## Access control models

One of the ways to defend against attacks is to prevent them by providing rigorous means of determining who has access to various pieces of information. All of the models assume that there are data managers, data owners, or system administrators who are defining the access control specifications. The access shall be restricted to those who have a need to access and/or modify the information in question. That is, they should apply the principle of least privilege.

Access Control Matrices (ACM)

It is a table that defines permissions. Each row of this table is associated with a subject, which is a user, group, or system that can perform actions. Each column of the table is associated with an object which is a file, directory, document, device, resource, or any other entity for which we want to define access rights. Each cell of the table is filled with the access rights for the associated combination of subject and object. Access rights can include actions such as reading, writing, copying, executing, deleting. An empty cell means that no access rights are granted.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | /etc/passwd | /usr/bin/ | /u/Roberto/ | /admin/ |
| Root | Read, write | Read, write, exec | Read, write, exec | Read, write, exec |
| Mike | Read | Read, exec |  |  |
| Roberto | Read | Read, exec | Read, write, exec |  |
| Backup | read | Read, exec | Read, exec | Read, exec |

Access Control Lists (ACL)

These are columns of ACM arranged as lists, showing for each object who (subject) has what access the object.

Capability Lists (CL)

These are rows of ACM showing for each subject what objects and in what mode are allowed for him/her

Role-Based Access Control (RBAC)

Administrators define roles, specify access control rights for them, and then assign roles to subjects/roles. Roles can be arranged hierarchically representing organization structure.

Mandatory Access Control (MAC), Bell – La Padula model (BLP)

BLP model is derived from the military multilevel security paradigm (Top secret, Secret, Confidential, Unclassified)

Each document has 1 out of 4 security levels, and each user has “clearance”, also 1 out of 4.

A document of a certain level can be accessed only by users with the same or higher clearance level, “no read-up” rule.

A user can write only in the documents of his or higher level of security, “no write down” rule, ‘\*’ property.