Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

WESTERN GOVERNORS UNIVERSITY

ONLINE. ACCELERATED. AFFORDABLE. ACCREDITED.

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Authorization

- After a user is identified then authenticated the next step is authorization.
- Authorization is what the user can access, modify, and delete.
- Principle of least privilege is the lowest level of authorization allowed to a user to perform duties.
- Violation of the principle of least privilege is a user having more access than necessary to perform duties assigned. This can allow user and bad actors to cause damage to the production data.

Access Control

- We have four basics tasks we might want to carry out: allowing access, denying access, limiting access, and revoking access.
- Allowing: lets us give a particular party, or parties, access to a given resource.
- Denying: is simply the opposite of granting access.
- Limiting: refers to allowing some access to our resource, but only up to a certain point. Sandbox used to describe the limitations that are put in place. A sandbox is simply a set of resources devoted to a program, process, or similar entity, outside of which the entity cannot operate.
- Revoking: takes access that was once allowed away from the user example termination of a user.

Access Control Lists

- Access control lists (ACLs), often referred to as "ackles," are a very common choice of access control implementation. ACLs are usually used to control access in the file systems on which our operating systems run and to control the flow of traffic in the networks to which our systems are attached. ACLs are most commonly discussed in the context of firewalls and routers.
- When we look at the ACLs in most file systems, we commonly see three permissions in use: read, write, and execute.
- Read: allowing us to access the contents of a file or directory
- Write: write to a file or directory
- Execute: execute the contents of the file.

Network ACLs

- Network ACLs: When we look at the variety of activities that take place on networks, both private and public, we can again see ACLs regulating such activity. In the case of network ACLs, we typically see access controlled by the identifiers we use for network transactions, such as Internet protocol (IP) addresses, Media Access Control (MAC) addresses, and ports.
- Permissions in network ACLs tend to be binary in nature, generally consisting of allow and deny. When we set up the ACL, we use our chosen identifier or identifiers to dictate which traffic we are referring to and simply state whether the traffic is to be allowed or not.

Capabilities

- Capability-based security can provide us with an alternate solution to access control that uses a different structure than what we see in ACLs. Where ACLs define the permissions based on a given resource, an identity, and a set of permissions, all generally held in a file of some sort; capabilities are oriented around the use of a token that controls our access.
- We have one door, and many people have a token that will open it, but we can have differing levels of access. Where one person might be able to access the building only during business hours on weekdays, another person may have permission to enter the building at any time of day on any day of the week.

Confused deputy problem

- Confused deputy problem is a type of attack that is common in systems that use ACLs rather than capabilities. The crux of the confused deputy problem is seen when the software with access to a resource has a greater level of permission to access the resource than the user who is controlling the software. If we, as the user, can trick the software into misusing its greater level of authority, we can potentially carry out an attack.
- These often involve tricking the user into taking some action when they really think they are doing something else entirely. Two of the more common uses of such an attack are client-side attacks such as cross-site request forgery (CSRF) and clickjacking.

Confused deputy problem continued

- CSRF is an attack that misuses the authority of the browser on the user's computer. If the attacker knows of, or can guess, a Web site to which the user might already be authenticated, perhaps a very common site such as Amazon.com, they can attempt to carry out a CSRF attack. They can do this by embedding a link in a Web page or HTML-based e-mail, generally a link to an image from the site to which he wishes to direct the user without their knowledge. When the application attempts to retrieve the image in the link, it also executes the additional commands the attacker has embedded in it.
- Clickjacking, also known as user interface redressing, is a particularly sneaky and effective client-side attack that takes advantage of some of the page rendering features that are available in newer Web browsers. In order to carry out a clickjacking attack, the attacker must legitimately control or have taken control of some portion of the Web site (without the owners of the site being aware their site is now serving malware) that is to be used as the attack vehicle. The attacker constructs or modifies the site in order to place an invisible layer over something the client would normally click on, in order to cause the client to execute a command differing from what they actually think they are performing.

Access Control Models

- Access controls are the means by which we implement authorization and deny or allow access to parties, based on what resources we have determined they should be allowed access to.
- There are 5 different models that will be discussed.
- Discretionary access control
- Mandatory access control
- Rule-based access control
- Role-based access control
- Attribute-based access control.

