8.1.3 Access Control Model Facts

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:

Access Control Model	Characteristics
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 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 allow 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.
Role-Based Access Control (RBAC)	*Role-based access control* allows access based on a role in an organization, not individual users. 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, and RBAC uses a collection of permissions.
Rule-Based Access Control (RBAC)	*Rule-based access control* uses characteristics of objects or subjects and rules 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.
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 constitute 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 to define access control policies.
Federated Access Control	Federated identity management (FIM) is an arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group. The use of such a system is sometimes called identity federation. Identity federation offers economic advantages (as well as convenience) to enterprises and their network subscribers. For example, multiple corporations can share a single application, resulting in cost savings and resource consolidation. In order for FIM to be effective, the partners must have a sense of mutual trust. Authorization messages among partners in an FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar XML standard that allows a user to log on once for affiliated but separate websites or networks.

The distinction between confidentiality and integrity is relevant to understanding academic access control models. Remember the following:

- *Confidentiality* is keeping secrets a secret. It is also referred to as *privacy*.

- *Integrity* is ensuring that information is not corrupted or inappropriately altered. There are four main statutes of integrity:
  - Data must be protected from modification by unauthorized users.
  - Data must be protected from modification by authorized users.
  - Stored data must be internally and externally consistent.
  - Databases must be internally and externally consistent.
- The implementation of either confidentiality or integrity does not imply the implementation of the other, as they do not address the same issues.
