Chapter 4(4.1 to 4.7)

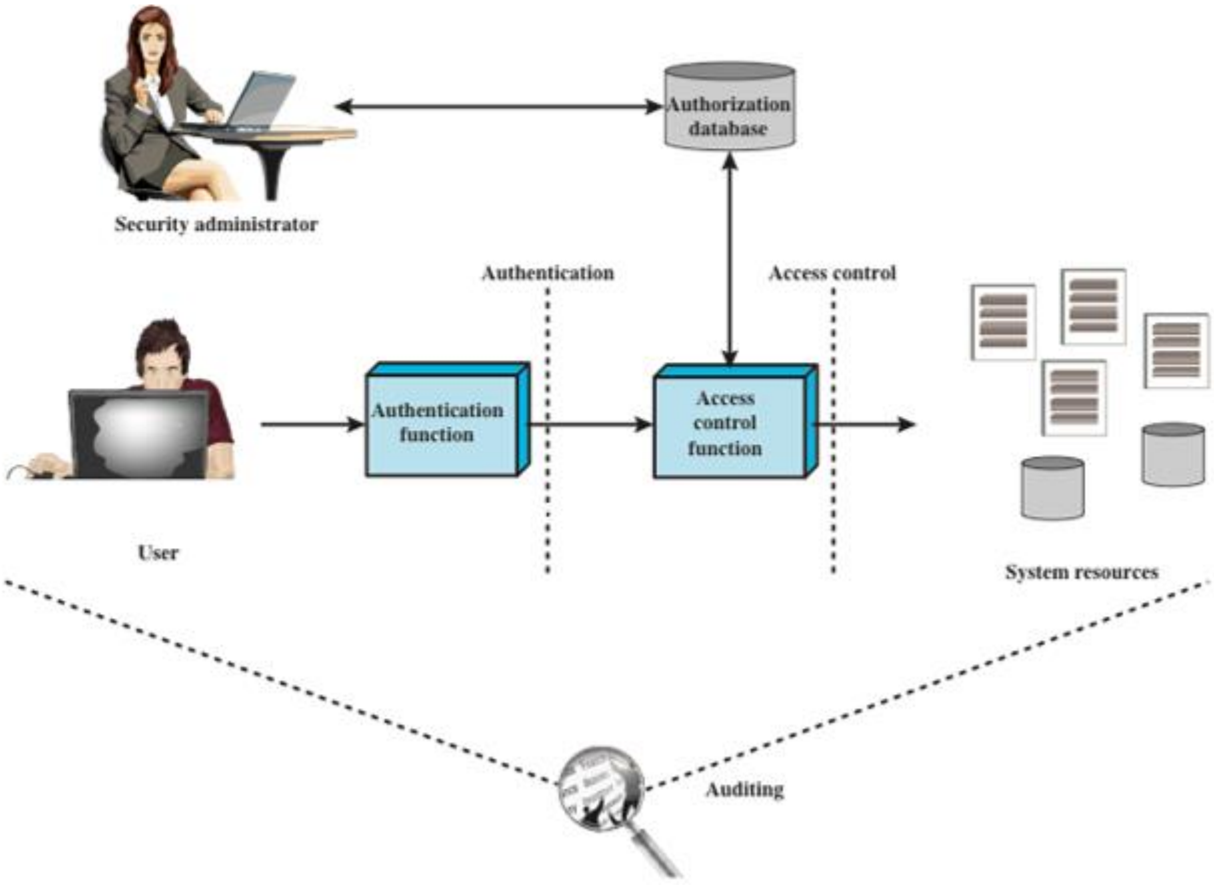


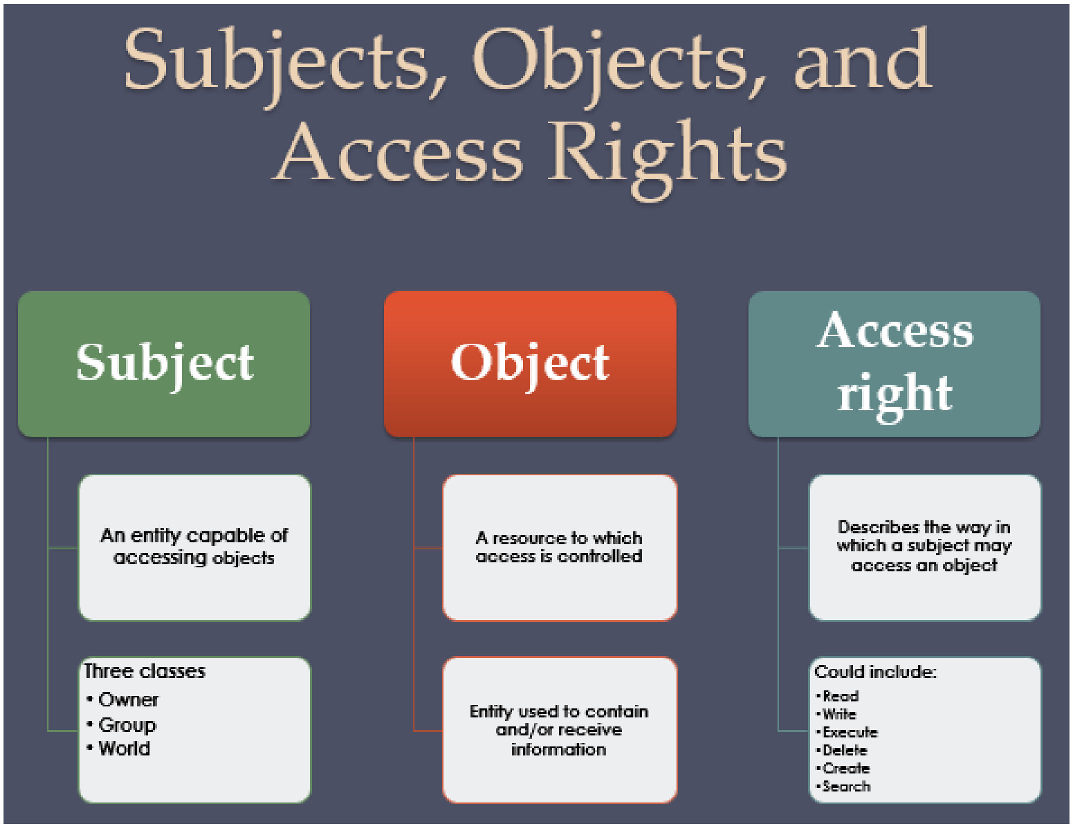
Figure 4.1 Relationship Among Access Control and Other Security Functions

