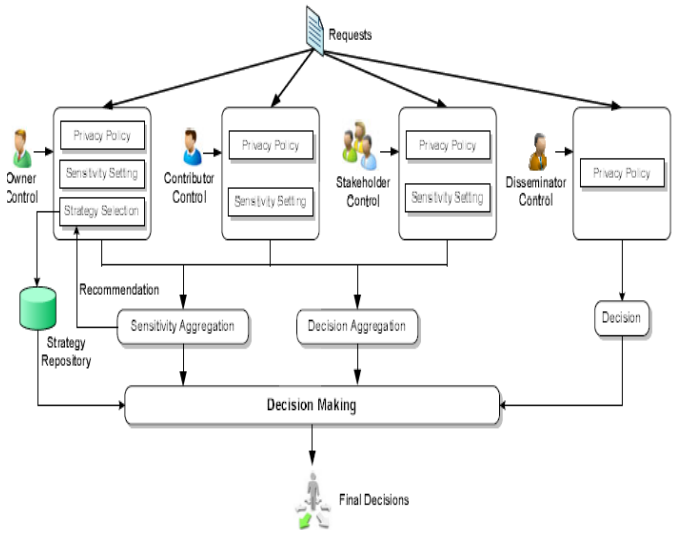

Figure 3: System Architecture of Decision Making in MController

In addition, multiparty privacy conflicts are also resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses the automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for making a decision. Otherwise, multiparty privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated sensitivity score is considered as the recommendation for the strategy selection. Regarding access requests to the disseminated contents, the final decision is made by combining the disseminator's decision and the original controllers' decision through a deny-overrides combination strategy.

V. CONCLUSION

The explosive growth of the sensitive or private user data that are readily available in OSNs has raised an urgent expectation for effective access control that can protect these data from unauthorized users in OSNs. For access control, we use an application called "Mcontroller". It enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. The core component of MController is the decision making module, which processes access requests and returns responses (either permit or deny) for the requests.

REFERENCES

[1] MySpace is the number one website in the U.S. according to Hitwise. Hit- Wise Press Release, July, 11, 2006. http://www.hitwise.com/press-center/ hitwiseHS2004/social-networking-june-2006.php.
[2] Google+ Privacy Policy. http://http://www.google.com/intl/en/+/ policy/.
[3] Facebook : http://www.facebook.com/.
[4] Carminati, B., Ferrari, E., Perego, A.: Rule-based access control for social networks. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM2006Workshops. LNCS, vol. 4278, pp. 1734– 1744. Springer, Heidelberg, 2006.
[5] Fong, P.: Relationship-Based Access Control: Protection Model and Policy Language. In: Proceedings of the First ACM Conference on Data and Application Security and Privacy. ACM, New York, 2011.
[6] Kruk, S., Grzonkowski, S., Gzella, A., Woroniecki, T., Choi, H.: D-FOAF: Distributed identity management with access rights delegation. In: Mizoguchi, R., Shi, Z.-Z., Giunchiglia, F. (eds.) ASWC 2006. LNCS, vol. 4185, pp. 140–154. Springer, Heidelberg, 2006.
[7] Fong, P., Anwar, M., Zhao, Z.: A privacy preservation model for facebook-style social network systems. In: Backes, M., Ning, P. (eds.) ESORICS 2009. LNCS, vol. 5789, pp. 303– 320. Springer, Heidelberg, 2009.
[8] Brands, S.A.: Rethinking public key infrastructures and digital certificates: building in privacy. The MIT Press, Cambridge, 2000.
[9] Squicciarini, A., Shehab, M., Paci, F.: Collective privacy management in social networks. In: Proceedings of the 18th International Conference on World Wide Web, pp. 521–530. ACM, New York ,2009.
[10] Fisler, K., Krishnamurthi, S., Meyerovich, L.A., Tschantz, M.C.: Verification and changei mpact analysis of access-control policies. In: ICSE 2005: Proceedings of the 27th International Conference on Software Engineering, pp. 196–205. ACM, New York, 2005.
[11] Fang, L., LeFevre, K.: Privacy wizards for social networking sites. In: Proceedings of the 19th International Conference on World Wide Web, pp. 351–360. ACM, New York ,2010.
12] Carrie, E.: Access Control Requirements forWeb 2.0 Security and Privacy. In: Proc. ofWorkshop on Web 2.0 Security & Privacy (W2SP), Citeseer, 2007.