Enabling Cross-Site Content Sharing between Social Networks

Moonam Ko, Hakim Touati, Mohamed Shehab
Department of Software and Information Systems
College of Computing and Informatics
University of North Carolina, Charlotte
Charlotte, NC, USA
Email: {mnko, htouati, mshehab}@uncc.edu

Abstract—Social Networks is one of the major technological phenomena on the Web 2.0. Hundreds of millions of people are posting articles, photos, and videos on their profiles and interacting with other people, but the sharing and interaction are limited within a same social network site. Although users can share some contents in a social network site with people outside of the social network site using a public link of content, appropriate access control mechanisms are still not supported. To overcome those limitations, we propose a cross-site content sharing framework named x-mngr, allowing users to interact with others in other social network sites, with a cross-site access control policy, which enables users to specify policies that allow/deny access to their shared contents across social network sites. We implemented our proposed framework through a photo sharing application that shares user’s photos between Facebook and MySpace based on the cross-site access control policy. To evaluate our approach, we conducted a user study for the x-mngr framework.

Keywords-social networks; sharing; access control;

I. INTRODUCTION

Social Networks(SN) sites provide different sets of services. Facebook and MySpace provide services that help users to connect with people and share contents. On the other hand, LinkedIn provides services that help users exchange information and opportunities with a broader network of professionals. Depending on context (i.e. age, gender, location, and interest) and purpose, users create accounts on multiple SN services [3]. Thus, to be able to share content with friends that are in different SN sites, users have to upload duplicate content and set up their policies on each site since current SN architecture provides limited cross-site content sharing mechanisms. Moreover, scattered friends do not generally migrate to other SN sites from their favorite SN sites to access a shared content. Enabling cross-site content sharing beyond SN site boundaries is a challenging task in both the semantics and the policies of the involved sites.

In this paper, we propose a cross-site content sharing framework named x-mngr that manages content sharing and access control across SN sites. We present a cross-site policy which enables users to setup policies that allow/deny access to their shared contents across different SN sites with different policy levels. To enable secure cross-site sharing, we designed the x-mngr that supports the principles of secure interoperation. We also proposed three policy levels to provide different policy enforcement for shared content. We implemented a proof-of-concept application that allows users to share photos between both Facebook and MySpace. As part of our assessment, we also present our survey results and usability result of the x-mngr. Users responded favorably to the approach, indicating a general understanding of the x-mngr, and we found our proposed approach to be useful.

II. BACKGROUND

In order to understand the challenge of cross-site content sharing, we conducted a survey to understand user’s content sharing experience on SN sites and identify the necessity of cross-site content sharing. The survey investigated users’ SN experience, privacy setting, and content sharing experience.

We recruited 403 participants to start the survey, of which 306 participants completed the online survey and 97 participants did not complete the survey. We investigate the survey results of 306 participants who completed the survey. The highlight of results are presented below, more detailed survey results are available at [2].

Most participants have accounts on multiple SN sites. 87.6% of participants reported they have accounts on multiple SN sites. The participants also reported the reason of using multiple SN sites is to get different services or to meet the scattered friends on different SN sites. In the question about spending time on SN services, 41.7% of participants said they access their SN sites a few times a day and 40.9% of participants said they access the SN sites constantly. It shows most participants’ daily life is connected with their favorite SN sites.

Some participants organized friends using the Friend List to apply different privacy settings. 92% participants out of 268 participants who had accounts on multiple SN sites reported they used similar privacy setting between SN sites. Also, 34.0% participants out of 306 participants stated they organized their friends using the Friend List to apply different privacy settings. Their average number of Friend List is 4-6 Friend Lists. They agreed that the Friend Lists are helpful to protect privacy on SN sites. These results showed participants who were concerned about their privacy on SN sites organized their friends using the Friend List to apply different privacy settings.
We found SN services to be the most common route for SN with allowed manages the cross-site. 44.4% participants had the same experience. Given a SN site, the local policy $P$ of an object $O$ is defined using two access control lists, namely the allow list $ACL^+$ and the exception list $ACL^-$, which are sets of the allowed and the denied users or groups respectively. Access control follows the closed world assumption, where if access is not explicitly specified it is assumed to be not accessible. For an object $O$ given $ACL^+$ and $ACL^-$, a user $u$ is given access to $O$ with allowed operation $OP$ iff $u \in ACL^+$ and $u \notin ACL^-$, or in compact form $u \in (ACL^+ \setminus ACL^-)$. The full format of local policy is $(O, ACL^+, ACL^-, OP)$.

