Reciprocal Access Direct for Online Social Networks: Model and Mechanisms

RAVULA VENKATESH
M. Tech scholar,
Department of CSE
Vijay Rural Engineering College, Jntuh
Email-id: Venky.5b8@Gmail.Com

N.SWAPNA
Associate Professor,
Vijay Rural Engineering College, Jntuh
email-id: swapnanaralas@gmail.com

Abstract:
There is knowledgeable marvelous growth in fresh years by online social networks and become a effectively doorway for hundreds of millions of Internet users. These online social networks offer eye-catching means for digital social exchanges and information distribution, but also move up a number of privacy and security issues. While online social networks allow users to control access to shared data, they presently do not provide any mechanism to enforce privacy concerns over data associated with many users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in online social networks. We prepare an access control model to take into custody the essence of multiparty authorization requirements, along with a policy enforcement mechanism and a multiparty policy specification system.

Via this paper we are going to study about model and mechanism systems in analysis of multiparty access control. The correctness of realization of an access control model is based on the premise that the access control model is valid...We pursue an efficient solution to facilitate collaborative management of common data in OSNs. We begin by investigate how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Some distinctive data sharing patterns with respect to multiparty authorization in OSNs are also identified. We make official a Multiparty Access Control (MPAC) model for OSNs.

Keywords: *Multiparty access control, Policy specification and management security model, Social network*

1. Introduction

(OSNs) ONLINE social networks such as Face book, Google+, and Twitter are essentially designed 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 unprecedented growth in the application of OSNs. For example, Face book, 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, etc.) shared each month [3]. To protect user data, access control has become a central feature of OSNs [2], [4]. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, 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 entrusted users. For example, in Face book, users can allow *friends*, *friends of friends*, *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, s/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, Face book allows tagged users to remove the tags linked to their profiles or report violations asking Face book 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 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, a multiparty access control (MPAC) model is formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for OSNs (e.g., [10], [11], [17], [18], [23]). 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 multiparty access control 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 multiparty access control 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 [20], trust management [25], and role-based access control [26]). 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 Face book. Our experimental results demonstrate the feasibility and usability of our approach.

The rest of the paper is organized as follows. In Section 2, we present multiparty authorization requirements and access control patterns for OSNs. We articulate our proposed MPAC model, including multiparty authorization specification and multiparty policy evaluation in Section 3. Section 4 addresses the logical representation and analysis of multiparty access control. The details about prototype implementation and experimental results are described in Section 5. Section 6 discusses how to tackle collusion attacks followed by the related work in Section 7. Section 8 concludes this paper and discusses our future directions.

2. Web Access Control Policies

2.1 Representing and Reasoning

We propose a systematic method to represent XACML policies in answer set programming (ASP), a declarative programming paradigm oriented towards combinatorial search problems and knowledge intensive applications. Compared to a few existing approaches to formalizing XACML policies. our formal representation is more straightforward and can cover more XACML features. Furthermore, translating XACML to ASP allows us to leverage off-the-shelf ASP solvers for a variety of analysis services such as policy verification, comparison and querying. In addition, in order to support *reasoning* about role-based authorization constraints, we introduce a general specification scheme for RBAC constraints along with a policy analysis framework, which facilitates the analysis of constraint violations in XACML-based RBAC policies. The expressivity of ASP, such as ability to handle default reasoning and represent transitive closure, helps manage XACML and RBAC constraints that cannot be handled in other logic -based approaches. We also overview our tool XACML2ASP and conduct experiments with real-world XACML policies to evaluate the effectiveness and efficient of our solution

2.2. Requirements for Web 2.0 Security and Privacy

The increased social networking capabilities provided by Web 2.0 technologies requires a examination of what we consider "private" and what we consider "personal" information, and will consequently drive a new way of limiting and monitoring the information that we make public online. Web 2.0 applications are creating large, composite conglomerations of personal data and so we need new approaches to describe and execute access organize on that data. "Private" information at present tends to be insecurely defined by legislation, rather than by what individuals consider to be personal. Generic information such as a person's home address and phone number are normally considered personally identical information (PII) and are to be protected when collected and stored by an organization in addition, the use and release of exact data, such as medical or financial information, is restricted legislatively. However, It also exists information that an individual may consider to be personal, and want to let loose only to people meeting particular criteria (such as people attending the same school) or particular people (such as close friends). Thus someone might want to control portions of their digital life in the same manner that they control what information is released in their analog life. In the world, a person can choose to tell someone or some group some piece of information about themselves. On the other hand, it is often the case that in the online world these controls do not exist, most important to de facto public disclosure.

