A User-Activity-Centric Framework for Access Control in Online Social Networks

Today's ever-evolving online social networks (OSNs) need an effective and usable access control framework. OSN users typically have discretionary control over their content, relationships, and interactions, while the OSN's policies consolidate these individual choices into specific access and filtering decisions. OSN access control can be built around the concept of user activity. To this end, the authors distinguish usage activity from control activity and identify four core control activities: attribute, policy, relationship, and session. Their user-activity-centric framework enables future extensions as needed.

Jaehong Park, Ravi Sandhu, and Yuan Cheng
University of Texas at San Antonio

Online social networks (OSNs) present a domain that's distinct from traditional access control. Although discretionary access control lets users configure access to their own resources, they typically do so in terms of user identities, group or role membership, and similar attributes. Access control in OSNs is driven more by user relationships based on social graphs, such as friends and friends of friends. In typical access control systems, a user accesses stored content, whereas in OSNs, additional activities occur, such as "poking" another user or recommending other users as friends. The targets of these activities are other users rather than shared content.

Furthermore, OSN systems make and enforce control decisions for user activities by collectively referencing related users' preferences and policies. Consider the user relationship graph that Figure 1a shows. Here, Homer might not want his coworkers to be notified of his activity. He might also want to prevent Bart from viewing any violent content, sharing contact information, or becoming a friend of Homer's coworkers. We call the expression of Homer's policies *control activities*. In both lattice- and role-based access controls, such control activities are administrative ones — that is, administrators or security officers define control policies for users. In OSNs, users participate in control activities on related users and content.

Myriad OSN services are available today, but users' control capabilities within these services are still rudimentary and will likely require further

1089-7801/11/$26.00 © 2011 IEEE

enhancement. For instance, a user might not want to reveal his location information or might want to use additional privacy rules on some occasions. Current OSNs rarely offer such options.

In this article, we propose developing an access control framework for OSNs around the concept of user activity. Our framework accommodates personalized privacy preferences for user activities and resources by separating individualized user and resource policies. Its scope goes beyond traditional access control in that it lets users control general *usage activity* as well as control activities such as attribute, policy, relationship, and session controls.

Access Control Framework

Figure 1b shows a conceptual depiction of our framework (its formalization is beyond our scope here). It comprises three main components: *users*, *sessions*, and *activities*. Each activity consists of an action, zero or more target resources, and zero or more target users.

Users

A user is a representation of a human and is associated with user attributes and policies. User attributes are properties or information about the user, such as a unique ID, name, address, age, or friend list. User policies are rules expressing preferences or limits. The user or his or her related users (such as parents) directly manage some attributes and policies. The OSN system manages others, often as a consequence of various user activities (as with consumable attributes, such as a credit balance, or a reputation attribute based on aggregated ratings from other users).

Sessions

A session is a representation of an active user who has logged into the OSN (we borrowed the term from role-based access control models[1]). The user-versus-session distinction is important if only to distinguish between those who are online and those who aren't. In the simplest case, a session inherits all the user's attributes and policies. More generally, a session might inherit only some, or might inherit them in a slightly modified form, such as substituting "over 18" for an actual age (represented via the "constrained by" relation in Figure 1b). A session might have additional attributes (such as an IP address or access to a device and its location) and policies (for instance, limited privileges if the session is on a mobile device). A user can have multiple concurrent sessions if the OSN permits, whereas a session belongs to exactly one user (indicated by the double versus single arrowheads in the figure).

