Mitch Meyer

9/28/15

Assignment 7.3 – Access Control Models

Access control is the process of authenticating and authorizing users to grant access to computer resources. To simplify the process of monitoring, authenticating, and authorizing users, there have been five access control models that have been developed. These various frameworks are embedded in the software and hardware of information systems and simplify the process of deploying access controls. Each model has its strengths, weaknesses, and most appropriate situations in which to be deployed. The five models of access control are discretionary access control, mandatory access control, role-based access control, rule-based access control, and task based access control.

Discretionary access control is the least restrictive of the control models. In this model, every object has an owner who has total control over that object. These owners can create and access their objects freely and can also grant permissions to other users to access their owned objects. DAC is used in operating systems such as most types of UNIX and Microsoft Windows. This model has significant weaknesses since it is up to the end user to determine the proper level of permissions to other users. This access control model would be well suited to be used in a home network or a very small business. This model provides a lot of freedom to users to share documents with other users and to control how much access other uses have to their created files. It also is built into Windows in most cases and wouldn’t be a burden to set up for a casual user. This access model, on the other hand, would be a terrible choice for controlling access to very sensitive information, such as at a nuclear facility. The ease of granting access to documents to another user makes this model very flexible, but if a user grants permissions in error, that could be a huge security breach and could create vulnerabilities to outside attacks.

Mandatory access control is the most restrictive access control model. In the MAC model, users are assigned access controls in accordance to administrator policies. The user has no freedom to set any controls in this model. Mandatory access control makes use of labels and levels to determine who can have access to what resources. Each item is considered an object and is assigned a classification label relative to the importance of that object. Each subject, or user is granted a level that grants access to objects that share the same classification label. An optimal use of this model for access control would be to limit and restrict access at a military facility. If you wanted to protect data pertinent to national security, strictly limiting who has access to that data through the MAC model would be the best choice because only users would only have access to objects that they have been cleared for. On the other hand, in a home setting, the MAC model may be more of a hindrance than a help. If the goal is to provide all members of a house hold access to digital movies and music files, this model would probably become cumbersome quickly.

The role based access control is a model that creates permission groups based on the role a user must perform. This access control determines what permissions are necessary for each role to be able to perform the proscribed job duties and users are assigned permissions according to their role within the organization. This model would be very useful in most business settings. It would be easy to implement and would limit access to resources to the users who require it. I could see this being deployed in a bank situation, where tellers would have a more limited set of permissions from say the bank manager. The bank manager would have fewer available permissions from the loan officers, and the load officers would have fewer permissions than the bank president. This staggering of permissions to specific roles allows each user to perform their duties and prevents them from accessing data not pertinent to their specific role. This protects sensitive data and creates a hierarchy of authority in case a situation arises where additional permissions are necessary. In this case, a teller could ask a bank manager to approve a large withdrawal. A situation where this method would not be optimal would be where there are limited or undefined roles. In a small business situation where there are one to two people working in the business, controlling access to information systems with a role based model would silly and cumbersome. It doesn’t make sense to outline permissions for specific roles in an organization that has one role.

Rule based access control is similar to role based access control, but each object has a specific set of access properties associated with it based on a list of rules created by the system administrator. When a user attempts to access an object, the system checks the rules contained in the object to determine if access is permissible. Rule based control is typically used to control access between one or more systems. An optimal use of this control model would be in the case of managing a network of multiple systems. For instance, at my place of employment, users have access to an intranet containing employee information, payroll, and scheduling information. Users also have access to production software and virtual machines use for tracking customer transports. These various systems are all controlled using a set of rules for managing user names and passwords. The administrators control the user names and mandate password changes every 90 days. This grants the system administrators and users greater access to resources with fewer moving parts to monitor. The least optimal use of this model would be in managing a small network with limited resources. It doesn’t make much sense to spell out the rules of a system that to control access when using another model would essentially accomplish the same task with fewer steps.

The final model is the task based model. The task based model assigns permissions to users based on tasks assigned to the user to be performed. These permissions can be limited based on the time allotted to complete an assigned task. Permission can also be granted as portions of a task are completed. This model also accounts for users who are assigned multiple tasks and watches for potential security conflicts based on the tasks assigned. This model deploys dynamic monitoring when a user enters into permission states that could compromise security policies and can actively deny a user’s request to compromise security policy with granted permissions. Meaning, this model could determine when a user has access to sales data and web publishing platforms at the same time and would allow the user to copy the sales data, but would prevent them from pasting that data to the web. This model is quite different from the others and I think it would be optimally used for large businesses, military, and governmental organizations. Deploying this model would require a large amount of resources to monitor and assign tasks appropriately. It would be incredibly secure and would not limit the users’ abilities to complete their assigned tasks. On the other hand, the cost of deploying this model would have to be enormous due to the complex nature it’s dynamic monitoring. and so small to medium sized organizations would be prevented from using this model.

In conclusion, each model is suited to control access to system resources, and each model has a place where it would be best suited for use. The models that seem most powerful are the mandatory access control and the task based access control. The amount of control over system resources these models grant the system administrator is impressive. The most pragmatic models seem to be the role based and rule based models. These seem to have the most practical applications and make sense for use in most business settings.