Access Control: Models and Methods

resources.infosecinstitute.com/access-control-models-and-methods/

There are times when people need access to information, such as documents, slides, etc., on a network drive but don't have the appropriate level of access to read and/or modify the item. This can happen at the most inconvenient time and they would need to get a hold of a system administrator to grant them the appropriate level of privileges. Of course, they end up asking why they can't just have overall access to the information in a folder so they can sort through the items and find what they need. The answer could be along the lines of, "Sorry, but you need to submit a ticket to the help desk with the appropriate information filled out which will go through a vetting process before we can grant you the appropriate access." This leads to more frustration with the individual potentially saying something like, "Is there a faster way to do this? I just need access to one folder, that's it." So now what? As painful as it may seem (and inconvenient at times), there are reasons why access control comes into play for a scenario like this especially in the age of cyberspace. In this discussion, I will define access control and talk about the four access control models. I will also describe the methods of logical access control and explain the different types of physical access control.

Access Control and Access Control Models

Access control is basically identifying a person doing a specific job, authenticating them by looking at their identification, then giving that person only the key to the door or computer that they need access to and nothing more. In the world of information security, one would look at this as granting an individual permission to get onto a network via a user-name and password, allowing them access to files, computers, or other hardware or software the person requires, and ensuring they have the right level of permission (i.e. read only) to do their job. So, how does one grant the right level of permission to an individual so that they can perform their duties? This is where access control models come into the picture.

Access control models have four flavors: Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Rule Based Access Control (RBAC or RB-RBAC). Let's look at each of these and what they entail.

The Mandatory Access Control, or MAC, model gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone. Now, there are two security models associated with MAC: Biba and Bell-LaPadula. The Biba model is focused on the integrity of information, whereas the Bell-LaPadula model is focused on the confidentiality of information. Biba is a setup where a user with low level clearance can read higher level information (called "read up") and a user with high level clearance can write for lower levels of clearance (called "write down"). The Biba model is typically utilized in businesses where employees at lower levels can read higher level information and executives can write to inform the lower level employees.

Bell-LaPadula, on the other hand, is a setup where a user at a higher level (i.e. Top Secret) can only write at that level and no lower (called "write up"), but can also read at lower levels (called "read down"). Bell-LaPadula was developed for governmental and/or military purposes where if one does not have the correct clearance level and does not need to know certain information, they have no business with the information. At one time, MAC was associated with a numbering system which would assign a level number to files and level numbers to employees. This system made it so that if a file (i.e. myfile.ppt) had is level 400, another file (i.e. yourfile.docx) is level 600 and the employee had a level of 500, the employee would not be able to access "yourfile.docx" due to the higher level (600) associated with the file. MAC is the highest access control there is and is utilized in military and/or government settings utilizing the classifications of Classified, Secret, and Unclassified in place of the numbering system previously mentioned.

The Role Based Access Control, or RBAC, model provides access control based on the position an individual fills in an organization. So, instead of assigning John permissions as a security manager, the position of security manager already has permissions assigned to it. In essence, John would just need access to the security manager profile. RBAC makes life easier for the system administrator of the organization. The big issue with this access control model is that if John requires access to other files, there has to be another way to do it since the roles are only associated with the position; otherwise, security managers from other organizations could possibly get access to files they are unauthorized for.

The Discretionary Access Control, or DAC, model is the least restrictive model compared to the most restrictive MAC model. DAC allows an individual complete control over any objects they own along with the programs associated with those objects. This gives DAC two major weaknesses. First, it gives the end user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to. Secondly, and worse, the permissions that the end user has are inherited into other programs they execute. This means the end user can execute malware without knowing it and the malware could take advantage of the potentially high level privileges the end user possesses.

The fourth and final access control model is Rule Based Access Control, also with the acronym RBAC or RB-RBAC. Rule Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator. For example, if someone is only allowed access to files during certain hours of the day, Rule Based Access Control would be the tool of choice. The additional "rules" of Rule Based Access Control requiring implementation may need to be "programmed" into the network by the custodian or system administrator in the form of code versus "checking the box."

Now that I have covered access control and its models, let me tell you how they are logically implemented.

Logical access control methods

Logical access control is done via access control lists (ACLs), group policies, passwords, and account restrictions. We will take a look at each of these to see how they provide controlled access to resources.

