Acess Control

Access Control Principles

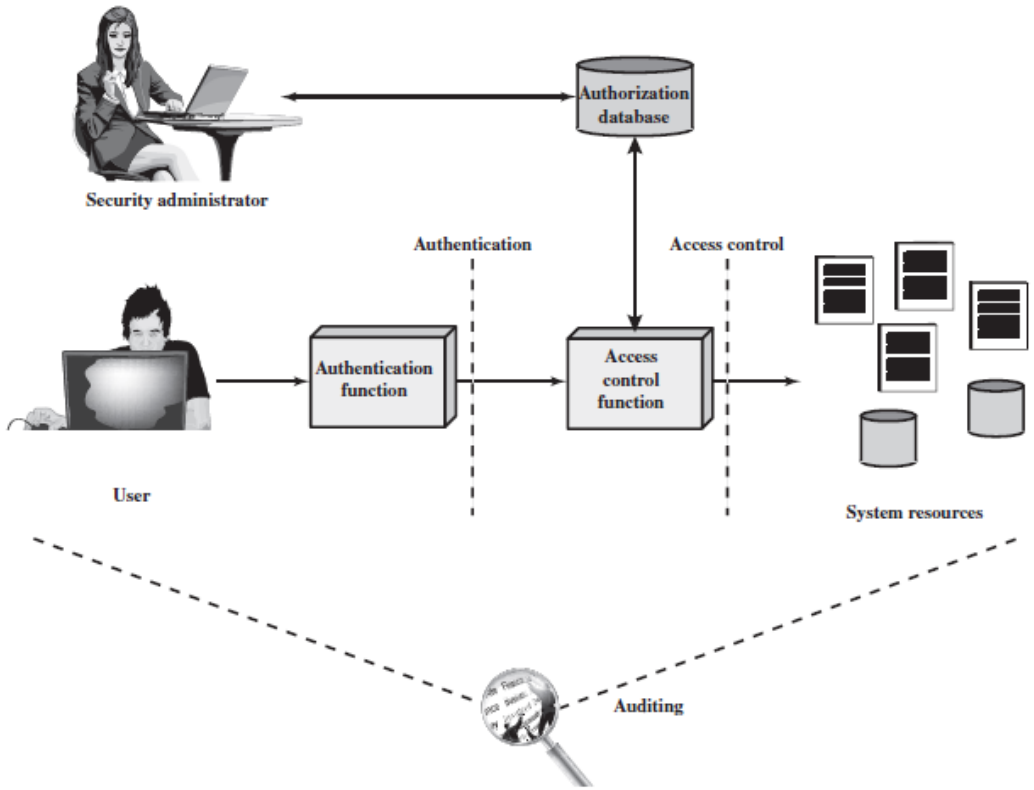


Figure 4.1 **Relationship Among Access Control and Other Security Functions**
Source: Based on [SAND94].

Introduction

- **Access control** is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system.
- It permits management to specify **what users can do**, **which resources they can access**, and **what operations they can perform on a system**.
- The goal of access control is to minimize the security risks of unauthorized access to physical and logical systems
- It consists of main components: authentication and authorization, audit

Access control types

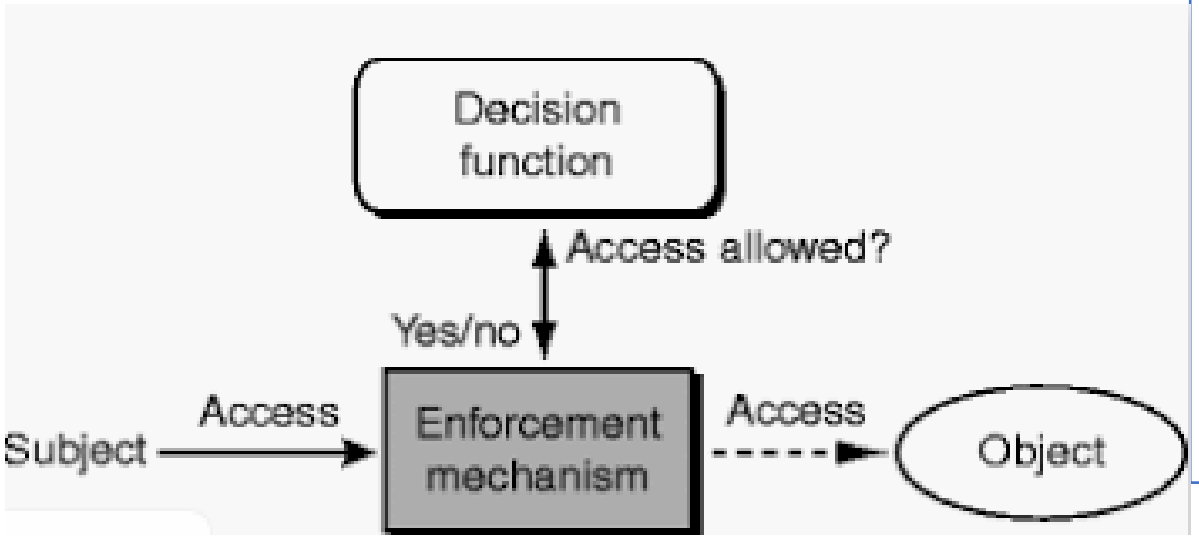
- **Physical access control**: limits access to campuses, building, rooms, and physical IT assets. (Fencing, hardware door locks,… that limit contact with devices)
- **Technical access control**: technology restrictions that limit users on computers from accessing data

Access controls encompass:

- ✓ **File permissions**, such as the right to create, read, edit or delete a file.
- ✓ **Program permissions**, such as the right to execute a program.
- ✓ **Data permissions**, such as the right to retrieve or update information in a database.