- **Authentication**: Verification that the credentials of a user or other system entity are valid.
- **Authorization**: The granting of a right or permission to a system entity to access a system resource. This function determines who is trusted for a given purpose.

Access Control Policies:

- **Role-based access control (RBAC):** This type of policy grants access to resources based on an individual's role within an organization. For example, a CEO might have access to all company resources, while a customer service representative might only have access to certain resources related to their job.
- **Discretionary access control (DAC):** This type of policy allows the owner of a resource to determine who has access to that resource. For example, a user might be able to share a file with other users on the same network, but only if they have permission from the file owner. Better to use in small scale organization.
- **Mandatory access control (MAC):** This type of policy uses a pre-defined set of rules to determine who has access to which resources. MAC ensures that only authorized individuals have access to sensitive resources, based on their clearance level and the sensitivity of the resource. Used mostly for military Information security.
- **Attribute-based access control (ABAC):** This type of policy uses attributes, or characteristics, of both the user and the resource to determine access. For example, a user might only have access to a

resource if they have a certain security clearance and are accessing the resource from a specific location.



Subjects, Objects, and Access Rights

Subject

- An entity capable of accessing objects
- Three classes
  - Owner
  - Group
  - World

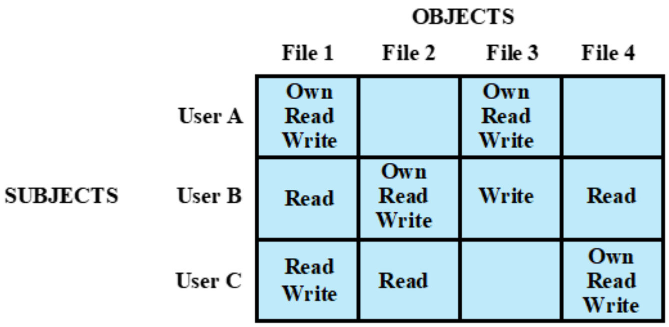
Object

- A resource to which access is controlled
- Entity used to contain and/or receive information

Access right

- Describes the way in which a subject may access an object
- Could include:
  - Read
  - Write
  - Execute
  - Delete
  - Create
  - Search

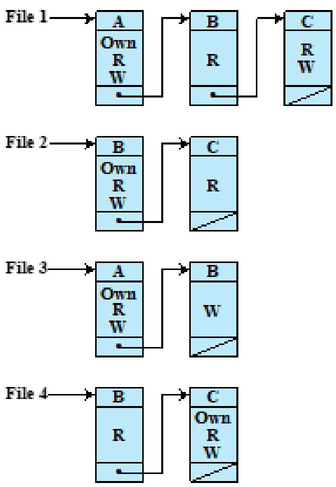
Access Control Structures:



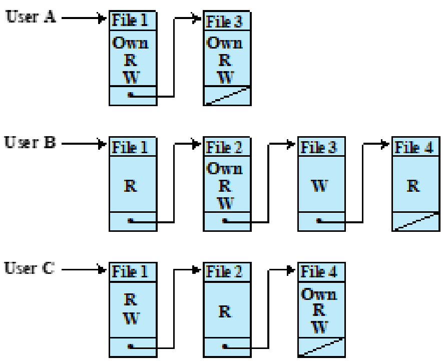
OBJECTS

SUBJECTS		File 1	File 2	File 3	File 4
	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

