IJDCST @ Dec, Issue- V-3, I-1, SW-34
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

A Mechanism to Control Multiparty Access for Online Social Networks

Mohamad Farzana Begum[1], Khamar Zahan[2]

[1]M.Tech (CSE), Nimra College of Engineering and Technology, A.P., India.

[2] Assistant Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering and Technology, A.P., India.

Abstract — Online social networks (OSNs) have witnessed the exponential growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We originate an access control paradigm to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model that allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

Keywords — Social network, multiparty access control, security model, policy specification and management

I. INTRODUCTION

The objective of the Online social networks (OSNs) such as Facebook, Google+, and Twitter are to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family, and even with strangers. In recent years, we have seen tremendous growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, and so on.) shared each month [2]. To protect user data, access control has become a central feature of OSNs [1].

In a typical OSN, each user is provided with a virtual space containing profile information, a list of the user's friends, and webpages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education, and work history, and contact information. In addition, 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. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to access their data, depending on their personal authorization and privacy requirements.

Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, she/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's

profile by means of the association link, but the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN managers is either too loose or too restrictive, relying on the OSN's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively.

In this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, an MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for OSNs (e.g., [3], [4], [5], [6], [7]). Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model.

Another compelling feature of our solution is the support of analysis on the MPAC model and systems. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Moreover, while the use of an MPAC mechanism can greatly enhance the flexibility for regulating data sharing in OSNs, it may potentially reduce the certainty of system authorization consequences due to the reason that authorization and privacy conflicts need to be resolved elegantly. Assessing the implications of access control mechanisms traditionally relies on the security analysis technique, which has been applied in several domains (e.g., operating systems [8], trust management, and role-based access control). In our approach, we additionally introduce a method to represent and reason about our model in a logic program. In addition, we provide a prototype implementation of our authorization mechanism in the context of Facebook. Our experimental results demonstrate the feasibility and usability of our approach.

II. Related Work

Access control for OSNs is still considered as a relatively new research area. Several access control models for OSNs have been introduced (e.g., [3], [4], [5], [6], [7]). Early access control solutions for OSNs introduced trust-based access control inspired by the developments of trust and reputation computation in OSNs.

In Paper [7], The D-FOAF system is primarily a friend of a friend 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 [3], Carminati et al. introduced a conceptually similar but more comprehensive trust-based access control model. This model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. They further presented a semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in OSNs.

Fong et al. [6] 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. Gates [5] described relationship-based access control (ReBAC) as one of new security paradigms that addresses unique requirements of Web 2.0. Then, Fong [5] recently formulated this paradigm called a ReBAC model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of this existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs.

The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work [9]. Squicciarini et al. [10] provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content. The Clarke-Tax mechanism

was adopted to enable the collective enforcement of policies for shared contents. Game theory was applied to evaluate the scheme. However, a general drawback of their solution is the usability issue, as it could be very hard for ordinary OSN users to comprehend the Clarke-Tax mechanism and specify appropriate bid values for auctions. Also, the auction process adopted in their approach indicates that only the winning bids could determine who can access the data, instead of accommodating all stakeholders' privacy preferences. Carminati et al. [10] recently introduced a new class of security policies, called collaborative security policies that basically enhance topology-based access control with respect to a set of collaborative users. In contrast, our work proposes a formal model to address the MPAC issue in OSNs, along with a general policy specification scheme and a simple but flexible conflict resolution mechanism for collaborative management of shared data in OSNs. In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used in OSNs, which has not been addressed by prior work.

