2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing

Sharing and Privacy-Aware RBAC in Online Social Networks

Ahmad Kamran Malik, Schahram Dustdar
Distributed Systems Group, Vienna University of Technology, Austria
{kamran, dustdar}@infosys.tuwien.ac.at

Abstract – **Online social networks have gained enormous popularity in the last decade. Users share their private information online with other users, which is becoming a serious privacy issue at the social and technical level. In a society, everyone is a member of many collaborative groups (social circles), for example, colleagues, class fellows. There are many collaborative relationships among group members. Current social networks mostly use friend as a relationship, which in our social life, is not practical. In a society, we have different levels of collaborative relationships with others and even some relationship with non-friends. We use collaborative groups and relationships that facilitate users in controlling the privacy and sharing level of their information in social networks. We present a sharing and privacy-aware SP-RBAC model by extending the well-known RBAC model. Our model increases the collaborative community of a user, and hence increases sharing of information, minimizing the privacy threats using simple user management.**

Keywords- Social network, Privacy, Access control, Information sharing.

I. INTRODUCTION

With the advances in social software technologies [1], information sharing and privacy issues become critical. Social network users share their private information like personal address, phone number, relationships, pictures, and other stuff with connecting users. They are conscious of the privacy of their information, and at the same time want to share their information like new pictures, status messages, and links with more and more users. Information sharing is a need of the day [2] that helps people get knowledge, stay connected, and enhance social circles, while information privacy laws like HIPAA [3] demand for the protection of user information from unauthorized access and usage. There is a trade-off among information sharing and privacy, which requires an information sharing and privacy model that preserves the privacy of user information but not at the cost of information sharing.

In our social communities, everyone is a member different collaborative groups (social circles), for example, colleagues, class fellows, etc. In a society, we have different levels of collaborative relationships with others and even some relationship with non-friends. In a collaborative group, there are different collaborative relationships among group members, for example, close friend, friend, friend-of-friend, not friend, etc. We use collaborative groups and relationships to facilitate user to control her information sharing and privacy in social networks. A user can allow everyone in a social circle to connect with and share a certain level of her information. A user will make many collaborative groups, and each collaborating user will be assigned a collaborative relationship. This is similar to our social interactions. We meet many people in different social circles and we talk/share with each person depending on our collaborative relationship. Our model increases the number of connected users and provides simple user management by grouping users and assigning a relationship. All users in one group and having the same relationship with the owner will get the same level of information in general. In certain cases, an owner can use separate sharing rules and conditions to allow or restrict other users.

Existing systems based on access control technology such as Role-Based Access Control (RBAC) are widely being used to control the access to information. RBAC and other access control models do not explicitly handle sharing and privacy issues using collaborative groups and relationships among users. For this reason, we extend RBAC model, which is described in [4] and standardized in [5], to handle our sharing and privacy requirements. We present a sharing and privacy-aware role-based access control (SP-RBAC) model. It includes new elements like collaborative relationship, access level, and condition. Many access control researchers have extended RBAC model for their specific requirements. For example, access control and privacy for social networks is described in [6][7]. Moreover, privacy-aware system for RBAC is described in [8] that extends RBAC model to include privacy elements. It provides a privacy permission assignment language using purpose, condition and obligation. A privacy policy model for enterprises is described in [9]. These systems concentrate only on privacy preserving without a focus on sharing enhancement, collaborative groups, and relationships among collaborating users.

The remainder of the paper is organized as follows. Section II describes sharing and privacy in online social networks. Section III explains sharing and privacy-aware role-based access control (SP-RBAC) model. Section IV describes permission assignments. Section V describes background and related work. Section VI concludes the paper and describes future work.

