UNIT III

CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS

Access Control

This section provides an overview of important aspects of access control. It is useful to begin by defining the following terms:

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

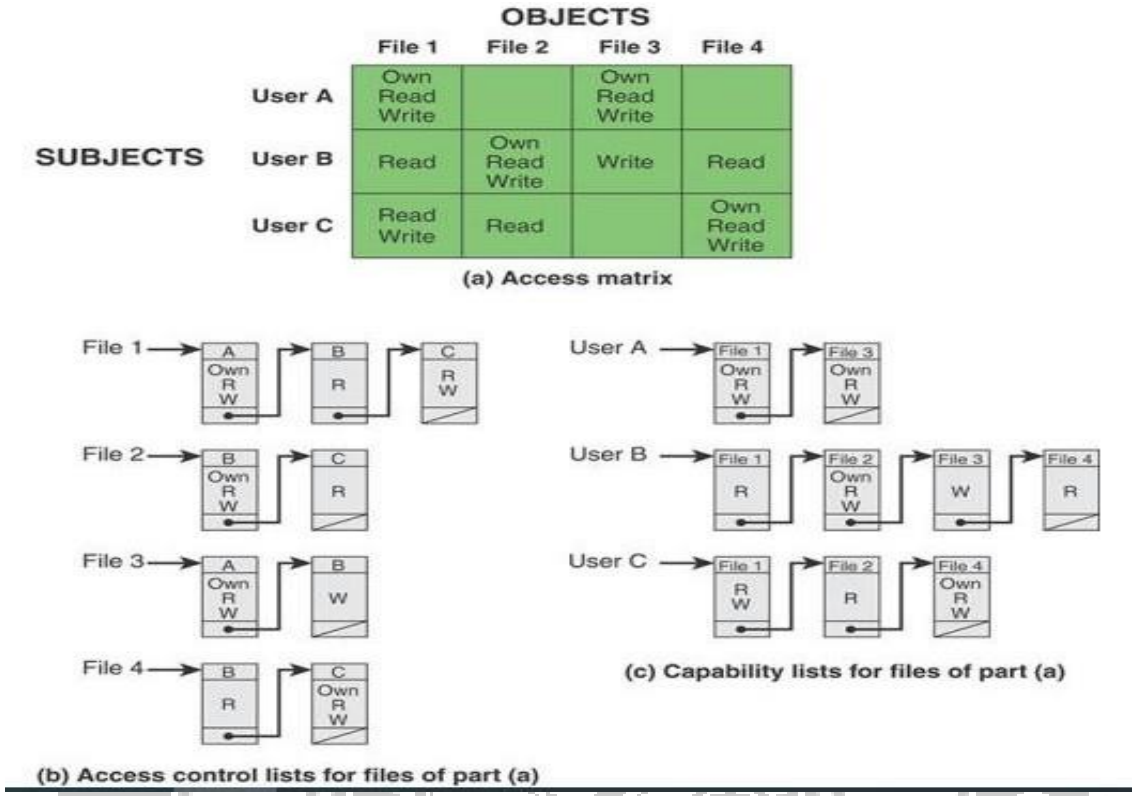
Access control: The process of granting or denying specific requests for obtaining and using information and related information processing services to enter specific physical facilities.

Access control mechanism: Security safeguards (that is, hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.

Access control service: A security service that protects against a system entity using a system resource in a way not authorized by the system9s security policy.

Basic access control systems typically define three classes of subject, with differentaccess rights for each class:

- **Owner**: This can be the creator of a resource, such as a file. For systemresources, ownership can belong to a system administrator. For project resources, a project administrator or leader can be assigned ownership.
- **Group:** In addition to the privileges assigned to an owner, a named group of users can also be granted access rights, such that membership in the group is sufficient to exercise these access rights. In most schemes, a user may belong to multiple groups.
- **World:** The least amount of access is granted to users who are able to access the system but are not included in the categories owner and group for this resource.



Examples of Access Control Structures

Access Control Policies

An access control policy dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories:

Access control policies are generally grouped into the following categories**:**

Discretionary access control (DAC): Access control based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Mandatory access control (MAC): Access control based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

Role-based access control (RBAC): Access control based on user roles (that is, a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions can be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role can apply to a single individual or to several individuals.

