OVERVIEW OF FOUR MAIN ACCESS CONTROL MODELS

Mandatory Access Control or MAC

MAC is a static access control method. Resources are classified using labels. Clearance labels are assigned to users who need to work with resources. For example, some data may have "top secret" or level 1 label. Other information may have a "secret" or level 2 level. Other information may have "free" or level 3 level. So, data can only be accessed by people with certain clearance level. If we don't have sufficient clearance, we can't access that data. For example, if we have clearance level 2, we can access data labeled with "secret" and "free", but we can't access information labeled with "top-secret". If we have clearance level 1, we can access all data.

With MAC method the data owner can't decide which individuals have access to the data. The data owner can only decide what level of clearance is required to see the data and who has which level of clearance. So, this model is not based on identity, it is based on policy or matching of labels.

Discretionary Access Control

When using DAC method, the owner decides who has access to the resource. So decisions are made directly for subjects. To accomplish this we use Access Control Lists (ACL). ACL controls who has access to the resource and the data owner sets the rights or permissions. The permissions identify the actions the subject can perform on the object. Example of DAC method is NTFS permissions on Windows operating systems. On NTFS file system each file and folder has an owner. The owner can use ACL and decide which users or group

of users have access to the file or folder. In fact, may operating systems use DAC method to limit access to resources.

Role Based Access Control

When using role-based access control method data access is determined by the role within the organization. It is not determined for individual users. This is a hybrid between MAC and DAC. The role can be a job position, group membership, or security access level. Users are members of some role and that gives them access to certain resources in the organization.

Rule Based Access Control

Rule-based access control is based on rules to deny or allow access to resources. If the rule is matched we will be denied or allowed access. The best example of usage is on the routers and their access control lists. With router ACLs we determine which IPs or port numbers are allowed through the router, and this is done using rules. In this method there are no user accounts, group membership or security labels. In some situations this method can be considered as a form of MAC, because we are either allowed or denied access, and that's it (it does not consider identity).

Source : http://www.utilizewindows.com/security/users/356-overview-of-four-main-access-control-models