978-0-7695-4578-3/11 $26.00 © 2011 IEEE
DOI

II. SHARING AND PRIVACY IN ONLINE SOCIAL NETWORKS

In online social networks, users share their personal information with friends, family, colleagues, and some unknown users for increasing their social interactions and networking. Users are conscious about their information being used in online communities of people, companies, and applications from all over the world. There is a need to control user's personal information at the user level in a way that reflect user's interactions in their social life. We propose a model that is based on collaborative groups and collaborative relationships among users. A user should not be limited to make contacts with only trusted or known users. User should also not be limited to declare every connected user as a friend. Using our model, a user can allow everyone in a certain social circle to connect with and share a certain level of her information. A user will make many groups of connections, and each collaborating user will be assigned a collaborative relationship. Users who are in close collaborative relationship can share more information than others.

A. Collaborative Groups

Our model uses collaborative groups of users. These groups are handled in our model similar to roles in RBAC. There can be different types of as many groups as user wishes. A user can create groups like class fellows in a certain college or colleagues of a certain company, etc. This helps managing a number of different types of users and their permissions. A collaborative group, assigned to a connected user, acts as the role of that user.

B. Collaborative Relationships

Collaborative relationships are the backbone of our social interactions. We think about our emotional relationships with other people as close friend, friend, not friend, etc. A person holds different relationships with different people in the same collaborative group. It depends on our relationship and trust on others. In our model, a user can use a *not friend* relationship with another user whom she wants to share a certain level of non-private information. Other users will not know what relationship she has mentioned about them. Generally, collaborations are called connections among users in our system, which is different from making everyone a *friend*, for example, in facebook. Many different types and names of collaborative relationships can be created by a user. Collaborative relationships help in managing different level of information sharing with each relationship within a group.

In the following sections, we formally define SP-RBAC model that uses collaborative groups as roles, collaborative relationships, access level, and conditions.

III. SHARING AND PRIVACY-AWARE ROLE-BASED ACCESS CONTROL (SP-RBAC) MODEL

Like NIST standard RBAC model [5], our SP-RBAC model is composed of three SP-RBAC components: Core SP-RBAC, Hierarchical SP-RBAC, Constrained SP-RBAC. We describe each of these components in the following subsections.

A. Core SP-RBAC

SP-RBAC model is shown in Figure 1.

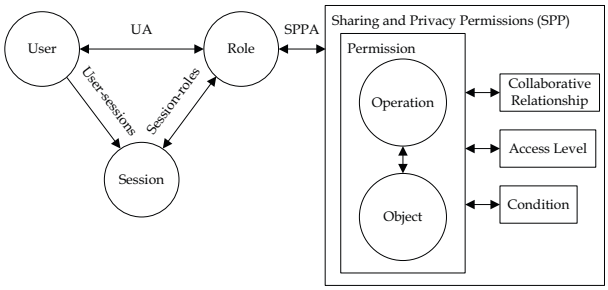

Fig. 1. Core SP-RBAC model

SP-RBAC model is based on and extends NIST standard RBAC [5]. For handling user controlled sharing and privacy, we introduce CR (Collaborative Relationships), AL (Access Levels), and Con (Condition) elements. User in our system is a human being. Role represents a collaborative group created by a user. When a user is assigned a certain group, she actually is assigned role representing that group which can be used for accessing objects from other users within that group. Object in our system is personal information related to collaborating users and their connections. Operation in our system is an executable image of a program, which a user can execute to perform some function. Permission (Perm) is an operation allowed on an object. Sharing and privacy based permissions (SP_Perm) are the permissions that include sharing and privacy elements and conditions. In SP-RBAC model, SP_Perm are assigned to roles. These permissions contain collaborative relationship, access level, and zero or more conditions. CR element restricts the sharing of information to only those users who are in certain collaborative relationship with each other. AL element describes the level of information sharing among users who are in certain CR with each other. Controlling information sharing using collaborative relationships among users can result in enhanced level of information flow among collaborating users in addition to preserving the privacy of user's information. User's personal information is stored in different levels of hierarchies. AL element uses these information levels to control the sharing of information among users having different collaborative relationships and roles (collaborative groups). Condition element is the user-defined condition that must be fulfilled to access information. One or more users are assigned one or more roles depending on how many collaborative groups they are participating. A session is a mapping of one user to one or more roles. A user establishes a session and activates roles in the session by selecting her collaborative groups.

