The types and functions of Access Control Methods

Posted on May 25, 2018

Mandatory access control refers to an access control method through which operating systems coerce the user's ability to perform and access operations on a target or object. It includes a set of security procedures that are subjected to system authentication, classification, and configuration.

Role-based access control is involved in computer security to regulate access to network resources by limiting the access to responsibilities of the personal user in the company. Based on RBAC, access refers to the capabilities of a particular resource object to effectively conduct an assigned task (Zhang et al. 2005).

Discretionary access control includes the mode of barring access to the target by the subject identity and the group they belong to. This method grants or restricts access based on access policies instilled by the owner group.

Starting with mandatory access control it has high security requirements compared to the other two access control systems, and the security requirements of availability are endorsed with higher standards than the others. Compared to security requirements, Role-based access controls instill integrity more than the other access control methods. In decision making, arguments are used in making DAC decisions. On the other hand, RBAC decisions are centered on functions while MAC is grounded on cataloging and authorizations (Sandhu et al. 1996, p. 45). MAC requires a lot of resources for it to be effectively and successfully put into action. Also, after installation, this access control system requires sensitive administration and regular updates to cover new clients and redesign existing control measures for the efficacy of the users. A mandatory access control system offers the best measures in ensuring resource security since the users and all user authorizations cannot alter the access controls determined by the system administrator.

Mitigation of Negative Factors

To mitigate the negative factors of mandatory access control, the organization can consider using it with other models. On the other hand, the negative factors of discretionary access control can be controlled by considering the utilization of reactive access controls. Lastly, role-based access control methods effectively reduce their implicit factors by giving users options and letting them decide which fits them in the current environment.

Evaluation of the Use of Access Control Methods

Mandatory access control is utilized to provide high-level security requirements. It includes the construction of dominance in which security levels are set and requirements outlined (Nyanchama and Osborn, 1996, p. 144). A user who is not classified under a certain security level cannot access data from that level. This is primarily done in military systems which have sensitive and classified information. This type of access control includes using security labels subjected to the resources and data available in the system that it regulates. Mandatory access control system offers the most secure platform for regulating and controlling security levels. It effectively implements high system requirements outlined by the owner group by managing and executing all security properties required in every security level classification. In commercial utilization, MAC is used in web servers to create policies.

Role-based access control targets databases, such as invoicing and customer services. This is achieved by allocating authorization to specific functions in the organization. Afterward, user groups are attached to those specific functions. For instance, in the company finance department, an accountant will be attached to an accounting role and hence gain access to the accounting system and thus have the ability to access all necessary data and resources needed to execute the accounting role successfully. This method ensures that specific users have specific roles attached to them. Therefore, every user accesses the authorized resources to fulfill the capacity of the work he/she is assigned to. By this users have the freedom to flow information and the integrity of the resources provided is highly considered by this type of access method. Also, it allows role differentiation in users that belong to the same group of roles but have different responsibilities and capacities, for example, the chief accountant and an accountant. RBAC allows user groups to have permissions not above or below their specified roles.

Discretionary access control allows users to manage content that they own. A good example is social media networks where system administrators allow users to have accounts in which they regulate the contents inside them. The users are given the ability of a system administrator in MAC by which the user gives or changes the authorization. In DAC each user has an access control list attributed to them and it allows the resource object to grant access to a user group under its own terms hence providing more flexibility than MAC and RBAC.

The best method for the organization would be Role-Based access control since it gives the staff the flexibility to access resources depending on their roles.

The challenges associated with RBAC would be making managers accountable for their subordinate staff, effective staff and communication, role definition and information confidentiality, and a long hierarchy. Top management should adopt the strategy of training the overall staff about the requirements of the access system and what is expected of every personnel in the workforce.

References

Nyanchama, M., & Osborn, S. (1996). Modeling mandatory access control in role-based security systems. In *Database Security IX* (pp. 129-144). Springer, Boston, MA.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47.

Zhang, N., Ryan, M., & Guelev, D. P. (2005, September). Evaluating access control policies through model checking. In *International Conference on Information Security* (pp. 446-460). Springer, Berlin, Heidelberg.