

## 8.1.2 Access Control Facts

---

*Access control* is the ability to permit or deny the privileges that users have when accessing resources on a network or computer. Access control involves three entities:

- *Objects* are the data, applications, systems, networks, and physical space.
- *Subjects* are the users, applications, or processes that need access to objects.
- The access control *system* includes the policies, procedures, and technologies that are implemented to control subjects' access to objects.

Access control includes the following processes:

- *Identification* identifies the subject. Examples include a user name or a user ID number.
- *Authentication* is the process of validating a subject's identity. It includes the identification process, the user providing input to prove identity, and the system accepting that input as valid.
- *Authorization* is granting or denying a subject's access to an object based on the subject's level of permissions or the actions allowed with the object.
- *Auditing* (also referred to as *accounting*) is maintaining a record of a subject's activity within the information system.

Authentication, authorization, and auditing are known as the AAA of access control.

An access control *policy* defines the steps and measures that are taken to control subjects' access to objects. Access controls can be classified according to the function they perform:

- *Preventive* access controls deter intrusion or attacks (such as separation of duties and dual-custody processes).
- *Detective* access controls search for details about the attack or the attacker (such as intrusion detection systems).
- *Corrective* access controls implement short-term repairs to restore basic functionality following an attack.
- *Deterrent* access controls discourage attack escalation.
- *Recovery* access controls restore the system to normal operations after the attack and short-term stabilization period.
- *Compensative* access controls are alternatives to primary access controls.

Access control measures can also be classified based on how they restrict or control access:

- *Administrative* controls are policies that describe accepted practices. Examples include directive policies and employee awareness training.
- *Technical* controls are computer mechanisms that restrict access. Examples include encryption, one-time passwords, access control lists, and firewall rules.
- *Physical* controls restrict physical access. Examples include perimeter security, site location, networking cables, and employee segregation.

On a computer network, a *directory service* is an example of a technical access control system that you use to manage and enforce access control policies. Examples of directory services include:

- Active Directory for Microsoft Windows networks
- NetIQ's eDirectory for Linux and Windows networks

Within the directory service:

- A user account is created for each subject.
- Identification is performed during logon when the user supplies a valid user account name.
- Authentication is performed during logon by when the user supplies a password or other requirements to prove his identity.
- Authorization to use network resources, such as files, printers, or computers, is controlled by *permissions* or *rights*.
- Auditing is performed by the operating system as it tracks subjects' actions toward objects.

---

TestOut Corporation All rights reserved.