Components

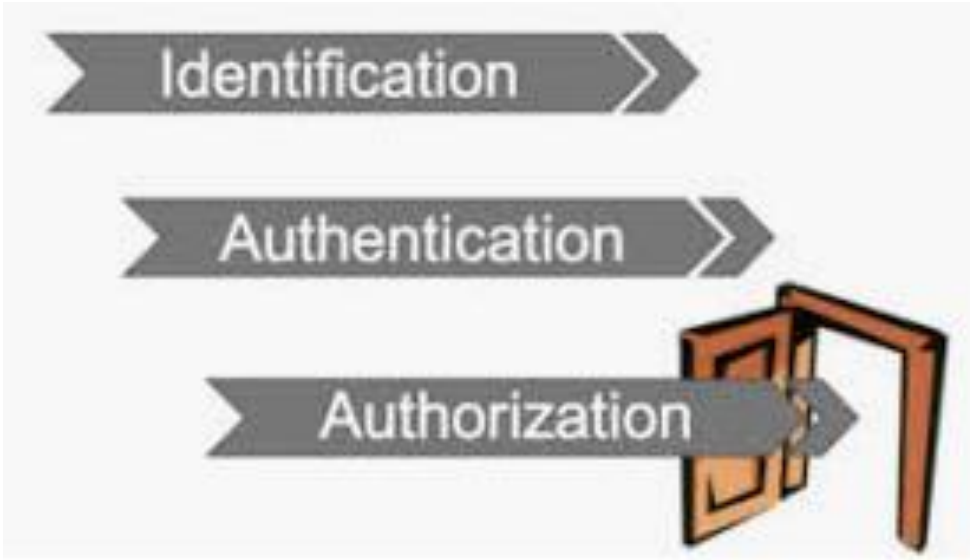
- The security features that control how users and systems communicate and interact with one another.



- **Access:** The flow of information between subject and object
- **Subject:** An active entity that requests access to an object or the data in an object
- **Object:** A passive entity that contains information

Access Control Terminology

Identification, authorization, and authorization are distinct functions.



- **Identification**

  Method of establishing the subject's (user, program, process) identity.

- **Authentication**

  Method of proving the identity

- **Authorization**

  Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.

Identification

- Identification asks the question: "Who are you?" When a new user completes the registration process, they are identifying themselves for you. Some companies limit their identity management process to just identification, taking the information users provide at face value. This can be very risky.
- Identification is the process of presenting an identity to a system. It is done in the initial stages of gaining access to the system and is what happens when you claim to be a particular system user.
- Verification moves from "Who are you?" to "Prove it." To verify the person is using their real name, address, phone number and so on, enterprises ask for verification. Verification can be in the form of a driver's license or government issued ID card, or biometric data, such as fingerprints or verified photos to be used for facial recognition.

Authentication

Authentication is the ability to prove that a user or application is genuinely who that person or what that application claims to be.

- For example, consider a user who logs on to a system by entering a user ID and password. The system uses the user ID to identify the user. The system authenticates the user at the time of logon by checking that the supplied password is correct.

Authentication

- Strong authentication is important

  To be properly authenticated, the subject is usually required to provide a second piece to the credential set (i.e., password, passphrase, key, PIN, token etc.

Authentication factors

Authentication factors determine the many different elements the system uses to verify one's identity before granting the individual access to anything.

