Decentralized Administration in Collaborating Organizations

SYLVIA ENCHEVA
Stord/Haugesund University College
Department Haugesund
Bjørnsonsg. 45, 5528 Haugesund
NORWAY

SHARIL TUMIN
University of Bergen
IT-Dept.
P. O. Box 7800, 5020 Bergen
NORWAY

Abstract: This paper focuses on a model preventing conflicts generated by applying positive and negative authorizations to users accessing resources in a large networked system.

Key–Words: Collaboration, positive and negative authorization

1 Introduction

Positive authorizations define accesses that are going to be allowed [1]. Unfortunately, positive authorizations cannot prevent a particular user without a given authorization from this policy to obtain an authorization from a different resource manager.

Authorization models supporting negative authorization apply open policy, i.e. accesses are to be allowed to all but a few users. Applications are discussed in [2], [4], and [9]. Negative authorizations are often used because they give opportunities to include exceptions [7].

This paper focuses on a model preventing conflicts generated by applying positive and negative authorizations to users accessing resources in a large networked system.

The rest of the paper is organized as follows. Related work, basic terms and concepts are presented in Section 2. The model is described in Section 3 and the system in Section 4. The paper ends with a conclusion in Section 5.

2 Background

A formal model of role based access control (RBAC) is presented in [12]. Permissions in RBAC are associated with roles, and users are made members of appropriate roles, thereby acquiring the roles' permissions. The RBAC model defines three kinds of separation of duties - static, dynamic, and operational. Separation of duties was discussed in [7], [13] and [17]. A framework for modeling the delegation of roles from one user to another is proposed in [3]. A multiple-leveled RBAC model is presented in [10]. The design and implementation of an integrated approach to engineering and enforcing context constraints in RBAC environments is described in [18] and [19].

While RBAC provides a formal implementation model, Shibboleth [16] defines standards for implementation, based on OASIS Security Assertion Markup Language (SAML). Shibboleth defines a standard set of instructions between an identity provider (Origin site) and a service provider (Target site) to facilitate browser single sign-on and attribute exchange.

The semantic characterization of a four-valued logic for expressing practical deductive processes is presented in [6]. The Belnap's logic has four truth values 'T, F, Both, None'. The meaning of these values can be described as follows:

- an atomic sentence is stated to be true only (T),
- an atomic sentence is stated to be false only (F),
- an atomic sentence is stated to be both true and false, for instance, by different sources, or in different points of time (Both), and
- an atomic sentences status is unknown. That is, neither true, nor false (None).

A user is defined as a valid domain identity at a particular organization Ξ_i. A group is a set of users. A resource defines a set of protected Web objects. A permission defines a right of a user to perform an action on a resource. An authorization gives a set of permissions to a user to execute a set of operations on a specific set of resources.

A billatice is a set equipped with two partial orderings $\leq_t$ and $\leq_k$. The t partial ordering $\leq_t$ means that if two truth values a, b are related as $a \leq_t b$ then b is at least as true as a. The k partial ordering $\leq_k$ means that if two truth values a, b are related as $a \leq_k b$ then b labels a sentence about which we have more knowledge than a sentence labeled with a.

3 Model

Assume existence of two groups, interested to access a particular resource, are managed by two different resource managers where one of them is applying closed policy and the other is applying open policy. Conflicts of access permits may occur if a user belongs to both groups. Such conflicts can be avoid if four-valued logic is applied.

If two collaborating organizations have groups described as above and wish to avoid conflicts related to access permits than sexteen-valued logic should be applied.

This management model refers to collaborating organizations using resources hosted by some of these organizations. Suppose a resource at one organization can be accessed by two groups Υ_1 and Φ_1 of members of organization Ξ_1 and two groups Υ_2 and Φ_2 of members of another organization Ξ_2. Suppose these four groups are administered by four resource managers, two at organization Ξ_1 and two at organization Ξ_2. Assume the resource managers of groups Υ_1 and Υ_2 apply closed policy and the resource managers of groups Φ_1 and Φ_2 apply open policy.

The following conflict situations that may occur
- a user belongs to group Υ_1 or group Υ_2 and at the same time belongs to group Φ_1 or group Φ_2,
- another user may be affiliated with two organizations and belong to three or four groups.

Solution

All groups $\Upsilon_i, i = 1, ..., n$ are considered as one group Υ and all groups $\Phi_i, i = 1, ..., n$ are considered as one group Φ with respect to the resource.