III. Proposed Work

A. *Prototype Implementation*

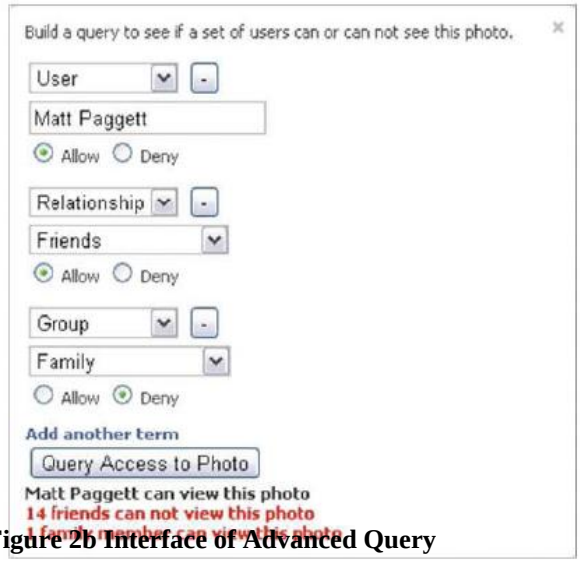
We implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController (http://apps.facebook.com/MController). Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to cocontrol a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs. Obversely, our approach can be generalized to deal with other kinds of data sharing, such as videos and comments, in OSNs as long as the stakeholder of shared data is identified with effective methods like tagging or searching.

Fig. 1 shows the architecture of MController, which is divided into two major pieces: Facebook server and application server. The Facebook server provides an entry point via the Facebook application page, and provides references to photos, friendships, and feed data through API calls. Facebook server accepts inputs from users, then forward them to the application server. The application server is responsible for the input processing and collaborative management of shared data. Information related to user data such as user identifiers, friend lists, user groups, and user contents are stored in the application database. Users can access the **MController** application through Facebook, which serves the application in an iFrame. 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 decisionmaking portion returns change-impact information to the interface to alert the user. Moreover, analysis services in **MController** application are provided by implementing an ASP translator, which communicates with an ASP reasoner. Users can leverage the analysis services to perform complicated authorization queries.

Figure 1 Overall architecture of MController application

MController is developed as a third-party Facebook application, which is hosted in an Apache Tomcat application server supporting PHP and MySQL database. MController application is based on the iFrame external application approach. Using the Javascript and PHP SDK, it accesses users' Facebook data through the graph API and Facebook query language. Once a user installs MController in her/his Facebook space and accepts the necessary permissions,

Figure 2a Main interface



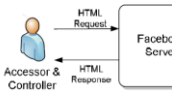


Figure 2b Interface of Advanced Query

MController can access a user's basic information and contents. Especially, MController can retrieve and list all photos, which are owned or uploaded by the user, or where the user was tagged. Once information is imported, the user accesses MController through its application page on Facebook, where she/he can query access information, set privacy for photos that she/he is a controller, or view photos she/he is allowed to access.

A snapshot of main interface of MController is shown in Fig. 2a. All photos are loaded into a gallery-style interface. To control photo sharing, the user clicks the "Owned," "Tagged," "Contributed," or "Disseminated" tabs, then selects any photo to define her/his privacy preference by clicking the lock below the gallery. If the user is not the owner of selected photo, she/he can only edit the privacy setting and sensitivity setting of the photo. Otherwise, if the user is the owner of the photo, she/ he has the option of clicking "Show Advanced Controls" to assign weight values to different types of controllers and configure the conflict resolution mechanism for the shared photo. By default, the conflict resolution is set to automatic. However, if the owner chooses to set a manual conflict resolution, she/he is informed of an Sc of shared photo and receives a recommendation for choosing an appropriate conflict resolution strategy. Once a controller saves her/his privacy setting, a corresponding feedback is provided to indicate the potential authorization impact of her/his choice. The controller can immediately determine how many users can see the photo and should be denied, and how many users cannot see the photo and should be allowed. MController can also display the details of all users who violate against the controller's privacy setting. The purpose of such feedback information is to guide the controller to evaluate the impact of collaborative authorization. If the controller is not satisfied with the current privacy control, she/he may adjust her/his privacy setting, contact the owner of the photo to ask her/him to change the conflict resolution strategies, or even report a privacy violation to OSN administrators who can delete the photo. A controller can also perform authorization analysis by advanced queries as shown in Fig. 2b. Both oversharing and undersharing can be examined by using such an analysis service in MController.