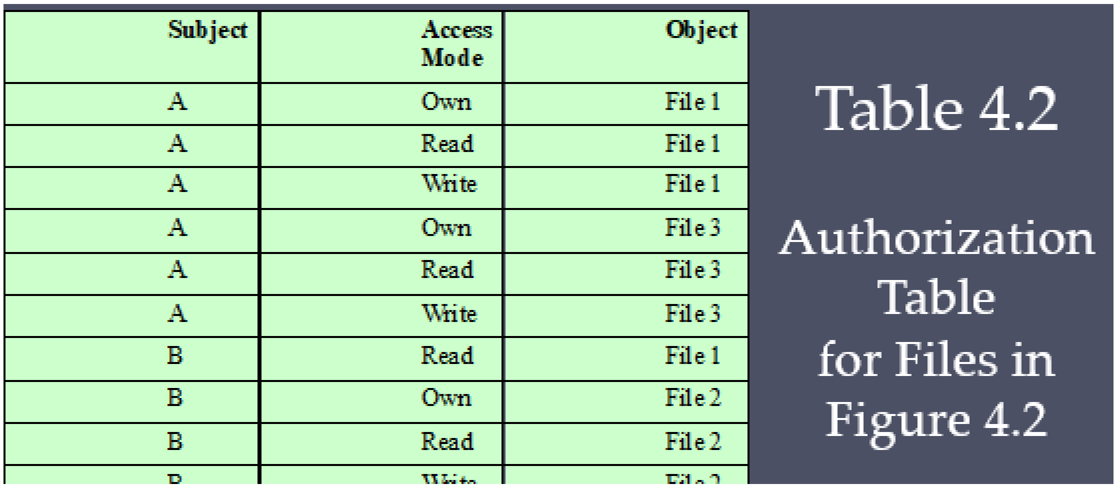
(a) Access matrix



(b) Access control lists for files of part (a)



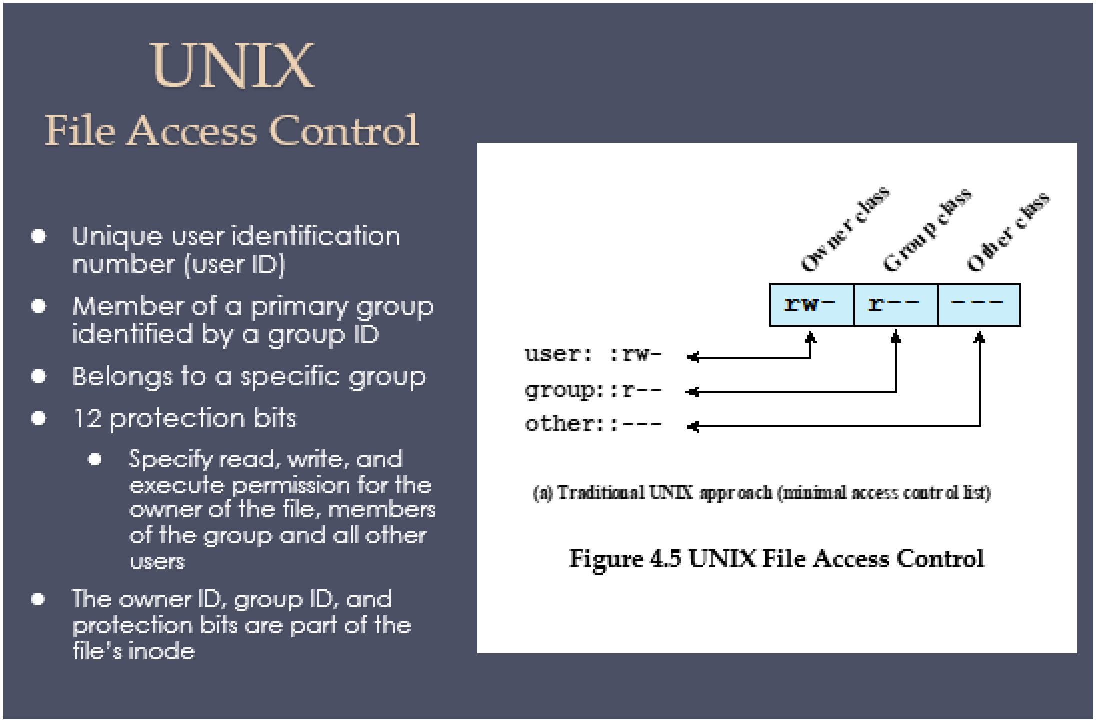
(c) Capability lists for files of part (a)



Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2

Table 4.2

Authorization Table for Files in Figure 4.2



UNIX

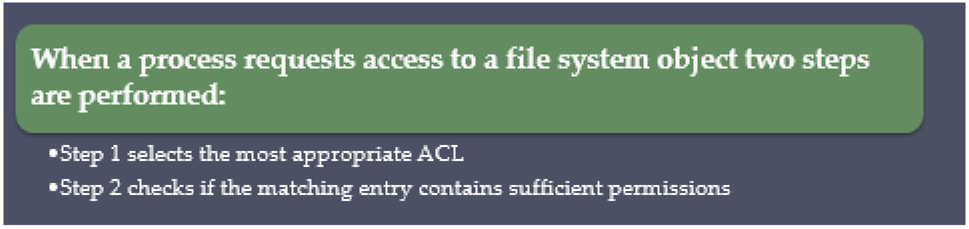
File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode

Owner class
Group class
Other class
rw-
r--
---
user: :rw-
group: :r--
other: :---

(a) Traditional UNIX approach (minimal access control list)

Figure 4.5 UNIX File Access Control



When a process requests access to a file system object two steps are performed:

- Step 1 selects the most appropriate ACL
- Step 2 checks if the matching entry contains sufficient permissions

RBAC systems assign access rights to roles instead of individual users. In turn, users are assigned to different roles, either statically or dynamically, according to their responsibilities.

