ROLE-BASED ACCESS CONTROL
A Position Statement

Ravi S. Sandhu[*]

ISSE Department, Mail Stop 4A4
George Mason University, Fairfax, VA 22030
sandhu@gmu.edu

Role-based access control (RBAC) is a good match for the security needs of many organizations. An individual's responsibility and authority in an organization derives from his or her job function(s). RBAC assigns privileges and users to roles. New users introduced to a role automatically acquire all privileges of that role. Similarly, new privileges assigned to a role are automatically granted to all members of the role. This is much more convenient and orderly than assigning privileges exclusively to users. There are corresponding advantages to RBAC when users, or privileges, are removed from a role.

The usual grouping mechanism of classical discretionary access control (DAC) can be used to implement roles. I have often been asked, "What is the difference between groups and roles?" The difference is fundamentally that between policy and mechanism. Roles are a policy component. All users in a role are presumed to be competent to carry out their job functions. Role-based authorization relates a job function to the information required to pursue that job activity. It embodies the principles of least privilege, need-to-know, need-to-do, competent-to-know and competent-to-do.

There are many dimensions to RBAC. RBAC can be extremely simple, much like the group mechanisms of typical operating systems in use today. On the other hand it can also be very complex embodying generalization and specialization hierarchies, such as found in object-oriented systems.

One question I wish to pose for the panel is, "What can the security community do to facilitate incorporation of RBAC in products?" The traditional response to this question would be to develop criteria with respect to which products can be evaluated. While evaluation criteria have their uses and benefits, I would urge caution in proceeding too far down this route. Criteria tend to simplify and rank order alternatives. Given the multi-dimensional nature of RBAC I would be reluctant to settle for a small number of linearly ranked RBAC alternatives, unless there is a strong scientific basis for a such a ranking.

My own answer to the question I have posed is twofold. Firstly, we need to continue theoretical analysis of RBAC and its variations. We should try to quantify the comparative expressive power of different versions of RBAC, and understand which policies are facilitated or hindered in these versions. Secondly, there should be experimental implementation of RBAC to better understand which aspects are easy to implement and which are cumbersome and costly. Implementations should, however, build to a rigorous (perhaps, even formal) model rather than the traditional ad hoc approach to construction of access control products.

Some other questions, and my personal responses, to them are given below.

1. Is RBAC just another fad? I do not think so, and hope others share my optimism.
2. How does RBAC relate to type-enforcement? I see RBAC as policy and type-enforcement as one mechanism. Type-enforcement can enforce some aspects of RBAC.
3. Is RBAC a panacea? No.

[*] Ravi Sandhu is an Associate Professor and Associate Chairman of Information and Software Systems Engineering at George Mason University in Fairfax, VA.