Week 3 Assignment: Access Control Models

Shaun Hoadley

CYB 300: System Administration and Security

Carl Marquez

September 13, 2021

**Discuss the difference between the following access control modules: Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC)**

Of the three access control models listed above, the most strict and secure level of control is mandatory access control (MAC). According to Smyth, MAC takes a hierarchical approach and architecture in controlling access to a system’s resources (2016). The rules used to determine the type of content a user has access to are created by an appointed system administrator. Users that do not have the approprieate credentials are not able to change the present resources access controls. All of the resources in the system are assigned security labels when using mandatory access control. The security labels contain two pieces of information about the resources: Category and Classification. Likewise, users are assigned category and classification tags that must match the security labels for the data they wish to access.

Discretionary access control (DAC) gives the owner of the software or data the ability to provide access to others at their discretion. This is done using an access control list (ACL) where the owner can add users and groups that is allowed access to the file(s). DAC is most commonly used in many everyday desktop operating system environments.

According to Bierman and Bjorklund, role-based access control (RBAC) is used to assign permissions to users based on their role, job, or title so that they may only access resources which pertain to them (2018). Many feel that a role-based access control is the best way for an organization to regulate their access control permissions.

**Describe when one would be used over the other.**

For different situations, one would use different access control methods. As I stated previously, DAC might be used on personal computers that may be shared by multiple users (i.e. a family PC). An organization might find it best to use RBAC to assign permissions for its people based on what they do for the organization. An organization may decide that MAC is preferred, though it costs additional work for system administrators, to assign permissions on a per user basis, rather than by their role.

**Discuss how information technology (IT) such as assigning new users security levels can manage data.**

Data can be managed this way by giving users access to only what they need instead of offering up all the resources of a system. By doing so, reduces the risk of data mismanagement, leaks, and limit the possibilities of introducing malicious software that might affect the entire system. System administrators can, thereby, efficiently govern the systems for which they are responsible through the assignment of permissions and access controls.

**Outline how you would explain to a junior system administrator which access control should be used for a given situation.**

What this means, according to Martin, organizations that need the highest levels of security (military, law enforcement, etc.), should be utilizing mandatory access controls (2019). Discretionary access controls should be used in individual desktop environments where the users are responsible for who can see what. For most other organiztions, the best option is likely to be role-based access controls.

**References**

Bierman, A., & Bjorklund, M. (2018). *Network Configuration Access Control Model*. STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018,< https://www. rfc-editor. org/info/rfc8341.

Martin, J. (2019). *What is access control? A key component of data security*. CSO Online. Retrieved from <https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html>.

Smyth, N. (2016). *Mandatory, Discretionary, Role and Rule Based Access Control*. Techotopia.com. Retrieved from <https://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control>.