Topic 2 Discussion 2

The textbook defines different types of access control: MAC, DAC, RBAC, and Lattice. Research either rule-based or discretionary-based access control. Compare and contrast your chosen access control to those provided by the textbook. Provide an example of how each should be deployed, and include an explanation of what makes each unique in comparison to the other.

Hello Class,

Comparison between Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

Mandatory Access Control (MAC):

Definition: Mandatory Access Control restricts access based on security labels assigned to resources and users.

Deployment Example: In a MAC system, access to files is determined by security levels such as "Top Secret," "Secret," and "Confidential." For instance, only users with a security clearance of "Top Secret" can access files labeled as such.

Unique Features:

Centralized Control: Access control is centrally managed by system administrators or security officers.

Hierarchical Security Levels: Users cannot change access permissions since they are based on security classifications.

Discretionary Access Control (DAC):

Definition: Discretionary Access Control allows users to control access to their own resources based on their discretion.

Deployment Example: In a DAC system, users can set access permissions on files they own, determining who can read, write, or execute them. For example, a user can decide to share a document only with specific colleagues.

Unique Features:

User-Centric: Users have the authority to grant or revoke access to their resources.

Decentralized Management: Access control decisions are made by resource owners rather than a central authority.

Comparison:

MAC vs. DAC:

Control Mechanism:

MAC: Access control is based on security labels and predefined rules set by administrators.

DAC: Users have control over access permissions to resources they own.

Flexibility:

MAC: Limited flexibility as access is strictly governed by system-wide policies.

DAC: Offers more flexibility as users can manage access based on their preferences.

Granularity:

MAC: Provides high-level security with strict control over access based on security classifications.

DAC: Offers finer granularity as users can set specific permissions for individual resources.

Both MAC and DAC play crucial roles in access control, with MAC focusing on enforcing strict security policies and DAC providing more user autonomy. The choice between these models depends on the security requirements and organizational structure of a system.

References:

Avigilon. (n.d.). Discretionary, Mandatory, Role and Rule Based Access Control. https://www.avigilon.com/blog/access-control-models#:~:text=Rule%2Dbased %20access%20control%20is

McMillan, T. (2020). CompTIA cybersecurity analyst (CySA+) CS0-002 certification guide (2nd ed.). Pearson. ISBN-13: 978-0136747161