MULTIPARTY ACCESS CONTROL (MPAC) POLICY FOR ONLINE SOCIAL NETWORKS (OSNS)

[1]SHASHANK RATHOD, [2]VINAYAK MUSALE

[1]M.E. [I.T.] Information Technology Department, Maharashtra Institute of Technology, Pune, India
[2]Assistant professor, Information Technology Department, Maharashtra Institute of Technology, Pune, India
E-mail: shashankrathod1@gmail.com, vinayak.musale@gmail.com

Abstract- Online Social Networks (OSNs) have tremendous growth in recent years and this can be existed in hundreds of millions of internet users. This paper offers different policy for sharing data and information, but also raises number of security and privacy issue. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. We begin by examining how the control lacks for shared data in OSNs based on the relationship between the user, data and their sharing patterns. Based on the sharing patterns, we formulate a Multiparty Access Control (MPAC) model to capture the core features of multiparty authorization requirements. Our model also contains a multiparty policy specification scheme. The future scope is to find conflicts and resolve the policies.

Index Terms- Online Social Networks (OSNs), Access Control Model, Multiparty Access Control (MPAC), Multiparty Policy Specification Scheme, Multiparty Authorization Requirements.

I. INTRODUCTION

Online Social Networks (OSNs) like Facebook, Google+ and Twitter are designed to make people to share his/her personal and public information and make people are socially connected with their Friends ,Family ,Colleagues and with Stranger. Today worlds, we have seen unprecedented growth of OSNs application. One of the typical social network sites is Facebook. In Facebook users can allow groups, friends, and friends of friends (FOF) or public to right to use their data, depending on their personal authorization and privacy requirements.

Although OSNs provide access control model, that allowing users to govern access to information contained in their own spaces. Users have no power to residing data outside their own spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. Online Social Networks (OSNs) provide access control model, that allowing users to access information in their own spaces. Users have no power to residing data outside their own spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. Also user uploads photo with his/her friend who are present in that photo are tagged. Tagged friends cannot have control to, who can see this photo, even though tagged friend have different policy of their profile. For such issue, OSNs offered a preliminary protection to existing systems.

Here, we start with examining, how multiparty access control (MPAC) for data sharing in OSNs has ability to protect the user data. With this we are identified typical data sharing pattern with respect to multiparty authorization in OSNs. On this pattern we are formulated Multipart Access Control (MAPC) model to capture some features requirements, that have not been provides by models of OSNs and existing systems. In MPAC model, correctness of access control model is based on that if access control model is valid. MPAC model also have multiparty policy specification scheme. This scheme is based on proposed MPAC model. MPAC police has to be place over shared data and representing authorized requirements from multiple users.

Pattern Sharing in Online Social Networks:
Users in OSNs can post statuses and notes, upload photos and videos in their own spaces, tag others to their content, and share the content with their friends. On the other hand, users can also post content in their friends' spaces. The shared content may be connected with multiple users.

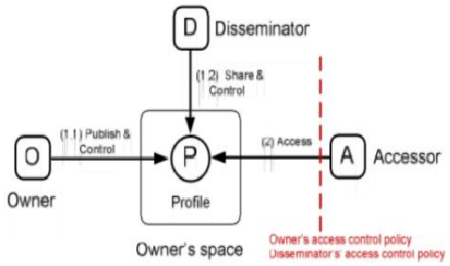


Figure 1: Pattern Sharing in OSNs

Consider an example it contains three users, Alice, Bob and Carol. If Alice uploads it to her own space and tags both Bob and Carol in the photo, we called Alice as owner of the photo, and Bob and Carol as stakeholders of the photo. All of them may be desired to specify privacy policies to control over that can see this photo. In another case, when Alice posts a note stating "I will attend a party on Sunday night with @Carol" to Bob's space, we call Alice the contributor

of the note and she may want to make the control over her notes. In addition, since Carol is explicitly identified by @-mention (at- mention) in this note, she is considered as a stakeholder of the note and may also want to control the exposure of this note. Since each associated user may have different privacy concerns over the shared content, privacy conflicts can occur among the multiple users.

The rest of the paper is organized as follows: In Section 2 provides overview of related work. Section 3 provides MPAC policies for OSNs in these defining different types of policy. Section 4 concludes this paper.

II. RELATED WORK

There are different types of sharing patterns occurring during OSNs where MPAC has different authorization requirements.

Profile sharing: An appealing feature of some OSNs is to support social applications written by third-party developers to create additional functionalities built on the top of users profile for OSNs. To provide meaningful and attractive services consider figure 1, these social applications consume user profile attributes, such as name, birthday, activities, interests, and so on. To make matters more complicated, social applications on current OSN platforms can also consume the profile attributes of a user's friends [1, 2]. In this case, users can select particular pieces of profile attributes they are willing to share with the applications when their friends use the applications.

Relationship sharing: Another feature of OSNs is that users can share their relationships with other members [1, 2]. Relationships are inherently bidirectional and carry potentially sensitive information that associated users may not want to disclose. Most OSNs provide mechanisms that users can regulate the display of their friend lists. A user, however, can only control one direction of a relationship.