Access Control Lists (ACLs) are permissions attached to an object (i.e. spreadsheet file) that a system will check to allow or deny control to that object. These permissions range from full control to read-only to "access denied." When it comes to the various operating systems (i.e. Windows®, Linux, Mac OS X®), the entries in the ACLs are named "access control entry," or ACE, and are configured via four pieces of information: a security identifier (SID), an access mask, a flag for operations that can be performed on the object, and another set of flags to determine inherited permissions of the object. So, as one can see, ACLs provide detailed access control for objects. However, they can become cumbersome when changes occur frequently and one needs to manage many objects.

Group policies are part of the Windows® environment and allow for centralized management of access control to a network of computers utilizing the directory services of Microsoft called Active Directory. This eliminates the need to go to each computer and configure access control. These settings are stored in Group Policy Objects (GPOs) which make it convenient for the system administrator to be able to configure settings. Although convenient, a determined hacker can get around these group policies and make life miserable for the system administrator or custodian.

Passwords are "the most common logical access control…sometimes referred to as a logical token" (Ciampa, 2009). However, that being said, they need to be tough to hack in order to provide an essential level of access control. If one makes the password easy to guess or uses a word in the dictionary, they can be subject to brute force attacks, dictionary attacks, or other attacks using rainbow tables. Keeping this in mind, experts agree that the longer the password is, the harder it is to crack, provided the user remembers it and used many different characters and non-keyboard type characters in creating it. Utilizing this concept also makes it more difficult for a hacker to crack the password with the use of rainbow tables. Having a two-factor authentication (i.e. Smart card with password) can make things more secure, especially with technology advancing to the point where cracking passwords can take only seconds as pointed out in this article: http://cyberarms.wordpress.com/2010/10/21/cracking-14-character-complex-passwords-in-5-seconds/.

In addition, ensuring patches are accomplished regularly, deleting or disabling unnecessary accounts, making the BIOS password-protected, ensuring the computer only boots from the hard drive, and keeping your door locked with your computer behind it will help ensure your passwords are protected.

Of course, not writing down the password will help, too.

Account restrictions are the last logical access control method in the list. Ciampa points out, “The two most common account restrictions are time of day restrictions and account expiration” (Ciampa, 2009). Time of day restrictions can ensure that a user has access to certain records only during certain hours. This would make it so that administrators could update records at night without interference from other users. Account expirations are needed to ensure unused accounts are no longer available so hackers cannot possibly utilize them for any “dirty work.”

Types of physical access control

Physical access control is utilizing physical barriers which can help prevent unauthorized users from accessing systems. It also allows authorized users to access systems keeping physical security in mind. This type of control include keeping the computer secure by securing the door which provides access to the system; using a paper access log; performing video surveillance with closed circuit television; and in extreme situations, having “mantraps.”

Securing the computer consists of disabling hardware so that if a bad guy were to gain access, they can’t do any damage to the computer due to disabled USB ports, CD or DVD drives, or even a password protected BIOS. Again, this just reduces the risk of malicious code being loaded onto the system and possibly spreading to other parts of a network.

Door security can be very basic or it can utilize electronic devices such as keyed dead-bolt locks on the door, cipher locks, or physical tokens. A keyed dead-bolt lock is the same as one would use for a house lock. The cipher lock only allows access if one knows the code to unlock the door. Physical tokens will typically consist of an ID badge which can either be swiped for access, or they may instead contain a radio frequency identification tag (RFID) that contains information on it identifying the individual needing access to the door.

Paper access logs are common in many places for physical security. This allows a company to log a person in with name, company, phone number, time in, and time out. It can also document the employee who escorted the person during the time they were there. Paper access logs, filled out accurately, will complement video surveillance.

Video surveillance on closed circuit television allows for the recording of people who pass through a security checkpoint. This type of door security allows one to observe the individuals going through the checkpoint, as well as the date and time, which can be useful when trying to catch bad guys. Video surveillance can also be utilized in mantraps which is what I will discuss next.

Mantraps take door security to another level. This type of security can be seen in military and government settings, among others, when entering very high security areas. A person will present their identification to the security attendant and the attendant will allow the person to enter the first door into a room. Only if the individual’s identification credentials are valid will they be allowed to pass through the room and go through the second door; if not, mantrap! They can only get out of the room by going back through the first door they came in.

1. Conclusion

In summary, I presented a definition of access control and discussed the four access control models. Additionally, I described the logical access control methods and explained the different types of physical access control. To conclude, no access control model or method is perfect; however, if one does something to deter an attacker, they can count that as a success in information security practice.

1. References

Ciampa, Mark. (2009). Security+ Guide to Network Security Fundamentals Third Edition. Boston, MA.