Role-Based Access Control (RBAC)
Feb 22, 2005
Discussant: Haiyan Cheng

Relationship to DAC/MAC/XACML/LDAP/GBAC (Group Based Access Control)

1. (Vinod Eligeti) What is the exact difference between DAC and MAC?
2. (Vinod Eligeti) Is the XACML is superior to the RBAC model? Because all you need is to access is some resources. But those resources are checked against permissions or roles in RBAC. But that is it and no extensions. But in XACML one can set policies besides these roles. So on what factors one can decide over RBAC over XACML?
3. (Vinod Eligeti) Is this RBAC advancement over the LDAP? Because in the present situations lot of companies has these roles and groups set up in the LDAP. But I do not have extensions like constraints (dynamic ad static). Is this is what the RBAC is solving?
4. (Varun Narayan Pandey) I think RBAC method is a just a new name for group based access control. Any thoughts on that?
5. (Vinod Eligeti) In which cases one need RBAC kind of access in comparison to XACML way of policies?
6. (Glenn Fink) In what situations is DAC more appropriate than RBAC? If the two coexist must DAC be subordinate to RBAC?
7. (Glenn Fink) Given a hierarchy of roles, can we characterize the cognitive difficulty of assigning, understanding, and using the roles in an RBAC system? Can we compare the level of effort required for RBAC to that required for a similarly capable model using DAC or MAC?
8. (Lee Smith) In the RBAC overview paper, the authors make the argument for RBAC as opposed to DAC by pointing out that RBAC policies are created in compliance with some existing organization specific guidelines derived from existing laws, ethics, etc. Doesn't any access control scheme derive from such existing guidelines? Without some set of guidelines, what is the point of restricting access in the first place?
9. (Glenn Fink) Since RBAC is a policy-based access control mechanism, how can it exist without MAC (or some other labeling system) as a foundation?
10. (Glenn Fink) What does RBAC look like when it is implemented with a "strong discretionary flavor?" How about a MAC-flavored RBAC? Does it have to favor one or the other flavor?
11. (Craig Bergstrom) The paper on role based access controls states that the "act of granting membership and specifying transactions for a role is loosely analogous to the process of clearing users and labeling of objects' [In MAC]. Aside from the fact that there is a hierarchy of roles in mandatory access control based systems, are there any other significant differences, or is RBAC simply a generalization of MAC?
Role/Role Hierarchy

12. (Ranjit Randhawa) Doesn't RBAC sacrifice specificity? I can see a case where users can have more access than intended just because either no role fits them perfectly or they are clumped into a job category whose access is predefined in the framework.

13. (Glenn Fink) Is it possible to assign roles as members of other roles in a circular fashion?

14. (Vinod Eligeti) Are these roles analogues what are called security tokens or access tokens in federated service access?

15. (Muhammad Abu-Saqr) How are Roles different from UNIX’s groups for access control purposes?

16. (Muhammad Abu-Saqr) How should Roles be delegated?

17. (Varun Narayan Pandey) Can we have delegation in RBAC? For e.g. one person has many roles to play and he can delegate each/some of those roles to someone else. One may also need to delegate roles during vacation or absence in the office. How to incorporate it in the models.

18. (Darrell Hyatt) What are some consequences of being de-assigned from an inherited role? Could the ability to do so nullify the administrative advantages of RBAC?

19. (Sean Kugele) It seems dangerous to assume that a Role Hierarchy should mirror an organizational hierarchy. For example, the CEO of a corporation would be at the highest level of an organizational hierarchy, but if the CEO is given permission to act as a network administrator, for instance, this could lead to disaster. In light of this, to what extent should the organizational hierarchy be used as a reference for the building of the Role Hierarchy?

20. (Sean Kugele) The more finely grained roles become the more likely that a given role will only have a single user, which would defeat the purpose of the system; on the other hand, to be consistent with the Principle of Least Privilege, roles should be defined as strictly as possible. How do these two competing design goals affect the implementation of an RBAC mechanism?

21. (Sean Kugele) Something about the use of private roles to limit inheritance in a Role Hierarchy bothers me. The concept is useful for simplifying the administrative tasks, but the result is a potentially large number of roles that are only used for inherited attributes. In turn this results in a Role Hierarchy that seems needlessly complicated. Are the advantages that private roles afford administrators enough to justify their usage?

Separation of Duties/Mutually Exclusive

22. (Ranjit Randhawa) Can users be assigned to more than one role per task? Or does this violate the case of some roles being mutually exclusive?

23. (Glenn Fink) How does RBAC guard against a single user taking on two mutually exclusive roles, one at a time?
24. (Ranjit Randhawa) How is the task where two mutually exclusive roles needed managed? When does one user/role know when the other has accomplished their part of the task?

25. (Haiyan Cheng) In the case that a user can have only one role at any time, does dynamic separation of duty still make sense? Or it just becomes a time constraint on that role user holds.