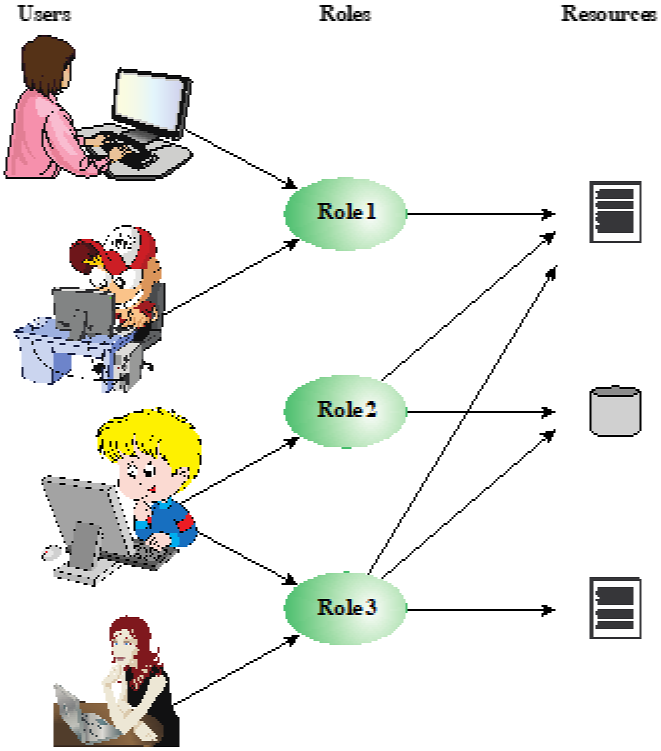
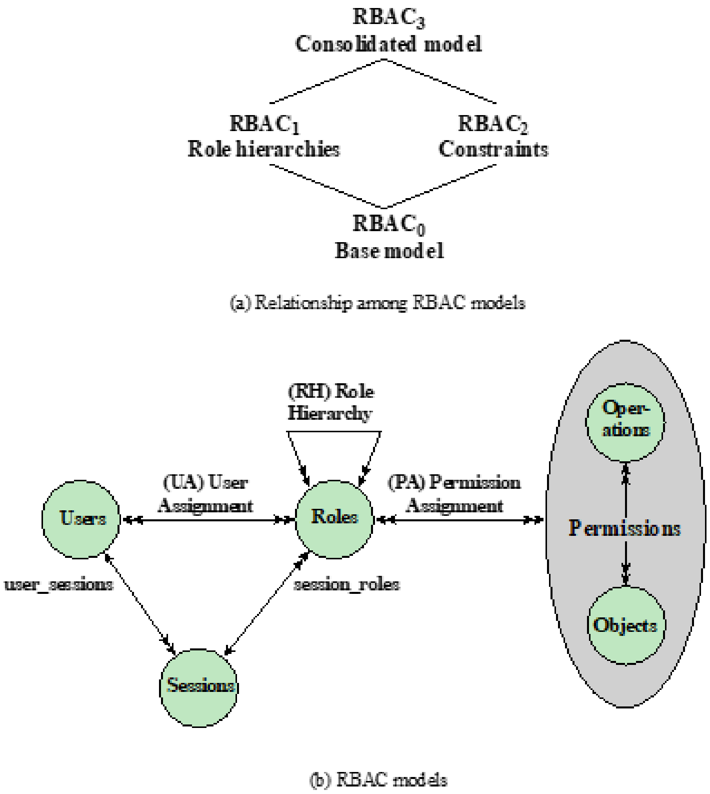


Figure 4.6 Users, Roles, and Resources

There is a many-to-many relationship between users and roles: One user may have multiple roles, and multiple users may be assigned to a single role. Similarly, there is a many-to-many relationship between roles and permissions. A session is used to define a temporary one-to-many relationship between a user and one or more of the roles to which the user has been assigned. The user establishes a session with only the roles needed for a particular task; this is an example of the concept of least privilege.



(a) Relationship among RBAC models

(b) RBAC models

Figure 4.8 A Family of Role-Based Access Control Models.