Based on the truth table for Belnap's logic [6] we propose the following:

- A user belongs to group Υ and does not belong to group Φ. The user is authorized to access the resource.
- A user belongs to both groups Υ and Φ. The user is not authorized to access the resource before his/her membership is considered by the corresponding resource managers.
- A user is neither a member of group Υ nor of group Φ. The user is authorized to access the resource, provided he/she belongs to at least one of the organizations applying open policy.
- A user does not belong to in group Υ and belongs to group Φ. The user is not authorized to access the resource.

4 System

Within this model, both the publisher organizations and the subscriber organizations need to provide Web services for each other in order to communicate user identities and authorizations to control access on shared Web resources. There are many ways of providing these services, where among most common ones are, Java based remote method invocation (RMI), XML remote procedure (XML-RPC) and Simple Object Access Protocol (SOAP). We propose a simpler mechanism inspired by Representational State Transfer.

The subscriber organizations provide a portal to their local users. By using cookies and redirect, an authenticated user can be transferred from local portal to a shared Web resource. The central issue in implementing the system is on how the XML responses from the server look like. We propose providing XML response containing security information together with the reply.

5 Conclusion

The problem with a user is affiliated with an organization applying both positive and negative authorization managed by different resource managers or with several organizations at the same time, is difficult to solve. Our proposed solution is based on many-valued logic.

References:

[1] Al-Kahtani M., Sandhu, R.: Rule-based RBAC with negative authorization. 20th Annual Computer Security Applications Conference, Arizona (2004)

[2] Andress, M.: Access control. Information security magazine, April, (2001)

[3] Barka, E., Sandhu, R.: Role-based delegation model/ hierarchical roles. 20th Annual Computer Security Applications Conference, Arizona (2004)

[4] Barkley, Beznosov, and Uppal: Supporting relationships in access control using Role Based Access Control, Fourth ACM Workshop on Role-Based Access Control (1999)

[5] Belnap, N.J.: How a computer should think. In Contemporary Aspects of Philosophy. Proceedings of the Oxford International Symposia, Oxford, GB, (1975) 30–56

[6] Belnap, N.J.: A useful four valued logic, *Modern uses of multiple-valued logic*, J.M. Dunn and G. Epstain (eds), D. Reidel Publishing Co., Dordrecht (1977) 8–37

[7] Bertino E., Bonatti, P.A., Ferrari E.: TRBAC: A temporal Role-Based Access Control model. ACM Tr. on ISS, **3**(3), (2001) 191-223

[8] Bertino E., Jajodia S., Samarati P. A Flexible Authorization Mechanism for Relational Data Management System, ACM Transactions on Information Systems, Vol. 17, No. 2, 1999, 101-140.

[9] Bhatti, R., Bertino E., Ghafoor A., Joshi, J.B.D.: XML-based specification for Web services document security. IEEE Computer **37**(4) (2004)

[10] Chou, S-C.; L^nRBAC: A multiple-levelled Role-Based Access Control model for protecting privacy in object-oriented systems. J. of Object Technology **3**(3), (2004) 91-120

[11] Davey, B. A. and Priestley, H. A.: Introduction to lattices and order. Cambridge University Press, Cambridge (2005)

[12] Ferraiolo, D., Cugini, J., Kuhn., D. R.: Role-Based Access Control (RBAC): Features and motivations. 1995 Computer Security Applications Conference (1995) 241-248

[13] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn R.D., Chandramouli R.: Proposed NIST standard for Role-Based Access Control. ACM Transactions on Information and System Security (TISSEC) **4**(3) (2001) 224-274

[14] Ferraiolo, D., Kuhn., D. R., and Chandramouli R.: Role-Based Access Control. Artech House, Computer Security Series, (2003)

[15] Schwoon, S., Jha, S., Reps, T., Stubblebine S.: On generalized authorization problems. Proc. 16th IEEE Computer Security Foundations Workshop, (June 30 - July 2, 2003, Asilomar, Pacific Grove, CA), (2003) 202-218

[16] http://shibbolethinternet2.edu

[17] Simon R., M. Zurko M.: Separation of duty in role-based environments. In Proceedings of 10th IEEE Computer Security Foundations Workshop, Rockport, Mass., June (1997) 183–194

[18] Strembeck, M.: Conflict checking of separation of duty constraints in RBAC-implementation experiences. http://wi.wu-wien.ac.at/home/mark/publications/se2004.pdf

[19] Strembeck, M., Neumann, G.: An integrated approach to engineer and enforce context constraints in RBAC environments. ACM Transactions on Information and System Security, **7**(3) (2004) 392-427