The role of $ACL^+$ is to enumerate the friends or groups who are allowed to access the content with allowed operation. On the other hand, the role of $ACL^-$ is to enumerate the friends or groups who are not allowed to access the content even if they hold an appropriate group relationship to access the content. For example, in $SN_B$ the user Alice would like all her high school friends (Group $G_1$) and music club friends (Group $G_2$) to be able to access her posted wedding photo album except her friend Bob (User $U_1$) refer to Figure 1 (a). Accordingly, for this photo album $ACL^+ = \{G_1, G_2\}, ACL^- = \{U_1\}$, and access is only given to users in $\{G_1, G_2\} \setminus \{U_1\}$. This exception based group approach $(ACL^+, ACL^-)$ is commonly adopted by state of the art SN sites such as Facebook.

### III. Proposed Framework

We propose the $x$-$mngr$ framework for managing content sharing and access control between SN sites as shown in Figure 2(a). The SN sites manage their own users, contents, and local policies. We refer to the $SN_B$ that hosts the shared content as the target site, and the $SN_A$ that accesses the shared content as the viewer site. We assume that a trusted party operates the $x$-$mngr$ between the SN sites. The $x$-$mngr$ manages user’s identity mapping across the SN sites. The user identity mapping includes the content owner’s identity mapping and friends’ identity mapping. All user’s identities are mapped by a unique identifier in the $x$-$mngr$. For example, Bob’s user id is $(U_1)$ on $SN_A$ and $(U10)$ on $SN_B$, and it is mapped by user id $(U1D1)$ on the $x$-$mngr$. The $x$-$mngr$ also manages the cross-site policies that control access across SN sites and the policy levels for the shared content. All cross-site sharing states are recorded in the Sharing State. It is used to help the content owners to maintain awareness about what they have shared and with who, which policy level is enforced, and who has accessed it. The details of the $x$-$mngr$ framework are discussed in subsequent sections.

### A. Local Policy

In each SN site, a user posting an object (content) $O$ on her profile is allowed to setup an access control policy to specify which friends are allowed/denied access to the posted object within each SN site. We named this access control policy LocalPolicy. The local policy is managed and stored by each SN site. We define the local policy as:

**Definition 1:** (Local Policy) Given a SN site, the local policy $P$ of an object $O$ is defined using two access control lists, namely the allow list $ACL^+$ and the exception list $ACL^-$, which are sets of the allowed and the denied users or groups respectively. Access control follows the closed world assumption, where if access is not explicitly specified it is assumed to be not accessible. For an object $O$ given $ACL^+$ and $ACL^-$, a user $u$ is given access to $O$ with allowed operation $OP$ iff $u \in ACL^+$ and $u \notin ACL^-$, or in compact form $u \in (ACL^+ \setminus ACL^-)$. The full format of local policy is $(O,ACL^+,ACL^-,OP)$.

The role of $ACL^+$ is to enumerate the friends or groups who are allowed to access the content with allowed operation. On the other hand, the role of $ACL^-$ is to enumerate the friends or groups who are not allowed to access the content even if they hold an appropriate group relationship to access the content. For example, in $SN_B$ the user Alice would like all her high school friends (Group $G_1$) and music club friends (Group $G_2$) to be able to access her posted wedding photo album except her friend Bob (User $U_1$) refer to Figure 1 (a). Accordingly, for this photo album $ACL^+ = \{G_1, G_2\}, ACL^- = \{U_1\}$, and access is only given to users in $\{G_1, G_2\} \setminus \{U_1\}$. This exception based group approach $(ACL^+,ACL^-)$ is commonly adopted by state of the art SN sites such as Facebook.