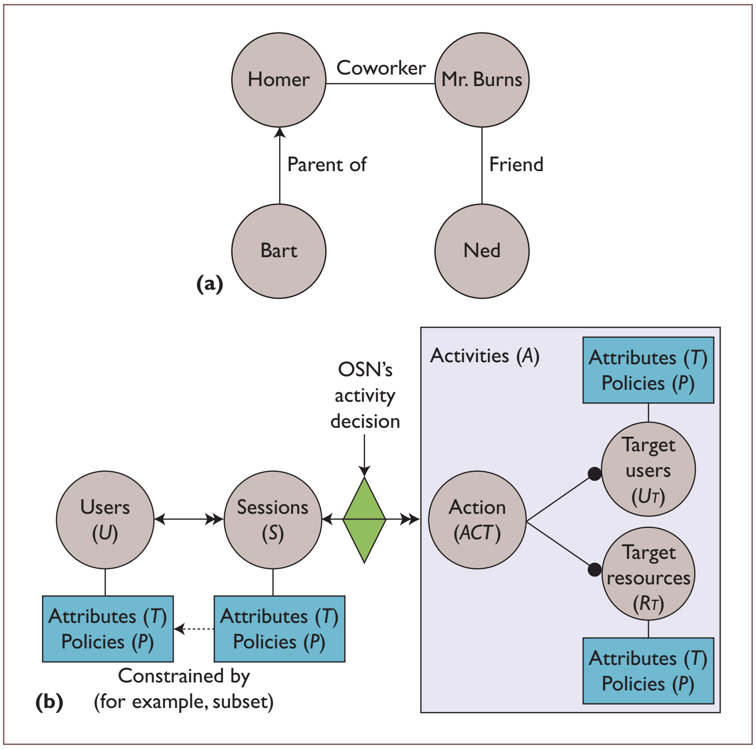

Figure 1. User-activity-centric framework. We can see (a) an example of online social network (OSN) user relationships and (b) the various framework components.

Although current OSNs don't support this capability, we believe future OSNs will find it useful to support sessions with user-controlled attributes and policies. For instance, a user might be allowed to disable some attributes or policies in some sessions, as when Homer doesn't want to reveal his friends' information to other users. He can achieve this by creating a session that doesn't convey his friends' information. On the other hand, some user attributes and policies might need to be required for a session that performs certain actions. For example, an OSN system might mandate some user attributes and policies in all sessions, such as a user ID or a basic geographic location. We believe the relationship between session and user attributes and policies provides a fertile arena for developing more nuanced access control and privacy in future OSNs.

Activities

The notion of activities encompasses both general usage activities and users' control activities.

A session initiates each activity on the user's behalf. The OSN decides whether the activity is permitted. A session can have multiple activities, whereas each activity is initiated by only a single session. Each activity comprises an *action*, *target resources*, and *target users*.

Action. Each action is an abstract function available to OSN users via a session. Examples include when a user reads or writes a comment, likes another user's posting, invites another user to be a friend or group member, or indirectly triggers an activity notification action that's delivered to friends. User actions can be carried out on target resources, target users, or both. For example, read and write actions require target resources, whereas friendship recommendation actions require two or more target users, and typical notification actions require both (that is, multiple target users will receive notification of an acting user's activity information, such as a comment on a picture).

Target resources. Target resources are those involved in an action. They can include users' shared content; profile information; user, resource, or session policies and attributes; and any other digital information that users can access or manage in the OSN. By considering policies and attributes (in addition to shared content) to be part of the resource abstraction, our framework supports users' ability to partially control their own attributes and policies as well those of related users. Furthermore, the framework covers the policies and attributes of these policy and attribute resources. For example, Bart's "no access to violent content" policy could have its own policy stipulating that only Homer can change it, or an attribute that provides information about the policy creator. As another example, a video clip's provider attribute can have a policy that says only the provider's friends can read the attribute information. Although, theoretically, this chaining can continue indefinitely, we believe practical OSN systems won't likely provide policies and attributes on policies and attributes beyond one or two levels.

Target users. Target users are the recipients of an action. For example, if Ned invites Homer as a friend or for a chat, Homer's the target user while Ned is the *acting user*. (More precisely, Homer's sessions receive the invitation.) If Homer's session has a policy that says it doesn't ever want to chat, Ned's attempt to chat will fail.

OSN Activity Decision

Ultimately the OSN system consolidates all the necessary individual policies and attributes together with its own policies and uses them to decide whether to permit specific users' activity requests. Assume Homer has a policy that says anyone who is his coworker or a direct friend of his coworker can't be a friend to his children. Using this policy, the OSN makes sure Bart's policy reflects Homer's policy by either updating Bart's policy or evaluating Bart's parents' policies each time Bart attempts an activity. If Bart (in a session) tries to send a friendship invitation (an action) to Ned (a target user), the OSN evaluates Bart's policy and possibly those of his parents, then verifies whether any of Ned's friends (the target user's attribute) are Homer's coworkers.

Discussion

Our framework has some distinctive characteristics. The first is policy individualization, which is essential for access control in OSN environments. Unlike in traditional access control systems — such as lattice- or role-based access control, where a single, system-wide security policy is applied to all users — OSN users have their own security and privacy policies and attributes, which the OSN uses collectively to make decisions on user activities. Individuals or related users can manage these policies and attributes themselves.