3. Online Social Networks

3.1 Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks

We propose a novel collaborative face recognition frame work, improving the accuracy of face annotation by effectively making use of multiple face recognition engines available in online social networks. Our collaborative face recognition framework consists of two major parts: merging (or fusion) and selection of face recognition engines of multiple face recognition results. The selection of face recognition engines aims at determining a set of modified face recognition engines that are suitable for recognizing query face images belonging to a particular member of the Online social networks. For this purpose, we use both social network context in an online social networks and social context in personal photograph collections. In addition, to take advantage of the availability of multiple face recognition results retrieved from the selected face recognition engines, we devise two effective solutions for merging face recognition results, adopting traditional techniques for combining multiple classifier outputs. Experiments were conducted using 547 991 personal photographs collected from an existing Online social networks. Our results demonstrate that the proposed collaborative face recognition method is able to significantly improve the accuracy of face annotation, compared to conventional face recognition approaches that only make use of a single face recognition engine. Further, we demonstrate that our collaborative face recognition framework has a low computational cost and comes with a design that is suited for deployment in a decentralized online social network.

3.2 Protection model and policy language

Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. The Gates coined the term Relationship-Based Access Control (Re BAC) to refer to this paradigm. Relationship-Based Access Control is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of Relationship-Based Access Control to application domains other than social computing. We prepare an archetypical Relationship-Based Access Control model to capture the essence of the standard, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the security system. A novelty of the model is that it captures the contextual nature of associations. We work out a policy language, based on modal logic, for composing access control policies that support delegation of trust. We use a case study in the domain of Electronic Health Records to demonstrate the utility of our model and its policy language. This provides initial evidence to the feasibility and utility of Relationship-Based Access Control as a general-purpose paradigm of access control.

3.3 Multiparty Authorization Framework for Data Sharing and an Active Detection of Identity Clone Attacks

We propose a multiparty authorization framework (MAF) to model and realize multiparty access control in online social networks. We begin by examining how the lack of multiparty access control for data sharing in online social networks can undermine the security of user data. A multiparty authorization model is then formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for online social networks. In Meanwhile, as conflicts are inevitable in multiparty authorization specification and enforcement, systematic conflict resolution mechanism is also addressed to cope with authorization and privacy conflicts in our framework. We first examine and characterize the behaviors of ICAs. Then we propose a detection framework that is focused on discovering suspicious identities and then validating them. Towards detecting suspicious identities, we propose two approaches based on attribute similarity and similarity of friend networks. The first approach addresses a simpler scenario where mutual friends in friend networks are considered; and the second one captures the scenario where similar friend identities are concerned. We also current experimental results to demonstrate flexibility and effectiveness of the proposed approaches. Finally, Some feasible solutions to validate suspicious identities.

4. Reciprocal Access Control Model For Owns

In this section, we formalize a Multi Party Access Control (MPAC) model for OSNs (Section 3.1), as well as a policy scheme (Section 3.2) and a policy evaluation mechanism (Section 3.3) for the specification and enforcement of MPAC policies in OSNs .

4.1 MPAC Model

OSN can be represented by a relationship network. OSNs provide each member a Web space where users can store and manage their personal data including profile information, friend list and content. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. We identified previously in the sharing patterns, in addition to the other controllers, owner of data including the stakeholder, contributor and disseminator of data, need to regulate the access of the shared data as well**.** We define these controllers as follows:

Definition 1: (Owner). Let **d** be a data item in the space of a user **u** in the social network. The user **u** is called the owner of **d**.

