(7) Roles Versus Groups

Ravi Sandhu

George Mason University and SETA Corporation
sandhu@isse.gmu.edu

1.0 Discussion

The question of what is different between roles and groups inevitably arises. Attendees at the workshop felt that if this workshop can settle this issue, that alone would represent major progress. Considerable time and energy was devoted at the workshop to discussion on this topic. The outcome of this discussion is summarized here.

Chris Sundt suggested a pragmatic approach which steered the discussion in a productive direction. He argued that groups are an established concept in operating systems with a generally well-understood meaning much like other operating system concepts such as directories. Although groups can be extended to provide the same features as roles, it is better to coin a new term to avoid confusion with the existing concept of a group. Moreover, groups are a useful concept without being extended to roles. What is needed therefore is a consensus definition of groups with respect to which a definition of roles can be developed and compared.

There was consensus that a group is a named collection of users and possibly other groups. A group is usually non-empty, and will typically have at least two members. A users can be directly made a member of a group or indirectly by means of including one group in another. Users are brought together in a group for some access control purpose. Groups serve as a convenient shorthand notation for collections of users and that is the main motivation for introducing them.

In the subsequent discussion two definitions were proposed for a role, as follows.

- A role is a named collection of users and permissions, and possibly other roles.
- A role is a named collection of permissions, and possibly other roles.

Another definition of role as a named collection of responsibilities, and possibly other roles was also proposed. It was decided that this definition was an enterprise-level definition of a role going beyond access control aspects. It was not pursued further in the workshop.

It was agreed that the motivation for roles is convenience in administration and convenience in articulating policy. Also that the name of a role has significance and indicates the purpose of the role. It was recognized that the enterprise-level motivation for roles stems from organizational theory and predates the use of computers. The workshop consistently took an access control viewpoint so it was felt that administrative convenience was the crucial motivation for roles for our purpose.

ACM RBAC Workshop, MD, USA
© 1996 ACM 0-89791-759-6/95/0011 $3.50

At this point there was spirited discussion on the two definitions of roles given above. It was evident that both definitions are present in the literature. Definition 1 has the implication that for a given role it should be easy to enumerate the collection of users and the collection of permissions brought together by the role. Definition 2 has the lesser implication that the permissions comprising a role be easy to enumerate. In contrast the definition of a group has the connotation that the users comprising the group be easy to enumerate.

Definition 2 focuses on the behavior embodied in a role. Permissions enable activity in the system. In terms of abstract operations, a physician role may have the permission to write prescription. Similarly, a manager role have may permissions to hire and fire employees. A role could be viewed as a collection of users (in which case there is no difference between a role and a group). In this view, the emphasis is on the people who occupy a position in an organization. The manager roles consists of all users appointed to the manager position.

In general, definition 1 emphasizes roles as a collection of users and permissions while definition 2 emphasizes roles as collections of permissions. The workshop attendees could not decide which of definition 1 or 2 is the “correct” definition. Perhaps the term role can be used in both ways, but we just need to make clear how it is being used in a given context. Or perhaps we need to agree as a community to use two different terms for these two different concepts of a role. In either case a role is different from a group.