

## Real-World Scenario 11-4: Understanding Access Control Models

Access control can deal with a lot of different things, but in technology what we are most concerned with is the access to data and how it is controlled.

Use the Internet to research the four types of access control listed in the table, and give a description of each and an example of technology environments for each.

Access Control Model	Description	Example
DAC		
MAC		
RBAC		
ABAC		

## Real-World Scenario 11-4 Solution

There is some overlap when it comes to access control models. That is partially true because the functional definitions of the various access models have changed over time, and the software that uses them has changed over time as well. For example, you might see that FreeBSD is considered to be either MAC-based or RBAC-based depending on its implementation.

The following table gives sample descriptions and examples of four access control models.

Access Control Model	Description	Examples
DAC	Access control policy generally determined by the owner. Objects such as files and printers can be created and accessed by the owner.	Windows domains Linux Red Hat networks
MAC	Access control policy determined by a computer system, not by a user or an owner.  Defines sensitivity labels that are assigned to <i>subjects</i> (users) and <i>objects</i> (files and folders).	Military Government SELinux Multilevel secure (MLS) systems; for example, NSA, Boeing, Honeywell, and so on

Access Control		
Model	Description	Examples
RBAC	Controlled by the system but works with sets of permissions known as roles.	Solaris SAP Active Directory (server roles)
ABAC	Access rights are granted to users through the use of multiple policies that combine user/group/resource attributes together.  Uses IF-THEN statements based on the user and the requested resource.	XACML  Claims-based access control (CBAC)—a Microsoft implementation

**Simulation:** Complete the simulation "11-4: Understanding Access Control Models."