A Meta Model for Access Control: Why is it needed and Is it even possible to achieve?

David Ferraiolo
National Institute of Standards and Technology
dferraiolo@nist.gov

Vijay Atluri
Rutgers University
atluri@rutgers.edu

Security policy enforcement is instrumental in preventing the unauthorized disclosure of sensitive data, protecting the integrity of vital data, mitigating the likelihood of fraud, and ultimately enabling the secure sharing of information. In accessing a given resource, policy may dictate, for example that a user has a need-to-know, is appropriately cleared, is competent, has not already performed a different operation on the same resource, the resource was previously accessed by a different user, is incapable of accessing other enterprise resources, or is capable of accessing an object or any copy of the object while performing a specific task. Currently, there exist a rich set of formal security models that can translate organizational policies. A small sample of well documented policies include, flavors of Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), ORCON, Chinese wall, and History-Based Separation of Duty. Enterprise policies that are designed to protect resources are also ad-hoc in nature.

As a major component of any operating system or application, access control mechanisms come in a wide variety of forms, each with their individual method for authentication, access control data constructs for specifying and managing policy, and functions for making access control decisions and enforcement of policies. Of the numerous recognized access control policies, today's OSs rigidly limit enforcement to a small subset of known policies. Policies are also routinely accommodated through the implementation of access control mechanisms within applications. Prominent among these applications are database management systems, but these applications can also include a number of smaller applications such as enterprise calendars, time and attendance, and workflow management. Essentially, any application that requires a user's authentication, typically also affords an independent access control service. Not only do these applications further aggravate identity and privilege management problems, applications can also undermine policy enforcement objectives. For instance, although a file management system may narrowly restrict user access to a specific file, chances are the content of that file can be copied to an attachment or a message and mailed to anyone in the organization, or for that matter, the world.

In consideration of these issues an important question is raised - does a Meta model exist that can serve as a unifying framework for specifying and comprehensively enforcing any access control policy? Some may argue that convergence towards a Meta model is already underway. For example, RBAC, and XACML have been shown effective in their specification and enforcement of access control policies and have been applied in providing interoperable protection.

Is RBAC fundamental to access control and can it eventually be extended and tinkered with to accommodate any policy? RBAC has already been shown to be able to be configured to enforce both DAC and MLS. And, since RBAC was formally proposed in the early and mid 90's a large number of extensions to the RBAC model have been proposed to accommodate a wide variety of policy issues and applications. The question here is - are these extensions getting closer to a Meta model or are we making it up as we go along.

At SACMAT 2005, NIST had proposed an access control framework, referred to as the Policy Machine (PM) that has been shown to accommodate a wide variety of access control policies including DAC, MAC, and RBAC. Since that publication the PM has been refined and to demonstrate its viability in specifying and enforcing a wide variety of attribute-based policies, NIST has developed a reference implementation. However, some have suggested that the basic relations of the PM are similar to that of RBAC and that its other policy appeasing relations and functions could be applied in extending the RBAC model.

In addressing the interoperability problem and the policy flexibility problem the XACML policy specification language has been growing in recognition and its use. Can this approach to access control be adopted or can it evolve as the Meta model? XACML's current focus is on providing access control that is interoperable among applications. As currently specified and applied XACML has does not deal with all types of objects, for example files in an operating system. It is not comprehensive (e.g., It would not prevent the leakage of a sensitive object to an unauthorized principle through copying and past to an email message that could be sent to anyone in the world).

In addition to discussions related to the above technologies, this panel will address two fundament questions. What practical good can the existence of a Meta Model Provide? And, is it even possible for a Meta model to be developed given the large diversity and types of access control policies?

SACMAT'08, June 11–13, 2008, Estes Park, Colorado, USA.
ACM 978-1-60558-129-3/08/06.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access controls*

General Terms

Security