B. Formal Description of Core SP-RBAC

Here we describe all elements, their assignments, and functions used in Core SP-RBAC model. Following are the elements in core SP-RBAC model:

U, R, Obs, Ops, CR, AL, and Con are users, roles, objects, operations, collaborative relationships, access levels, and conditions.

Following are the core RBAC model elements:

- U: the set of users in our system.
- R: the set of roles.
- 2^R: the power set of R.
- Obs: the set of objects that need to be accessed/shared.
- Ops: the set of operations on objects. Operations are executable image of a program that performs some operation on objects when invoked by a user.

Following elements are added in SP-RBAC model for handling sharing and privacy of information:

- CR: the set of collaborative relationships defined in system.
- AL: the set of access levels (hierarchical levels defined for objects) defined to allow access at a particular level of granularity.
- Con: Condition expression.

Following are the assignment relations among elements of SP-RBAC model:

- $UA \subseteq U \times R$, a many to many mapping user-to-role assignment relation.
- $Perm = 2^{(Ops \times Obs)}$, the set of permissions.
- $SP\_Perm = (Perm, CR, AL, Con)$, the set of sharing and privacy based (SP) permissions.
- $PA \subseteq Perm \times R$, a many to many mapping permission-to-role assignment relation.
- $SPPA \subseteq SP\_Perm \times R$, a many to many mapping sharing and privacy based permission-to-role assignment relation.

Following are the function mappings used in SP-RBAC model:

- $assigned\_users : (r : R) \rightarrow 2^U$, the mapping of role r onto a set of users.
- $assigned\_users(r) = \{u \in U \mid (u, r) \in UA\}$.
- $assigned\_permissions : (r : R) \rightarrow 2^{SP\_Perm}$, the mapping of role r onto a set of SP-based permissions.
- $assigned\_permissions(r) = \{p \in SP\_Perm \mid (p, r) \in SPPA\}$.

Following are the details of sessions and their mappings:

- $SessionS$: the set of sessions
- $user\_sessions(u : U) \rightarrow 2^S$, the mapping of user u onto a set of sessions.
- $session\_user(s : S) \rightarrow u \in U$, the mapping of each session s_i to a single user of session s_i.
- $session\_roles(s : S) \rightarrow 2^R$, the mapping of session s_i onto a set of roles.
- $session\_roles(s_i) \subseteq \{r \in R \mid (session\_user(s_i), r) \in UA\}$.
- $avail\_session\_permissions(s : S) \rightarrow 2^{SP\_Perm}$, the SP_permissions available to a user u in a session, $\bigcup_{r \in session\_roles(s_i)} \{assigned\_permissions(r)\}$

C. Hierarchical SP-RBAC Model

Hierarchical RBAC component of the RBAC model introduces role hierarchies where a role can inherit permissions of other roles. SP-RBAC introduces CR hierarchy, AL hierarchy, and Object hierarchy in addition to role hierarchies. Similar to role hierarchy, where a higher-level role can inherit permissions of its lower-level roles, CR, AL, and objects have hierarchical relationships. For example, in CR hierarchy, a close friend relationship can inherit permissions of friend relationship. Similarly, instead of specifying permission assignments for each AL, the permission to the most detailed access level of an object can be assigned to a user, for example, user's complete address instead of only city name or country name. Moreover, different objects can have hierarchical relationships. A single permission for a higher-level object like an album can be used instead of each picture permission.

IV. PERMISSION ASSIGNMENTS

In this section, we describe the permission assignment used in SP-RBAC model called sharing and privacy-aware permission assignment (SPPA).