### B. Cross-Site Policy

The $x$-$mngr$ manages access control policy for shared content across SN sites. We named this policy Cross-Site Policy. The cross-site policy is defined as follows:

**Definition 2:** (Cross-Site Policy). Given a viewer site $SN_A$ and a target site $SN_B$, the cross-site policy $PA_{A-B}$ specifies the access control list $(O,ACL^+,ACL^-,OP)$ w.r.t subjects from the viewer site $SN_A$ and objects from the target site $SN_B$.

For instance, Alice posted her wedding album in the site $SN_B$. Alice would like to share the wedding album in site $SN_B$ with her college friends (Group $G_3$) in the site $SN_A$. The corresponding cross-site policy for Alice’s wedding album is $PA_{A-B} = (ACL^+ = \{SN_A, G_3\},ACL^- = \{\})$. Figure 1 (a) shows that the sites $SN_A$ and $SN_B$ manage the local policy $PA$ and $PB$ respectively and the $x$-$mngr$ manages the cross-site policy $PA_{A-B}$.

The cross-site policy includes content information, access control list, and permission elements as described in the XML representation in Figure 1 (b). The content information includes details of shared object such as content id, type, url, owner, site, and policy level. The access control list information includes the users and groups who are assigned to $ACL^+$ and $ACL^-$ respectively. The permission includes the allowed permissions. The default permission is read.
C. Secure Interoperation

The x-mngr maintains both the autonomy and security principles of secure interoperation [1]. The autonomy principle requires that any access permitted within an individual site must also be permitted in the same site under secure interoperation. The security principle requires that any access not permitted within an individual site must also be denied under secure interoperation.

Definition 3: (Safe). The x-mngr is safe if it does not deny legal requests or permit illegal requests from a viewer site to a target site.

The x-mngr has no control on enforcing the local policy on local sites. For example, the local policy $P_B$ is controlled and enforced by site $SN_B$ irrespective of the x-mngr decisions. It implies that the autonomy principle is obeyed. The challenge is to enforce the security principle as it requires the x-mngr to deny access to objects that would have been denied by the target site’s local policy $P_B$. For an object $O \in SN_B$ with a local policy $P_B$ defined as $P_B(ACL^+ \land ACL^-$, and a cross-site policy $P_{A \rightarrow B}$ defined by $P_{A \rightarrow B}(ACL^+)$ and $P_{A \rightarrow B}(ACL^-)$, a user $u$ from the viewer site $SN_A$ is given access to object $O \in SN_B$ if all the below conditions are satisfied:

- **C1.** $u \in P_{A \rightarrow B}(ACL^+ \land \neg ACL^-)$
- **C2.** $M_{A \rightarrow B}(u) \notin P_B(ACL^-)$

The condition (C1) ensures that the requesting user $u \in SN_A$ from the viewer site is permitted access via the cross-site policy $P_{A \rightarrow B}$. The condition (C2) involves the user identity mapping function $M_{A \rightarrow B} : u \rightarrow v$, where $u \in SN_A$ and $v \in SN_B$, which maps a user $u$ from a viewer site to a corresponding user $v$ from the target site. The mapped user $v = M_{A \rightarrow B}(u)$ is checked against $P_B(ACL^-)$ to ensure that this user is not explicitly denied access by being in the exception access list in the target site $SN_B$. The condition (C2) ensures that the exception list of the target site is respected, and it is not violated when requests are made through the x-mngr framework.

D. Policy Levels

In the III-C, the condition C1 and C2 are only applied when a viewer has accounts on both $SN_A$ and $SN_B$ and the content owner has specified the $P_B(ACL^-)$. Depending on the state of viewer’s accounts and the privacy sensitivity of the shared content, the condition C1 and C2 vary. For example, some viewers only have accounts on the viewer site, whereas other have accounts in both sites. Some contents are very private, so it might be shared with a specific friend group on the viewer sites. To support various cross-site sharing cases, we formulate three different policy levels as Figure 1(c) describes.

- **StrictLevel:** The first condition (C1) ensures that a viewer $u \in SN_A$ from the viewer site is permitted access via the cross-site policy $P_{A \rightarrow B}$. The second condition (C2) ensures that the mapped user $M_{A \rightarrow B}(u)$ is not explicitly denied by the local policy $P_B(ACL^-)$. If the viewer $u$ has accounts on both the viewer site and the target site, the viewer must satisfy the condition (C2), but if the viewer $u$ only has an account on the viewer site, the condition (C2) is not enforced. The strict policy level fits to the content owners who want to share a private content, and have blocked friends on the target site.

