

Comparison of ACL Based Security Models for securing resources for Windows operating system

Author: Prof. S. A. Ubale¹; Dr. S.S. Apte²

Affiliation: SKN Sinhgad College of Engineering, Korti, Pandharpur¹; WIT College of Engineering, Solapur²

ABSTRACT

In this paper ACL based security model for securing resources and data for windows operating system are compared on criteria such as security, flexibility etc.

Keywords

MAC, DAC, RBAC, ACL, resource security

1. INTRODUCTION

Now a day people use different types of resources for different purposes, may be for any company, for personal reason, for any organization or for social reason. But also now a day there are increasing number of hackers, they want to steal or misuse data or resources of others. So that it is needed to make sure that only people which are permitted to access resource or data can access that resources. Resource it may be physical, informational or personnel. In this paper ACL based models are compared for securing resources and data for windows operating system.

2. ACL BASED MODEL

Basically people just rely on username- password for security but access control is more than just relying on it. There are many models and techniques that can be implemented here. Access controls exist to keep the bad guys out and to keep the good guys honest. What is needed here is not to allow un authorized access and proper access to authorized users so that authorized users also may not do anything that breach security.

Access control models are created to enforce the rules and objectives of an established security policy and to dictate how subjects can access objects. Access control, one can say it as an ambiguous term. For someone it can be just treated as controlling login with the help of password or biometrics etc. But access control is not only referred to as authentication, access control originally refers to the control over access to system resources and data. Also after user enters account credentials and gets authenticated and access to system

granted, might only be permitted access to certain file after logging into system, while simultaneously being denied access to all other resources.

There are three models that will be covered in this section: discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC).

3. MANDATORY ACCESS CONTROL

Where security is of most important such as in Government or military appliance Mandatory Access control model is used. Security labels are the core decision-making component in MAC environments; they are assigned by system administrators or security officers and should be changed only in a well-defined manner so the security policy is supported and enforced.

Mandatory Access Control (MAC) is the strictest model in all ACL base models. But this model is not used widely. MAC takes a hierarchical approach to controlling access to resources. In case of this model access to resources is defined by system administrator. It is not possible for users to change access control for any resource.

In case of Mandatory access control there are security labels associated with every resource object on the system. Security labels consist of two main information as classification (top secret, confidential etc) and category (for which the object is available).

It is important to note that both the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object. Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects. When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the

object's security label. If the user's credentials match the MAC security label properties of the object access is allowed.

For implementation of the MAC model it is required to have well planned management of the system. It also imposes high management overhead for updating account label, new users and changes in the organization and system. But MAC is the so far most secure access control model.

4. DISCRETIONARY ACCESS CONTROL

Unlike mandatory access control, discretionary access control allows each user to control access to their own data. DAC is generally default access control model for operating system. As in case of Mac it works with security labels but in DAC model Access Control List (ACL) is associated with object. An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group. For example, User A may provide read-only access on one of her files to User B, read and write access on the same file to User C and full control to any user belonging to Group I.

Here important thing to note is that User A cannot change the access control for the file owned by User B but User B can set access for the file owned by User B.

Discretionary Access Control provides a much more flexible environment than Mandatory Access Control but also increases the risk that data will be made accessible to users that should not necessarily be given access.

5. ROLE BASED ACCESS CONTROL

As earlier covered discretionary access control, role based access control is nothing but non-discretionary access control. Until now in MAC security labels are used in DAC Access control list is used, but this approach is going to be more realistic approach for structuring access control. Access under RBAC is based on a user's job function within the organization to which the computer system belongs. It works on rights and permission assigned to group or role and not to the individual user. In this model also administrator is going to create roles any group according to their specifications and administrator is going to assign the permissions not to the user but to the role or group.

The user that is placed into a role or group inherits the permissions and access rights from the role, thus is implicitly assigned access rights. This model is very useful and flexible for large organization. Because here it allows just to put new users or employees to the role instead of creating and assigning new permission to each user. It simplifies task very effectively. Comparison of these three models is summarized as

Table1. Comparison of ACL Based Models

| ACL Based Model | Resource Access | Security | Flexibility | Approach followed |
|-----------------|----------------------------|-------------|-------------|-------------------|
| MAC | Centrally by Administrator | Most Secure | Better | Security Label |
| DAC | Based on user | Secure | Good | ACL |
| RBAC | Based on Role | Secure | Best | Role Based |

DAC, MAC, and RBAC controls can be used together in combination within different environments to support and implement the organization's security policy.

6. REFERENCES

- [1] Myong H. Kang, Joon S. Park, Judith N. Froscher, "Access Control Mechanisms for Inter-Organizational Workflow", SACMAT'01, May 3-4, 2001, Chantilly, Virginia, USA pp 66-74. ACM 1-58113-350-2/01/0005.
- [2] D. Ferraiolo, G.-J. Ahn, and S. Gavrila. The role control center: Features and case studies. In Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, June 2003.
- [3] M. Bishop. Computer Security: Art and Science. Addison-Wesley Publishing Company, Boston, Massachusetts, 2004.
- [4] Sandhu. The next generation of access control models: Do we need them and what should they be? In SACMAT'01, page 53. SACMAT, May 2001.