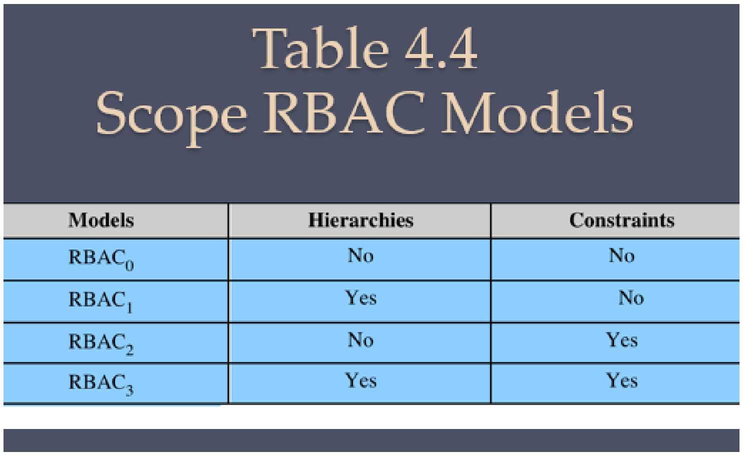
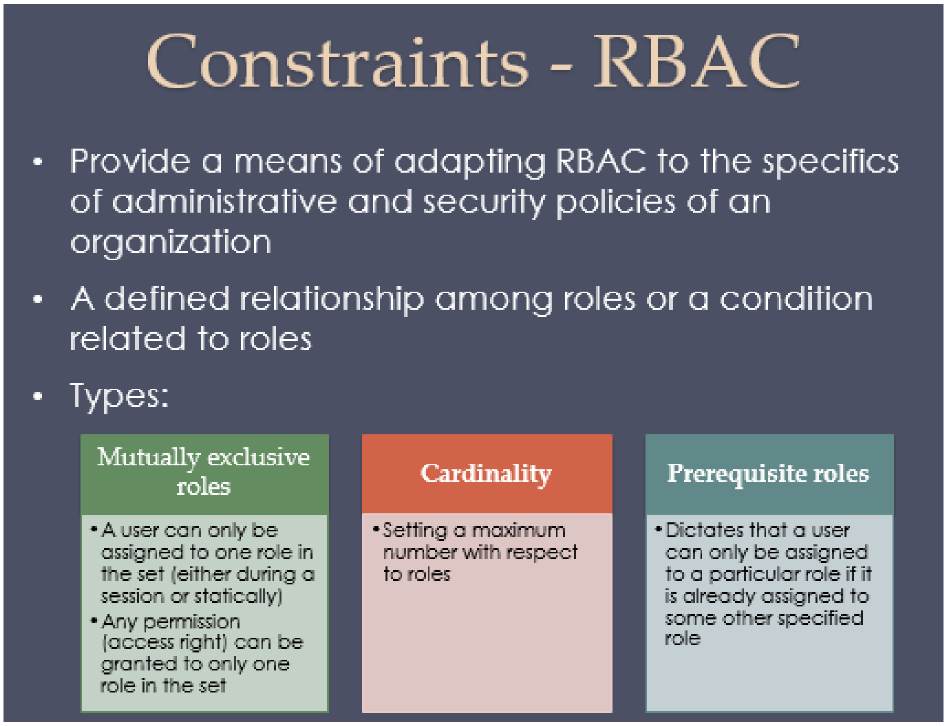


Table 4.4
Scope RBAC Models

Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes



Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles

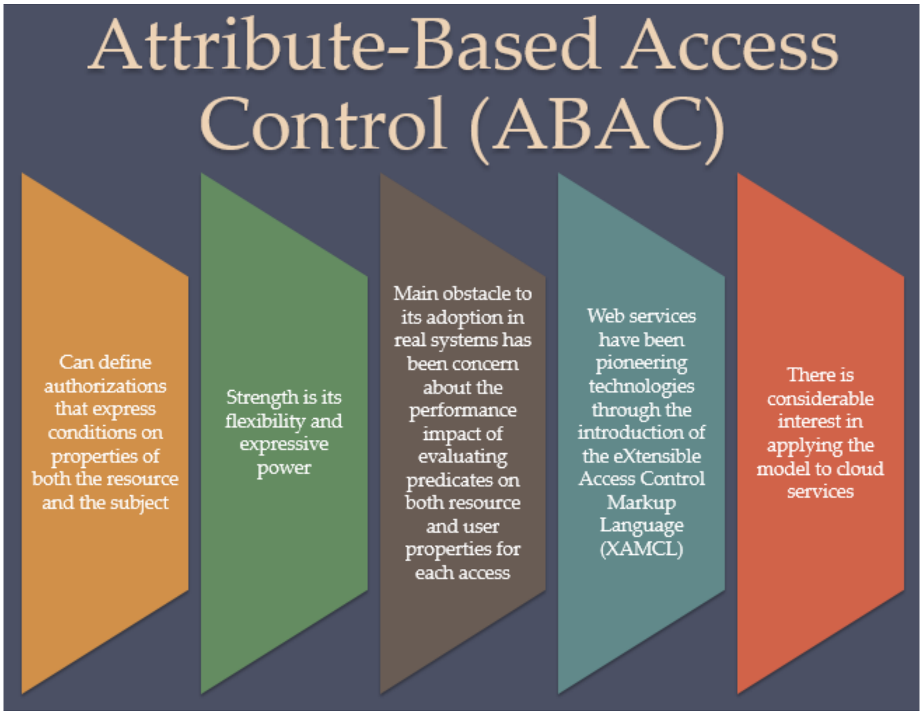
- A user can only be assigned to one role in the set (either during a session or statically)
- Any permission (access right) can be granted to only one role in the set

Cardinality

- Setting a maximum number with respect to roles

Prerequisite roles

- Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role



Attribute-Based Access Control (ABAC)