Content sharing: OSNs provide built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and videos in their own spaces, tag others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friends' spaces. The shared contents may be connected with multiple users.

Profile Access: Once the search listing of a profile owner is reached; the accessing user may elect to access the profile, thereby initiating Stage II of authorization. Whether the profile as a whole can be accessed is dictated by another user species policy, the details of which we omit [1]. Not every accessing user sees the same profile items when a profile is displayed. The owner may assign an access policy to each profile item, dictating who can see that profile item when the profile is accessed.

Policies: We have seen in the above discussion that various aspects of user activities are controlled by user species policies (e.g., search policy, access policy, etc). This is typical of a discretionary access control systems [1], in which a user may grant access privileges to other users. Facebook offers a fixed vocabulary of predefined policies for users to choose from when they are to identify sets of privileged users. As in many capability systems, there is no global name space of users that can be used for the purpose of identifying user sets. Therefore, many of the predefined policies identify user sets indirectly in terms of the topology of the social graph. For example, one may specify that a certain profile item is accessible only by "friends", or that messaging is only available to "friends of friends. We also defines Facebook has groups and networks of users so that policies can be formulated in terms of these concepts. We deem user grouping a well-understood concept, and thus focus only on topology based policies in the sequel.

III. MPAC POLICY FOR OSNS

Online Social Networks (OSNs) provide application for the collaborative management of shared data, is called as MController. This application enables multiple users to specify their authorization policies and privacy preference to co-control a shared data items. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism.

OSNs should allow multiple controllers, who are associated with shared data and to specify access control policies. The sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to control the access of the shared data as well.

Privacy Policy Specification:
To enable a collaborative management of data sharing in OSNs, it is essential for privacy policies to be in place to regulate access over shared data, representing privacy requirements from multiple associated users. Recently, several access control schemes have been proposed to support fine-grained privacy specifications for OSNs. Unfortunately, these schemes can only allow a single user to specify her/his privacy concern. Indeed, a flexible privacy control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are

associated with the shared data, to specify privacy policies.

Controller Specification:
As in the privacy conflict scenarios, in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, also need to regulate the access of the shared data. We define these controllers as follows:

1. Owner :
Let d be the Data item of owner module in the space m of user u in the social network. User u is called the owner of d. This module analyze the three features like profile sharing, relationship sharing and content sharing for understanding of collaborative control in OSNs.

2. Contributor :
Let d be the data item of contributor module is placed by user u in the other space in social network. User u is called the contributor of d.

3. Stakeholder :
Let d be the Data item of stakeholder module in the space m of user u in the social network. Let tagged users T can associate with d. Then user u is called the stakeholder of d if u?T.

4. Disseminator :
Let d be the data item is placed by the user u from others space to his/her space in the social network. User u is called the disseminator of d.

Accessor Specification:
Accessors are a set of users to whom the authorization is granted. Accessors can be represented with a set of user names, the friendship or a set of group names in OSNs. To facilitate collaborative privacy management, we further introduce trust levels, which are assigned to accessors when defining the privacy policies. Focus on OSNs for collaborative rating. We believe that such considerations can also apply to our privacy management. Trust is one of the factors in our approach for resolving privacy conflicts. The notation of trust in our work mainly conveys information about how much confidence a controller put on her/his friends who would not disclose the sensitive information to untrusted users. Also, trust levels can be changed in different situations.

Data Specification:
In the context of OSNs, user data is composed of three types of information. User profile describes who a user is in the OSN, including identity and personal information, such as name, birthday, interests and contact information. User friendship shows who a user knows in the OSN, including a list of friends to represent connections with family, co-workers, colleagues, and so on. User content indicates what a user has in the OSN, including photos, videos, statues, and all other data objects created through various activities in the OSN.

Again, to facilitate effective resolution of privacy conflicts for collaborative privacy control, we introduce sensitivity levels for data specification, which are assigned by the controllers to the shared data. The users' judgment of the sensitivity levels of the data is not binary (private/public), but multi-dimensional with varying degrees of sensitivity. Formally, the data specification is defined as follows:

5. Data Specification
Let d ∈ D be a data item, and sl be a sensitivity level, which is a rational number in the range [0, 1], assigned to d. The data specification is defined as a tuple < d; sl >.

Privacy Policy:
To summarize the aforementioned features and elements, we introduce a formal definition of privacy policies for collaborative data sharing as follows:

6. Privacy Policy
A privacy policy is a 4-tuple P =< controller; accessor; data; effect >.

CONCLUSION

In this paper we defining the different types of policy used in OSNs. Using MPAC, OSNs has different controllers which shared data to find access control policies. An MPAC policy was formulated, along with a multiparty policy specification scheme and policy evolution mechanism. As part of future work, is to find conflicts and resolve the policies. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent works has evaluated the effectiveness of the MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss.

REFERENCES

[1] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems," Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 2009.

[2] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[3] B. Carminati and E. Ferrari, "Collaborative Access Control in On- Line Social Networks," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Work sharing (Collaborate- Com), pp. 231-240, 2011.

★★★