Definition 2: (Contributor). Let **d** be a data item published by a user **u** in someone else's space in the social network. The user **u** is called the contributor of **d.**

Definition 3: (Stakeholder). Let **d** be a data item in the space of a user in the social network. Let **T** be the set of tagged users associated with **d**. A user **u** is called a stakeholder of **d**, if **u** & **T**.

Definition 4: (Disseminator). Let **d** be a data item shared by a user **u** from someone else's space to his/her space in the social network. The user **u** is called a disseminator of **d.**

MPAC Policy
Specification: The
MPAC policies

(1) "Alice authorizes her friends to view her status identified by status 01 with a medium sensitivity level, where Alice is the owner of the status."

(2) "Bob authorizes users who are his colleagues or in hiking group to view a photo, summer.jpg, that he is tagged in with a high sensitivity level, where Bob is a stakeholder of the photo."

(3) "Carol disallows Dave and Edward to watch a video, play.avi, that she uploads to someone else's spaces with a highest sensitivity level, where Carol is the contributor of the video." are expressed as:

(1) p1 = (Alice,OW, {< friendOf,RN >},
< status01, 0.50 >, permit)
(2) p2 = (Bob, ST, {< colleageOf,RN >,
< hiking,GN >},< summer.jpg,
0.75 >, permit) (3) p3 =
(Carol,CB, {< Dave,UN >,

< Edward,UN >},< play.avi, 1.00 >, deny)

5. Methodologies

A methodology is the process of acquiring communication traces in large scale parallel application.

Modules Name: Authentication (login /Registration), Profile, Friends, Send request, Group, Photos

Authentication (submit/Reset)