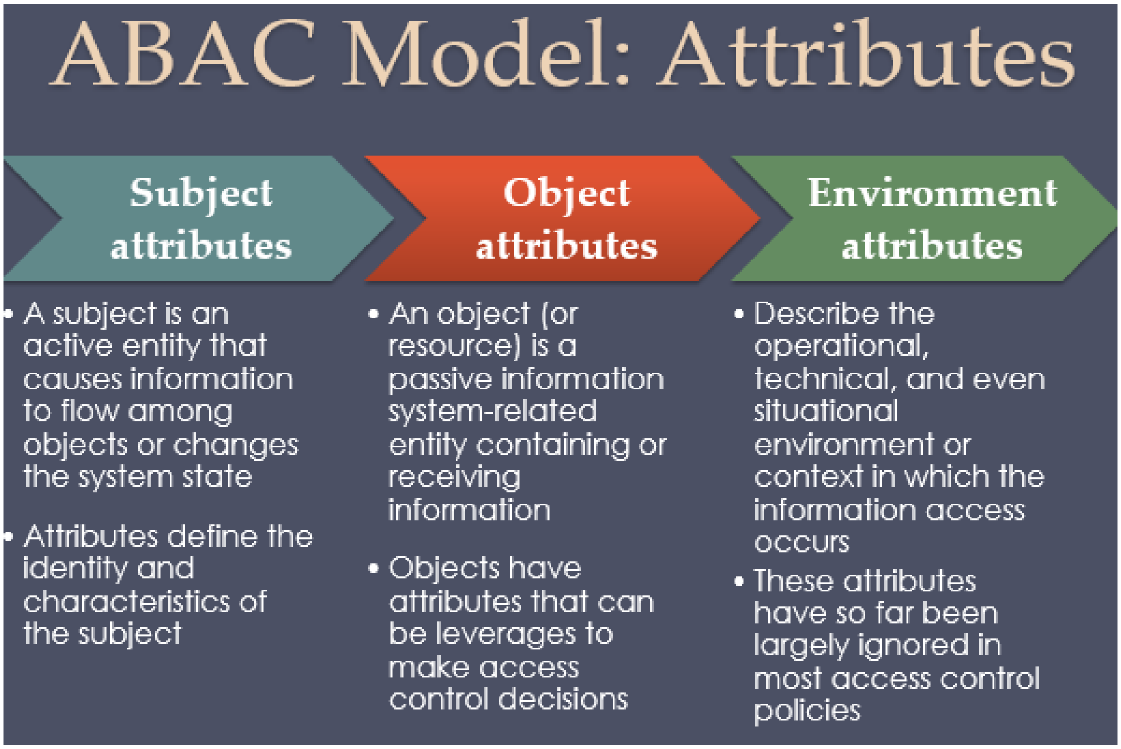
Can define authorizations that express conditions on properties of both the resource and the subject

Strength is its flexibility and expressive power

Main obstacle to its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access

Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL)

There is considerable interest in applying the model to cloud services



ABAC Model: Attributes

Subject attributes

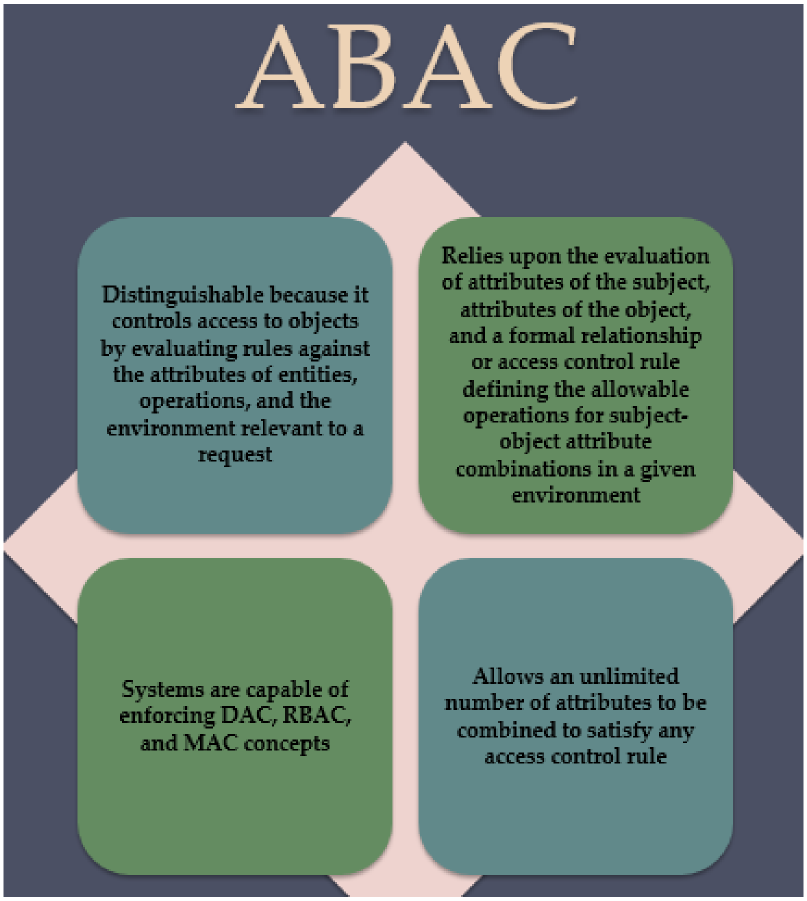
- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions

Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies



ABAC

Distinguishable because it controls access to objects by evaluating rules against the attributes of entities, operations, and the environment relevant to a request

Relies upon the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject-object attribute combinations in a given environment