Elements used in our model consist of following types: RBAC-based elements like user, role, session, object, operation and sharing and privacy-aware elements like CR, AL, and Condition. Conditions in our system can be described as simple or complex conditions. Simple conditions consist of a condition variable, an operator, and a condition value: $(cond\_var\ op\ val)$. Complex conditions consist of many disjunctions of conjunctive statement. Formally complex conditions are described below:

$condition := clause \cup clause... \cup clause$
$clause := stemenet \cap statement... \cap statement$
$statement :=< context >< OP > \{< value > | < context >\}$

Condition variables in SP-RBAC are either context variables, or element-based conditions that include user, collaborative group, or collaborative relationship. Individual element-based conditions provides instance level permissions and thus result in providing fine-grained access control.

Sharing and privacy permission assignments include all the elements used in SP_RBAC model and are formally shown below.

- Object permission $Perm$ consist of object Obs and their operations Ops. So the set of permissions is defined as:

  $Perm = \{(obs, ops) \mid obs \in Obs, ops \in Ops\}$.

- Sharing and privacy-aware permissions SP_Perm contain sharing and privacy elements and are defined as:

  $SP\_Perm = \{(perm, cr, al, con) \mid perm \in Perm,$
  $cr \in CR, al \in AL, and\ con \in Con\}$.

- Sharing and privacy-aware permissions assignments $SPPA$ is defined as:

  $SPPA \subseteq R \times SP\_Perm$.

SPPA are type-based permissions that use role types. A permission for a specific element can also be defined in SP-RBAC and such condition is specified using the condition element. In the presence of hierarchies, many permission assignments (SPPAs) containing same operation can be replaced by single SPPA. This is because higher-level data objects in a hierarchy inherit permissions of their lower-level data objects.

V. BACKGROUND AND RELATED WORK

Access control researchers have extended RBAC model for their specific requirements. A number of languages and systems have been described in literature to enforce privacy by extending RBAC model. For example, privacy-aware systems for social networks are described in [6] and [7]. They describe privacy threats and define protocols for privacy-aware collaborative social networks. Furthermore, a privacy-aware system for RBAC is described in [8]. It describes a privacy permission assignment language using purpose, condition and obligation. A privacy policy model for enterprises is described in [9]. These systems concentrate only on privacy preserving without a focus on sharing enhancement among collaborators. Other collaborative systems include Team-Based Access Control model [10], and Task-Based Access Control model [11]. They extend RBAC to assign permissions based on team and task of the user. They do not handle privacy and enhanced sharing requirements, and collaborative relationships among users. Context-based RBAC systems have been an interesting area of research as can be seen in [12] [13].

Access policy for collaborative environments and their requirements have been described in [14]. RBAC can be used in collaborative systems as explained in [15] and in a survey by [16]. Access control lists and capability lists were used to describe the access of subjects to objects [17], but they were not scalable to handle a large number of users in a system. The breakthrough in modeling access control systems was the creation of RBAC model [4], which defines roles for user rights. RBAC is an efficient model for the management of permissions in large-scale systems. Still, it lacks in fulfilling the privacy, enhanced sharing, and fine-grained access level requirements of collaborative systems. Collaborative system requirements for RBAC can be seen in the system [15] and in a survey by [16]. RBAC is basically a type-based access control model using roles and is a rather static model. It lacks in handling fine-grained level access control and dynamic access control requirements of collaborative systems.

VI. CONCLUSION AND FUTURE WORK

The paper describes sharing and privacy-based role-based access control model (SP-RBAC). It describes sharing and privacy of user information in online social networks. Our model is based on and extends the RBAC NIST standard model. SP-RBAC uses collaborative groups and collaborative relationships among users. It includes collaborative relationships, access level, and condition elements in addition to role (as collaborative group) and user entities in RBAC. These elements provide sharing and privacy based data permissions. SP-RBAC is a family of models, including core SP-RBAC model, Hierarchical SP-RBAC model, and Constrained SP-RBAC model. Sharing and privacy-based permission assignments are described. In future we intend to handle different types of permission assignments and their conflict types in different scenarios.