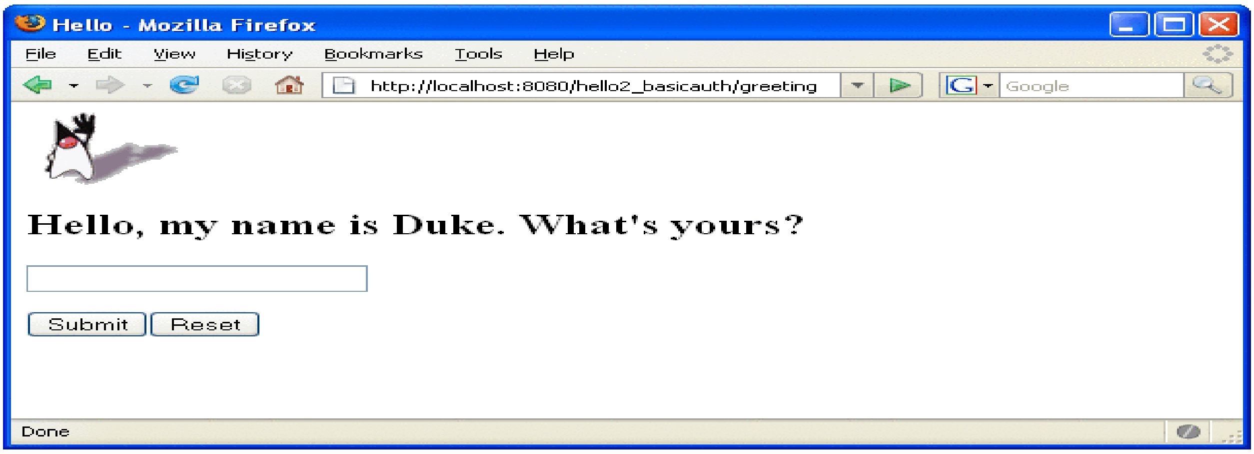


Fig. 1 Example of an Authentication

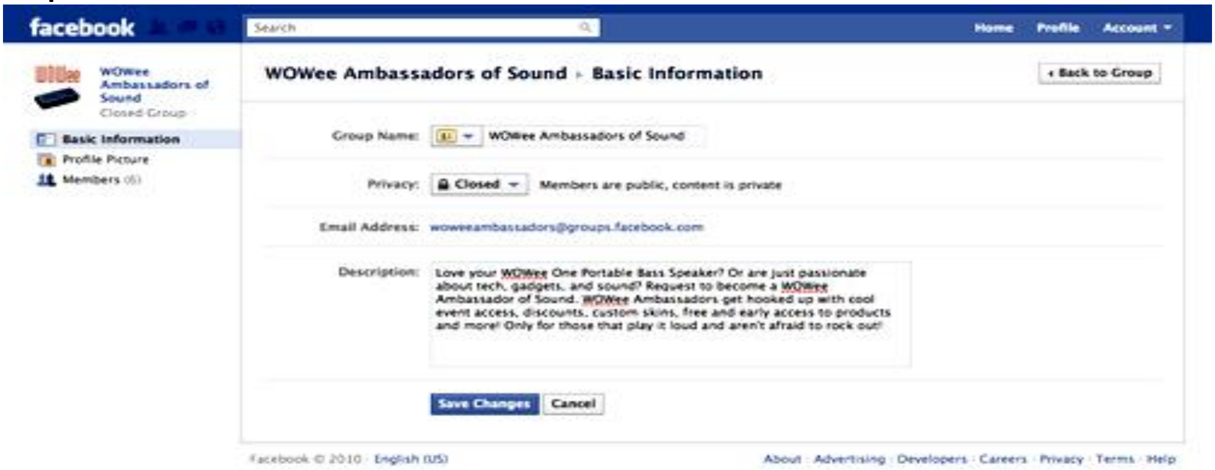
Home

Fig. 2 Example of Home

Profile

In this module user make our profile that details store in database the profile contains name, contact no, and email address, photos, and other information. Logged users can see their details and if they wish to change any of their information they can edit it.

Groups



Photos

In this module user add new photo and publish the content based on our selected members in that group. Who appear in the photo, the tagged friends can restrict who can see this photo if (user = = Allow) that User will be allowed to access the data's Else User will be not allowed to access the data's This module enables the user to upload the photos to their photo gallery and maintain their album.

6. Existing System

OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. In another case, while a user uploads tags and the photograph friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph, even though the tagged friends may have different privacy concerns about the photo. To address such a serious issue, beginning protection mechanisms have been offered by existing online social networks (OSNs).

- Access to a resource is granted while the requestor is able to demonstrate of being authorized.

- Every user in the group can access the shared content.
- Not give any mechanism to enforce privacy concerns over data associated with multiple users
- if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment
- while a user uploads a photo and tags friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph

7. Proposed System

Our solution is to support the analysis of multiparty access control model and mechanism systems. The correctness of execution of an access control model is based on the premise that the access control model is suitable. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in Online social networks (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. We specially analyze the scenario like content sharing to understand the risks posted by the lack of collaborative control in online social networks (OSNs).

- It checks the access request against the policy specified for every user and yields a decision for the access.
- The use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in online social networks.
- present any mechanism to enforce privacy concerns over data associated with many users
- if a user posts a comment in a friend's space, he/she can specify which users can view the comment

8. Conclusion

In our multiparty access control system for model and mechanism, a group of users could collude with one another so as to manipulate the final access control decision. An attack scenarios, anywhere a set of malicious users may want to make a shared photo available to a wider audience. Suppose they can access the photo, and then they all tag themselves or fake their identities to the photo. In addition, they collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo with a large number of colluding users; the photo may be disclosed to those users who are not expected to gain the access. To prevent such an attack scenario from occurring, three conditions need to be satisfied: (1) there is no fake identity in OSNs; (2) all tagged users are real users appeared in the photo; and (3) all controllers of the photo are honest to specify their privacy preferences.

References

1. Besmer, A. and Richter Lipford H. (2010). Moving beyond untagging: Photo privacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563– 1572. ACM.
2. Bilge, L. T. Strufe, D. Balzarotti., and Kirda, E. (2009). All your contacts are belonging to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World Wide Web, pages 551–560. ACM.
3. Face book Developers. http://developers.facebook.com/.
4. Face book Privacy Policy. http://www.facebook.com/policy.php/.
5. Face book Statistics. http://www.facebook.com/press/info.php? Statistics.
6. Google+ Privacy Policy. http://http://www.google.com/intl/en/+/ policy/.
7. Open Social Framework. http://code.google.com/p/ open social-resources/.