Another characteristic is the separation of user and resource policies. Some policies are specific to individual users, whereas others are specific to resources, so certain activity controls should be enforced with user policies (such as a filtering policy[2]) and others using resource policies. For instance, using resource policies to filter out violent content from Bart (and other users) would require adding one rule per excluded user in the resource policies of every violent resource, which isn't scalable. Including the rule "no access to violent content" in each excluded user's policy is better.

Unlike others' work on OSNs,[2–6] which focuses exclusively on user relationships, our framework also supports user-relationship-independent access controls. More specifically, it can support attribute-based access control in general, such as the authorization component of usage control.[7]

Our framework also supports sessions that represent active users, which allows for enhanced controls that we don't find in existing OSN services and literature. Specifically, a user can minimize shareable attributes and change his or her policies to have better security and privacy control, while the OSN system ensures that this doesn't violate other users' policies. Many existing OSNs (such as Facebook or MySpace) allow a session with some additional attributes or policies that the OSN controls but don't enable any user-controllable session attributes or policies. Much of the recent literature on OSN access controls doesn't distinguish a session from a user.[2–6]

The recent OpenSocial specification seeks to standardize API language specifications for OSNs,[8] and is complementary with our framework. Proposals for OpenSocial Access Control Lists (ACLs), Activity Privacy API, and Album and MediaItem Privacy API suggest API specifications for ACLs that are attached to resources in OSNs.[9] Unlike our framework, OpenSocial narrowly defines activity to mean information (a log) about events (such as user actions), which our framework views as a resource. Thus, the OpenSocial Activity Privacy API is mainly for user activity notification controls and defines a specification language for policies that are attached to the user activity log. In our framework, users can control activity notification by specifying either user policies or resource (for example, activity log) policies, depending on whether the notification policy applies to a specific user or a specific activity.

In contrast to traditional access control application domains, OSNs are uniquely centered around users' usage and control activities. Studying access control issues simply based on user relationships is insufficient to comprehensively understand security and privacy issues in OSNs. Our proposed user-activity-centric framework provides a conceptual sketch for understanding the essential nature of OSN access control. This framework will provide a foundation for future development of access control policies and models for OSNs with enhanced security and privacy protection support.

Acknowledgments

This work is supported by grants from the US National Science Foundation and the state of Texas.

References

1. R.S. Sandhu et al., "Role-Based Access Control Models," *Computer*, vol. 29, no. 2, 1996, pp. 27–38.
2. B. Carminati et al., "A Semantic Web-Based Framework for Social Network Access Control," *Proc. 14th ACM Symp. Access Control Models and Technologies*, ACM Press, 2009, pp. 177–186.
3. 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, 2009, pp. 1–38.
4. P.W.L. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems," *Proc. 14th European Symp. Research in Computer Security*, Springer, 2009, pp. 303–320.
5. P.W.L. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," *Proc. ACM Conf. Data and Application Security and Privacy* (CODASPY 11), ACM Press, 2011.
6. A. Cinzia Squicciarini, M. Shehab, and F. Paci, "Collective Privacy Management in Social Networks," *Proc. 18th Int'l Conf. World Wide Web*, ACM Press, 2009, pp. 521–530.
7. J. Park and R. Sandhu, "The UCON_{ABC} Usage Control Model," *ACM Trans. Information and System Security*, vol. 7, no. 1, 2004, pp. 128–174.
8. *OpenSocial Specification 1.1*, OpenSocial, 2010; www.opensocial.org/specs.
9. C. Renner, *Privacy in Online Social Networks*, master's thesis, Swiss Federal Institute of Tech., Zurich, 2010.

Jaehong Park is a research associate professor at the Institute for Cyber Security at the University of Texas at San Antonio. Contact him at jae.park@utsa.edu.

Ravi Sandhu is the founder and executive director of the Institute for Cyber Security, holds the Lutcher Brown Endowed Chair in Cyber Security, and is a professor in the Department of Computer Science at the University of Texas at San Antonio. Contact him at ravi.sandhu@utsa.edu.

Yuan Cheng is a doctoral student in the Department of Computer Science and the Institute for Cyber Security at the University of Texas at San Antonio. Contact him at ycheng@cs.utsa.edu.