Systems are capable of enforcing DAC, RBAC, and MAC concepts

Allows an unlimited number of attributes to be combined to satisfy any access control rule

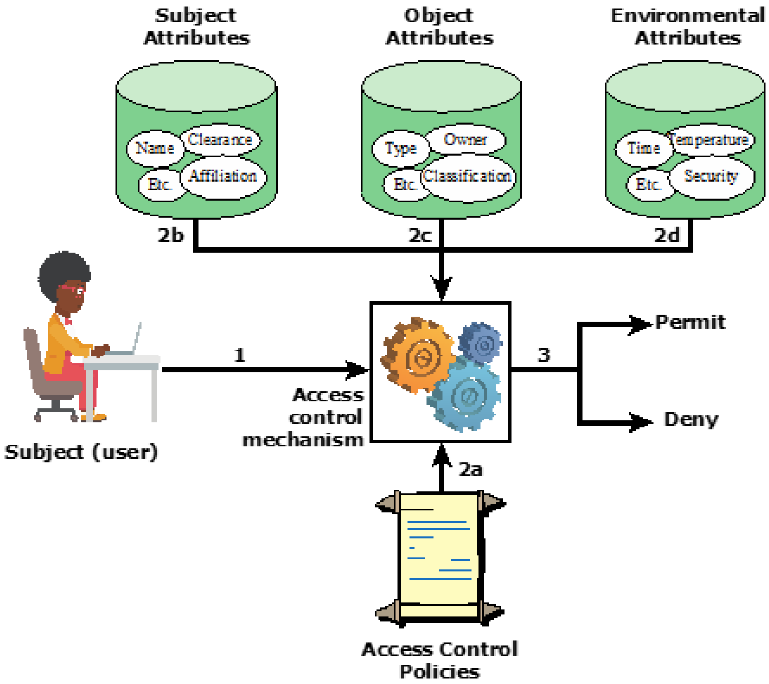


Figure 4.10 ABAC Scenario

Identity, Credential, and Access Management (ICAM):

ICAM is a comprehensive approach to managing and implementing digital identities (and associated attributes), credentials, and access control.

Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE

Goal is to establish a trustworthy digital identity that is independent of a specific application or context

Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program

Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application

Final element is lifecycle management which includes:

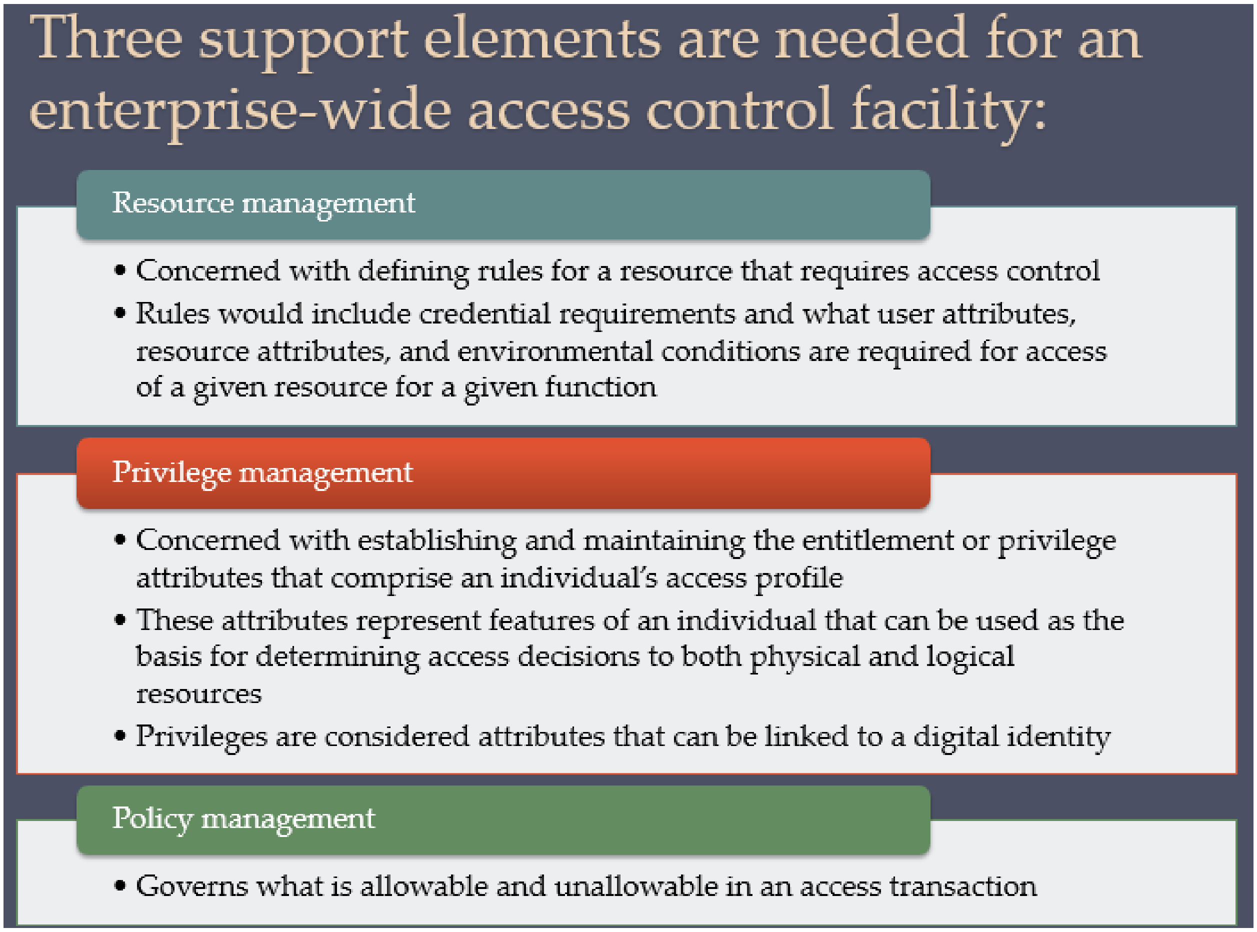
- Mechanisms, policies, and procedures for protecting personal identity information
- Controlling access to identity data
- Techniques for sharing authoritative identity data with applications that need it
- Revocation of an enterprise identity