Access Control Models

- Discretionary access control: (DAC) is a model of access control based on access being determined by the owner of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have. In Microsoft operating systems, we can see DAC implemented. If we decide to create a network share, for instance, we get to decide who we want to allow access.
- Mandatory access control: (MAC) is a model of access control in which the owner of the resource does not get to decide who gets to access it, but instead access is decided by a group or individual who has the authority to set access on resources. We can often find MAC implemented in government organizations, where access to a given resource is largely dictated by the sensitivity label applied to it (secret, top secret, etc.), by the level of sensitive information the individual is allowed to access (perhaps only secret), and by whether the individual actually has a need to access the resource, as we discussed when we talked about the principle of least privilege earlier in this lesson.
- Rule –based access control: (RuBAC) is a model that is based off allowing or denying based of a set of predetermined rules. Example Firewalls and Routers.
- Role-based access control: (RBAC) is a model of access control that, similar to MAC, functions on access controls set by an authority responsible for doing so, rather than by the owner of the resource. The difference between RBAC and MAC is that access control in RBAC is based on the role the individual being granted access is performing.
- Attribute-based access control: (ABAC) is, logically, based on attributes. These can be the attributes of a particular person, of a resource, or of an environment. Subject attributes are those of a particular individual. We could choose any number of attributes, such as the classic "you must be this tall to ride" access control, which exists to prevent the altitudinally challenged from riding on amusement park rides that might be harmful to them.

Multilevel access control

- Multilevel access control models are used where the simpler access control models that we just discussed are considered to not be robust enough to protect the information to which we are controlling access. Such access controls are used extensively by military and government organizations, or those that often handle data of a very sensitive nature. We might see multilevel security models used to protect a variety of data, from nuclear secrets to protected health information (PHI).
- The Bell–LaPadula model
- The Biba model
- The Brewer and Nash model

The Bell–LaPadula model

- The Bell–LaPadula model implements a combination of DAC and MAC and is primarily concerned with the confidentiality of the resource in question. Generally, in cases where we see DAC and MAC implemented together, MAC takes precedence over DAC, and DAC works within the accesses allowed by the MAC permissions.
- The simple security property: The level of access granted to an individual must be at least as high as the classification of the resource in order for the individual to be able to access it.
- The * property: Anyone accessing a resource can only write its contents to one classified at the same level or higher.
- These properties are generally summarized as "no read up" and "no write down," respectively. In short, this means that when we are handling classified information, we cannot read any higher than our clearance level, and we cannot write classified data down to any lower level.

The Biba model

- The Biba model of access control is primarily concerned with protecting the integrity of data, even at the expense of confidentiality. Biba has two security rules that are the exact reverse of those we discussed in the Bell–LaPadula model.
- The simple integrity axiom: The level of access granted to an individual must be no lower than the classification of the resource.
- The * integrity axiom: Anyone accessing a resource can only write its contents to one classified at the same level or lower.
- We can summarize these rules as "no read down" and "no write up," respectively. This may seem completely counterintuitive when we consider protecting information, but remember that we have changed the focus from confidentiality to integrity. In this case, we are protecting integrity by ensuring that our resource can only be written to by those with a high level of access and that those with a high level of access do not access a resource with a lower classification.

The Brewer and Nash model

- The Brewer and Nash model, also known as the Chinese Wall model, is an access control model designed to prevent conflicts of interest. Brewer and Nash is commonly used in industries that handle sensitive data, such as that found in the financial, medical, or legal industry.
- Objects: Resources such as files or information, pertaining to a single organization.
- Company groups: All objects pertaining to a particular organization.
- Conflict classes: All groups of objects that concern competing parties.
- If we look at the example of a commercial law firm working for companies in a certain industry, we might have files that pertain to various individuals and companies working in that industry. As an individual lawyer at the firm accesses data and works for different clients, he could potentially access confidential data that would generate a conflict of interest while working on a new case. In the Brewer and Nash model, the resources and case materials that the lawyer was allowed access to would dynamically change based on the materials he had previously accessed.

Physical Access Controls

- Physical Access control for individuals often revolves around controlling movement into and out of buildings or facilities.
- One of the more common issues with physical access controls is that of tailgating.
- Tailgating occurs when we authenticate to the physical access control measure, such as using a badge, and then another person follows directly behind us without authenticating themselves. Tailgating can cause a variety of issues, including allowing unauthorized individuals into the building and creating an inaccurate representation of who is actually in the building in case there is an emergency.