- **GeneralLevel:** it focuses on the cross-site policy. The first condition (C1) ensures that the viewer $u \in SN_A$ from the viewer site is permitted access via the cross-site policy $P_{A \rightarrow B}$. The second condition (C2) is not considered since the viewer $u$ only has account on the viewer site. This policy level is suitable for general content sharing between SN sites.

- **PublicLevel:** The cross-site policy is setup as $P_{A \rightarrow B}(ACL^+(ALL))$. By adding ALL value to $ACL^+$, any viewer $u \in SN_A$ from the viewer site can access the shared content.
IV. Evaluation

As a proof of concept, we provided an implementation of x-mngr framework between Facebook and MySpace. We developed a social application named MyCrossAlbum that enables users to share photos with their friends between Facebook and MySpace. We also conducted a user study to assess participants' understanding of the x-mngr framework and usability of the MyCrossAlbum interfaces. We recruited 13 participants from the university community.

![Image](a) The Cross-Site Policy panel (b) The Access History panel

Figure 2. The State of Sharing Photo interfaces

User Study Results: First, we showed a short introduction video of the x-mngr framework and measured participants' understanding using true/false quizzes. All participants selected right answers for all quizzes. We also measured the usefulness and preference of the x-mngr framework using Likert scale (5 point rating scale, where 1 = Strongly Disagree and 5 = Strongly Agree). The participants indicated that the content sharing across SN sites using the x-mngr framework is useful (M = 4.34, SD = 0.87), and they have the willingness to use it (M= 3.92, SD = 1.19). The difficulty of understanding and usefulness for the policy level was measured on Likert scale. The question is “The concept of policy level is difficult to understand”. The participants disagreed on the question (M=2.46, SD=1.05) and agreed the policy level is a useful way to control the policy enforcement for sharing content across SN sites (M=4.00, SD=0.58). These results showed the participants understood the x-mngr framework before we conducted the usability test. In addition, the participants had a positive attitude for the x-mngr framework and the policy level.

In the usability test of the cross-site policy interface, we asked the participants set up cross-site policy and refer to the assigned tasks. The test measures whether the participants are able to select right policy level, add right Friend List and exception on the cross-site policy interface. The participants spent average 63 seconds to complete the tasks. Six participants completed the tasks correctly. Three participants made a mistake on the policy level. Four participants failed the tasks. After the test, the participants indicated that the cross-site policy interface is easy to use (M=3.69, SD=0.95). However, we would like to know the reason why the participants failed or made mistakes. After finishing all user study, we had an interview with the participants who failed or made mistakes on the mission. The participants who failed the mission said they did not read the mission and just tested the interface. The participants who made a mistake on the policy level said they did not recognize the policy level, since they focused to specify the cross-site policy using the drag and drop. From these results, we found the participants who read the mission carefully completed the tasks easily, and few participants forget to change the policy level. In order to reduce the mistake in the policy level change, one possible solution is to ask the content owner to select a policy level after specifying the cross-site policy.

In the usability test of the status of sharing photo interface, we asked four questions that measure whether the participants can figure out the allowed Friend List and friends, the excepted friend on a Friend List, the accessed friends, and current policy level. All participants reported the correct answers for all questions. The participants indicated that the state of sharing photo interface is easy to use to figure out the current sharing state of photos (M=4.31, SD=0.63), and the state of sharing photo interface is useful to trace access history, and modify the cross-site policy (M=4.38, SD=0.65). These results show the state of sharing photo interface is useful to know the current sharing state of photo and modify the cross-site policy.

V. Conclusion

We presented a new cross-site content sharing framework between SN sites. We provided a cross-site policy and the policy levels to support the framework. Moreover, we demonstrated the feasibility of the x-mngr framework by implementing a photo sharing application between Facebook and MySpace. The user study results show that the participants had a positive attitude for the x-mngr framework and they specified the cross-site policy and understood the sharing status easily using the MyCrossAlbum interfaces. In the future, we will extend the cross-site policy as an open standard to promote the adoption of the x-mngr framework by current SN sites.

REFERENCES