Credential Management:

A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber. For example: smart cards, private/public cryptographic keys, and digital certificates.

Credential management encompasses the following five logical components:

1. An **authorized individual sponsors an individual or entity for a credential** to establish the need for the credential. For example, a department supervisor sponsors a department employee.
2. The **sponsored individual enrolls for the credential**, a process which typically consists of identity proofing and the **capture of biographic and biometric data**.
3. A **credential is produced.** Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smartcard, or other functions.
4. The credential is **issued to the individual** or NPE.
5. Finally, **a credential must be maintained over its life cycle**, which might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement.



Three support elements are needed for an enterprise-wide access control facility:

Resource management

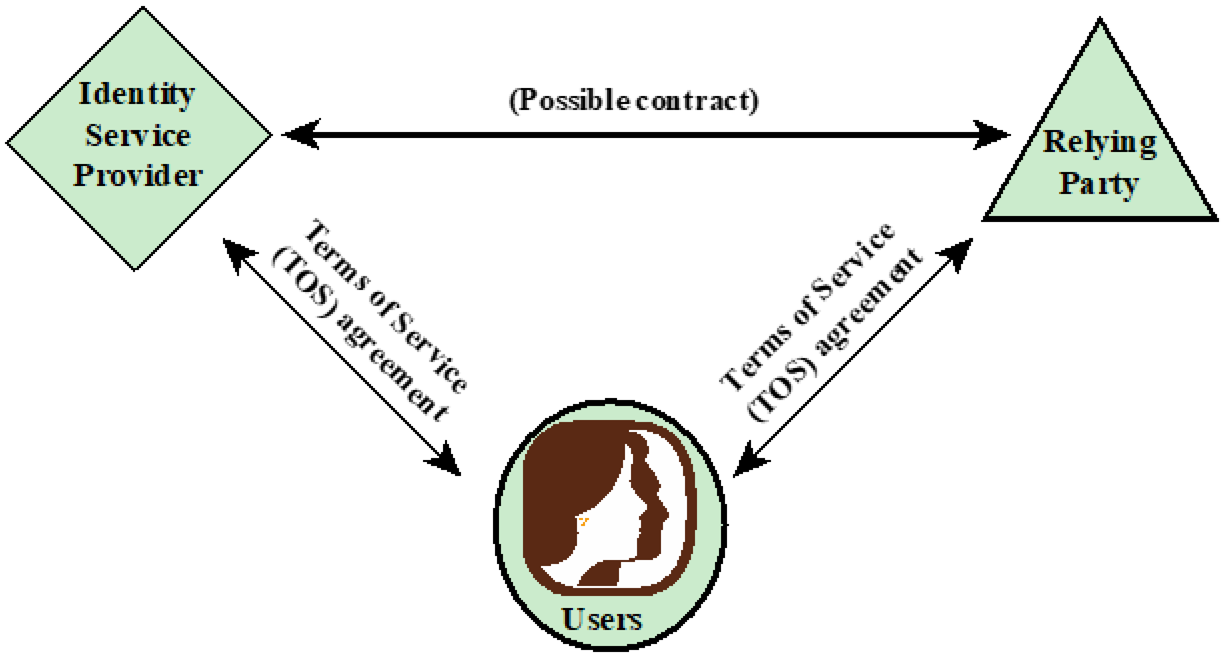
- Concerned with defining rules for a resource that requires access control
- Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

Privilege management

- Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile
- These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
- Privileges are considered attributes that can be linked to a digital identity

Policy management

- Governs what is allowable and unallowable in an access transaction



Identity Service Provider
(Possible contract)
Relying Party
Terms of Service (TOS) agreement
Terms of Service (TOS) agreement
Users

(a) Traditional triangle of parties involved in an exchange of identity information

- The **relying party** requires that **the user has been authenticated to some degree of assurance**, that the attributes imputed to the user by the identity service provider are accurate, and that the **identity service provider is authoritative for those attributes.**
- The **identity service provider** requires assurance that **it has accurate information about the user** and that, if it shares information, the relying party will use it in accordance with contractual terms and conditions and the law.
- The **user** requires assurance that the **identity service provider and relying party can be entrusted with sensitive information** and that they will abide by the user's preferences and respect the user's privacy.