26. (Darrell Hyatt) In the Consolidated Model, the authors claim that the project supervisor role violates the mutual exclusion rule of test engineer and programmer, but I disagree. If the supervisor is simply a supervisor, his would be an entirely different role that had only read access to test scripts and source code. Otherwise, he could violate a conflict of interest by changing the test scripts to hide deficiencies in the source code. So what would be a better example of this issue?

27. (Vinod Eligeti) Can any one give good example of Static separation of duty and dynamic separation of duty?

28. (Vinod Eligeti) I don’t feel that there should be separation of static and dynamic separation of duty. SSD is done when the user gets some roles and DSD on the done while session is created. But all that the RBAC cares is that there should be no conflicts while issuing the roles. Then why does it matter whether the constraints are imposed before session (in SSD) and after session (in DSD)? One can check always when there is a session since user has to any way creates a session in order to do transactions?

29. (Muhammad Abu-Saqer) What kinds of separation of duties may be useful in the context of administrative roles?

30. (Sean Kugele) To my understanding, Dynamic Separation of Duties (DSD) is meant resolve conflicts of interest on a session by session basis in cases when the roles an individual “statically” has would create a conflict of interest; however, I don’t understand how limiting active roles to one of these at a time would solve the problem. Consider for example the case of an individual who has the roles account manager and purchasing manager. Couldn’t this individual switch to the purchasing manager role and put in an order for a new car and then switch to the account manager role and then clear this purchase? Wouldn’t there need to be some record of historical actions in both roles to make this authorization decision?

31. (Lee Smith) It seems like for dynamic separation of duty policies to be implemented one would need a way of describing relationships between sets of data or transactions. This would necessitate having the ability to enumerate all possible sets of data you could make a relationship with. Is this practical from an access-control perspective?

**RBAC Models**

32. (Ranjit Randhawa) Can a user be involved in more than one task at a time or are there constraints against this?

33. (Ranjit Randhawa) Isn't there a problem with using generalizing user access based on roles/job category instead of user specific?
34. (Ranjit Randhawa) As there is a central administrator who assigns roles can RBAC also be used across different companies or is it usually only intended as an in-house framework?
35. (Haiyan Cheng) In the RBAC3 model, it says “minimum cardinality constraints maybe difficult to implement”. Under what circumstance is the minimum cardinality constraint necessary?
36. (Glenn Fink) RBAC (3) seems very expressive. Are there sets of permissions that cannot be expressed via RBAC (3)?
37. (Muhammad Abu-Saqer) Are negative Permissions useful for RBAC?
38. (Muhammad Abu-Saqer) Should a User be allowed to take on multiple Roles in a single Session and if so, how?
39. (Muhammad Abu-Saqer) Should a User be allowed to take on multiple simultaneous Sessions?
40. (Muhammad Abu-Saqer) Would the proposed NIST standard would be useful if widely adopted by the security industry?

Other Issues

41. (Haiyan Cheng) Referring to the RBAC model paper, the author suggested that a formal notation for stating and enforcing constraints, along with some measure of difficulty of enforcement, should be developed. Is the difficulty of enforcement subjective and organization independent? How can this be generalized?
42. (Haiyan Cheng) Is constraints part of the security policy?
43. (Muhammad Abu-Saqer) What does it means that RBAC is open ended?
44. (Varun Narayan Pandey) How to merge roles when there is a merger of organizations? What are the issues involved in RBAC in systems involving multiple organizations? The papers consider RBAC in the context of only single organization.
45. (Glenn Fink) What is the difference between a constraint and a negative permission?
46. (Glenn Fink) When the paper says that interactions with the system are transactions that are processed via the RBAC policy, does that mean that all interactions are transactions in the same sense as in a database (e.g., atomicity, etc.)?
47. (Glenn Fink) Basic rule #3 states that a subject can execute a transaction only if the transaction is authorized for the subject's _active_ role, but equation (3) specifies that transaction t is an element of TA(RA(s)), the set of authorized roles. So is it the active role, or just any authorized role?
48. (Varun Narayan Pandey) Should temporal dependencies be incorporated in RBAC? For e.g. in VT the authority to insure that I have an acceptable Health Insurance is different than the authority that lets me sign up for classes. I am allowed to sign up for classes before I have purchased an acceptable Health Insurance.
49. (Muhammad Abu-Saqer) In emergency cases where the person in charge of the network administrator are absent RBAC could be lead to bad thing, is there any way to avoid such cases in RBAC?
50. (Lee Smith) Systems such as these definitely have their benefits, but they are fairly intuitive, and the authors even state that they have been in use for some time in various capacities, so what is the benefit of standardizing RBAC? Wouldn't it be better for applications needing this functionality to implement it in exactly the way that they need, with their own particular combination of features rather than propose a standardized RBAC?

51. (Glenn Fink) Is the strength of RBAC in its descriptive power (similar to the power of OOP)? If so, does it share any of the weaknesses of OOP such as inefficiency, etc.?

52. (Glenn Fink) Are there realistic situations where the optimal assignment of RBAC roles, users, permissions and constraints results in a computationally difficult access control system? Is RBAC NP-Complete? If so, is it practical, or just a nice theoretical framework?