6.1.6 Access Control Model Facts

This lesson covers the topic of access control models.

Access Control Models

Access control is the process by which resource and service use is granted or denied. The following table lists the most commonly used access control models, also known as *access control schemes*.

Model	Description
Attribute-based access control (ABAC)	*Attribute-based* access control restricts access by assigning attributes to resources. ▪ Attributes can be things like a user's role, position, or current project. ▪ The set of attributes assigned to a resource constitutes a policy that uses Boolean logic to determine who can access the resource. ▪ An example of a file access policy might include the following attributes: role = manager, department = development, and project = NewApp. Only users who possess all three attributes can access the file. ▪ ABAC uses a special markup language called eXtensible Access Control Markup Language (XACML) to define access control policies.
Role-based access control (RBAC)	*Role-based* access control allows access based on a role in an organization; it is not user specific. Role-based access control is also known as non-discretionary access control. ▪ Roles are defined by job description or security access level. ▪ Users are made members of a role and receive the permissions assigned to the role. ▪ RBAC is similar to group-based access control. Group-based access control uses a collection of users; RBAC uses a collection of permissions.
Rule-based access control	*Rule-based* access control uses rules applied to characteristics of objects or subjects to restrict access. ▪ Access control entries identify a set of characteristics that are examined for a match. ▪ If all characteristics match, access is either allowed or denied based on the rule. ▪ An example of a rule-based access control implementation is a router access control list that allows or denies traffic based on characteristics within the packet, such as IP address or port number. ▪ Because rule-based access control does not consider the identity of the subject, a system that uses rules can be viewed as a form of mandatory access control.
Mandatory access control (MAC)	*Mandatory* access control uses labels for both subjects (users who need access) and objects (resources with controlled access, such as data, applications, systems, networks, and physical space). Every operation performed is tested against a set of authorization policies to determine if the operation is allowed. ▪ Classification labels, such as secret or top secret, are assigned to objects by their owner, who is usually a managerial or governmental entity. ▪ Clearance labels are assigned to subjects. ▪ When a subject's clearance lines up with an object's classification and the user has a need to know (referred to as a category), the user is then granted access. ▪ Access control is mandatory because access is based on policy (the matching of the labels) rather than identity. Owners can only assign labels; they cannot grant access to

	specific subjects.
Discretionary access control (DAC)	*Discretionary* access control assigns access directly to subjects based on the owner's discretion. ▪ Objects have a discretionary access control list (DACL) with entries for each subject. ▪ Owners add subjects to the DACL and assign rights or permissions. The permissions identify the actions the subject can perform on the object. ▪ With discretionary access control, subjects can pass permissions on to other subjects. Many computer systems use discretionary access control to limit access to systems or other resources.
Conditional access	*Conditional* access is a way to enforce access control while also encouraging users to be productive wherever they are. Conditional access isn't intended to be the first point of security. Instead, it steps in after the first-factor authentication has been granted. Conditional access policies work by asking a user to complete an action in order to access a resource. Depending on the level of security of the requested resource, the user may be required to complete more actions. For policy decisions, conditional access can be configured to consider many different factors including: ▪ Implement control at the user or group level. ▪ Permit or deny access based on an IP address or an IP range. ▪ Permit or deny access to users who are using specific applications. ▪ Permit, restrict, or deny access to users who are using specific devices or device states.