B. Participants and Procedure

MController is a functional proof-of-concept implementation of collaborative privacy management. To measure the practicality and usability of our mechanism, we conducted a survey study (n = 35) to explore the factors surrounding users' desires for privacy and discover how we might improve those implemented in MController. Specifically, we were interested in users' perspectives on the current Facebook privacy system and their desires for more control over photos they do not own. We recruited participants through university mailing lists and through Facebook itself using Facebook's built-in sharing API. Users were given the opportunity to share our application and play with their friends. While this is not a random sampling, recruiting using the natural dissemination features of Facebook arguably gives an accurate profile of the ecosystem.

Participants were first asked to answer some questions about their usage and perception of Facebook's privacy controls, then were invited to watch a video (http://bit.ly/ MController) describing the concept behind MController. Users were then instructed to install the application using their Facebook profiles and complete the following actions: Set privacy settings for a photo they do not own but are tagged in, set privacy settings for a photo they own, set privacy settings for a photo they contributed, and set privacy settings for a photo they disseminated. As users completed these actions, they answered questions on the usability of the controls in MController. Afterward, they were asked to answer further questions and compare their experience with MController to that in Facebook.

C. Performance Evaluation

To evaluate the performance of the policy evaluation mechanism in MController, we changed the number of the controllers of a shared photo from 1 to 20, and assigned each controller with the average number of friends, 130, which is claimed by Facebook statistics [3]. Also, we considered two cases for our evaluation. In the first case, each controller allows "friends" to access the shared photo. In the second case, controllers specify "FOF" as the accessors instead of "friends." In our experiments, we performed 1,000 independent trials and measured the performance of each trial. Since the system performance depends on other processes running at the time of measurement, we had initial discrepancies in our performance. To minimize such an impact, we performed 10 independent trials (a total of 10,000

calculations for each number of controllers). For both cases, the experimental results showed that the policy evaluation time increases linearly with the increase of the number of controllers. With the simplest implementation of our mechanism, where n is the number of controllers of a shared photo, a series of operations essentially takes place n times. There are O(n) MySQL calls and data fetching operations and O(1) for additional operations. Moreover, we could observe there was no significant overhead when we run MController in Facebook.

IV. Conclusion

In our paper, we have proposed a novel solution for collaborative management of shared data in OSNs. An MPAC model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method.

As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs. 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. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time-consuming and tedious tasks. Therefore, we would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

References

[1]. Facebook Privacy Policy, http://www.facebook.com/policy. php/, 2013.

[2]. Facebook Statistics, http://www.facebook.com/press/info.php?statistics, 2013.

[3]. B. Carminati, E. Ferrari, and A. Perego, “Rule-Based Access Control for Social Networks,” Proc. Int’l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

[4] B. Carminati, E. Ferrari, and A. Perego, “Enforcing Access Control in Web-Based Social Networks,” ACM Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[5] 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.

[6] 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.

[7] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi, “D-FOAF: Distributed Identity Management with Access Rights Delegation,” Proc. Asian Semantic Web Conf. (ASWC), pp. 140-154, 2006.

[8] M. Harrison, W. Ruzzo, and J. Ullman, “Protection in Operating Systems,” Comm. ACM, vol. 19, no. 8, pp. 461-471, 1976.

[9] A. Besmer and H.R. Lipford, “Moving beyond Untagging: Photo Privacy in a Tagged World,” Proc. 28th Int’l Conf. Human Factors in Computing Systems, pp. 1563-1572, 2010.

[10] B. Carminati and E. Ferrari, “Collaborative Access Control in On- Line Social Networks,” Proc. Seventh Int’l Conf. Collaborative Computing: Networking, Applications and Worksharing (Collaborate- Com), pp. 231-240, 2011.