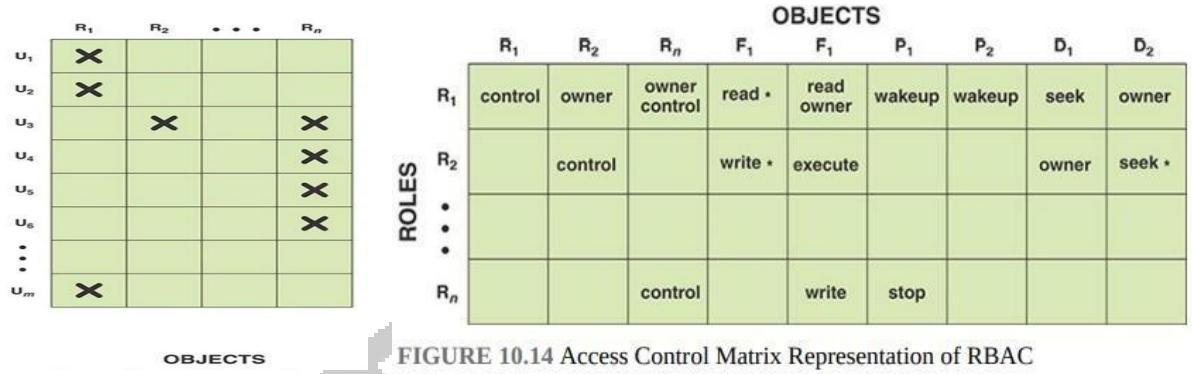


FIGURE 10.14 Access Control Matrix Representation of RBAC

Attribute-based access control (ABAC): Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access takes place.

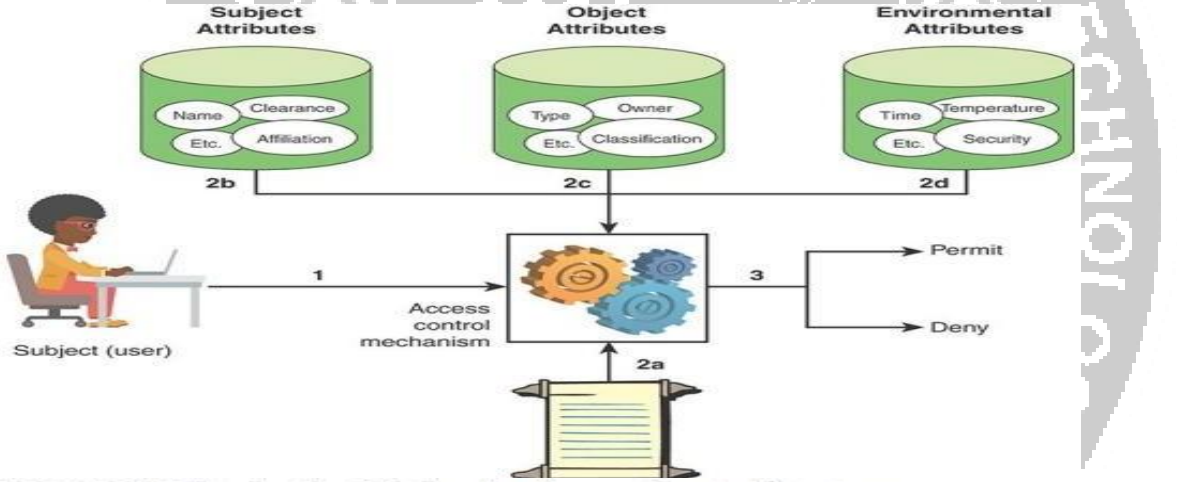


TABLE 10.7 Evaluation Metrics for Access Control Systems

Administrative Properties	Enforcement Properties
Auditing Privileges/capabilities discovery Ease of privilege assignments Syntactic and semantic support for specifying AC rules Policy management Delegation of administrative capabilities Flexibilities of configuration into existing systems The horizontal scope (across platforms and applications) of control The vertical scope (between application, DBMS, and OS) of control	Policy combination, composition, and constraint Bypass Least privilege principle support Separation of Duty (SoD) Safety (confinements and constraints) Conflict resolution or prevention Operational/situational awareness Granularity of control Expression (policy/model) properties Adaptable to the implementation and evolution of AC policies
Support Properties	**Performance Properties**
Policy import and export OS compatibility Policy source management User interfaces and API Verification and compliance function support	Response time Policy repository and retrieval Policy distribution Integrated with authentication function