ACKNOWLEDGEMENT

This work is partially supported by the Higher Education Commission (HEC), Pakistan and the European Union through the FP7-216256 project COIN.

REFERENCES

[1] M. N. Kamel Boulos and S. Wheeler, "The emerging web 2.0 social software: an enabling suite of sociable technologies in health and health care education," *Health Information & Libraries Journal*, vol. 24.

[2] K. Smith, L. Seligman, and V. Swarup, "Everybody share: The challenge of data-sharing systems," *IEEE Computer*, vol. 41, no. 9, pp. 54–61, 2008.

[3] "United state department of health. health insurance portability and accountability act of 1996," Available at http://www.hhs.gov/ocr/hipaa/.

[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[5] D. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," ACM Trans. on Information and System Security (TISSEC), 4(3): 224-274, Aug. 2001.

[6] B. Carminati and E. Ferrari, "Access control and privacy in web-based social networks," *IJWIS*, vol. 4, no. 4, pp. 395–415, 2008.

[7] B. Carminati and e. Ferrari, "Enforcing relationships privacy through collaborative access control in web-based social networks," in *CollaborateCom*. IEEE, 2009, pp. 1–9.

[8] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C.-M. Karat, J. Karat, and A. Trombeta, "Privacy-aware role-based access control," *ACM Trans. Inf. Syst. Secur.*, vol. 13, pp. 24:1–24:31, July 2010. [Online]. Available: http://doi.acm.org/10.1145/1805974.1805980

[9] G. Karjoth and M. Schunter, "A privacy policy model for enterprises," in *CSFW*. IEEE Computer Society, 2002, pp. 271–281. [Online]. Available: http://csdl.computer.org/comp/proceedings/csfw/2002/1689/00/16890271abs.htm

[10] C. K. Georgiadis, I. Mavridis, G. Pangalos, and R. K. Thomas, "Flexible team-based access control using contexts," in *Proceedings of the sixth ACM symposium on Access control models and technologies*, ser. SACMAT '01. New York, NY, USA: ACM, 2001, pp. 21–27. [Online]. Available: http://doi.acm.org/10.1145/373256.373259

[11] R. K. Thomas and R. S. Sandhu, "Task-based authorization controls (tbac): A family of models for active and enterprise-oriented autorization management," in *Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Securty XI: Status and Prospects*. London, UK, UK: Chapman & Hall, Ltd., 1998, pp. 166–181. [Online]. Available: http://portal.acm.org/citation.cfm?id=646115.679940

[12] R. J. Hulsebosch, A. H. Salden, M. S. Bargh, P. W. G. Ebben, and J. Reitsma, "Context sensitive access control," in *Proceedings of the tenth ACM symposium on Access control models and technologies*, ser. SACMAT '05, New York, NY, USA, 2005, pp. 111–119.

[13] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using environment roles," in *Proceedings of the sixth ACM symposium on Access control models and technologies*, ser. SACMAT '01. New York, NY, USA: ACM, 2001, pp. 10–20. [Online]. Available: http://doi.acm.org/10.1145/373256.373258

[14] H. Shen and P. Dewan, "Access control for collaborative environments," in *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, ser. CSCW '92. New York, NY, USA: ACM, 1992, pp. 51–58. [Online]. Available: http://doi.acm.org/10.1145/143457.143461

[15] G. Ahn, "Authorization management for role based collaboration," IEEE int. conf. on System, Man and Cybernetic, Washington, 2003.

[16] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Access control in collaborative systems," *ACM Comput. Surv.*, vol. 37, pp. 29–41, March 2005. [Online]. Available: http://doi.acm.org/10.1145/1057977.1057979

[17] R. Sandhu and P. Samarati, "Access control: Principles and practice." IEEE Communications, 1994.