- something you know
- Something you have
- Something you are

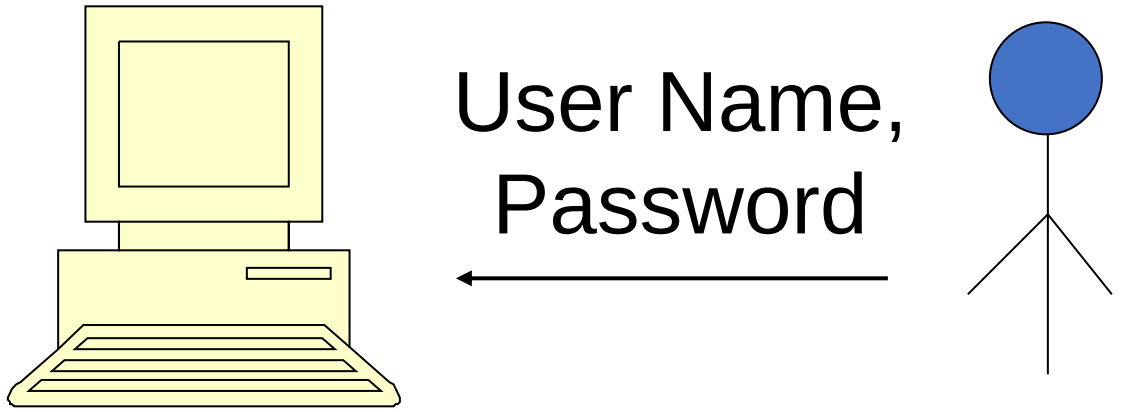
Authentication factors

- Based on the security level, authentication factors can vary from one of the following:
  - **Single- Factor Authentication**
  - **Two- Factor Authentication (2FA)**
  - **Multi- Factor Authentication (MFA)**

Something you know *(Knowledge-based)*

- Passwords are the most common form of authentication
- PIN

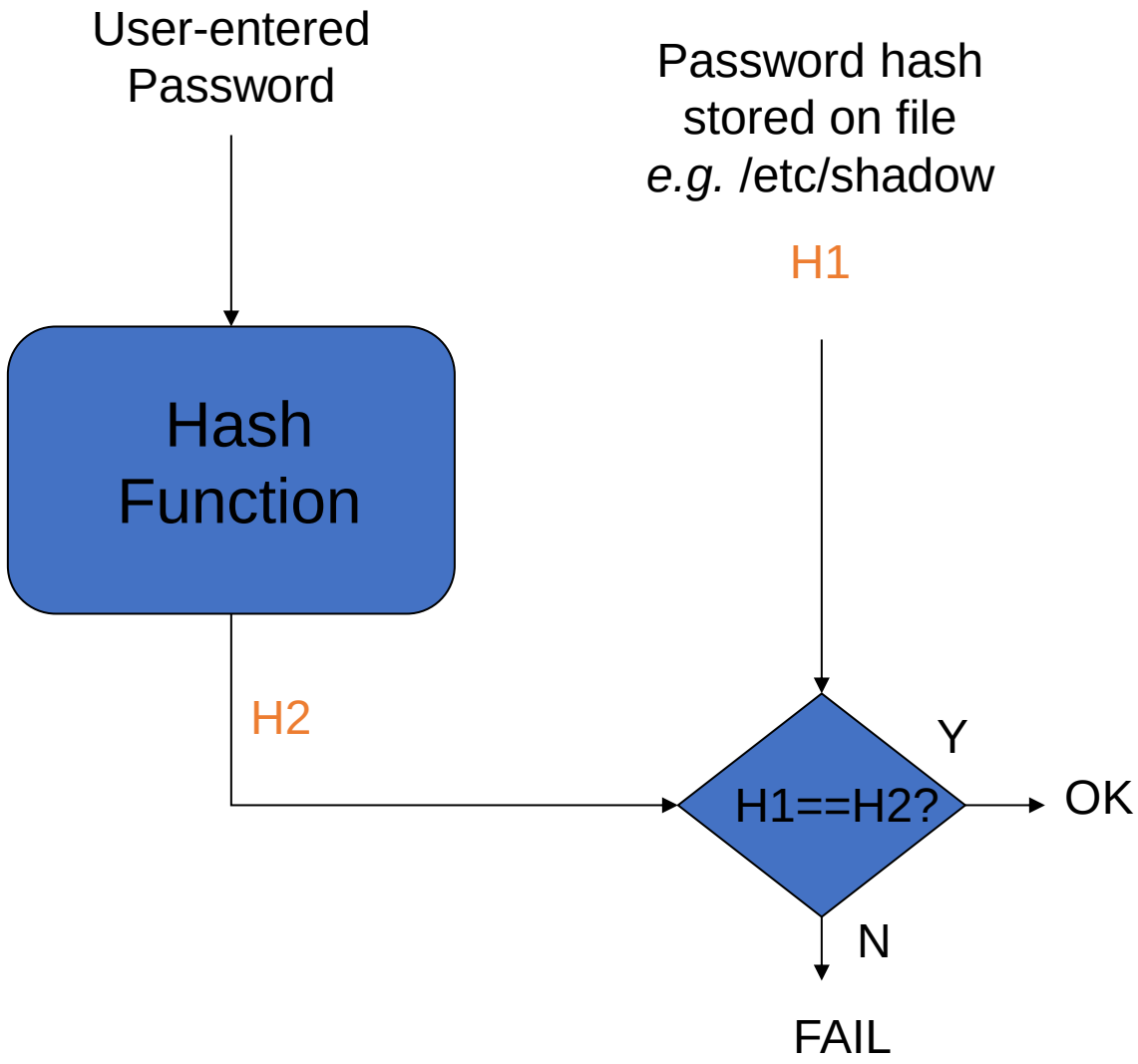
Simple Password Authentication



/etc/shadow

Something you know

Password Verification



Something you know

"Passwords are one of the biggest practical problems facing security engineers today."

Problems:

- Easy to share (intentionally or not)
- Easy to forget
- Often easy to guess
- Too many passwords to remember

Password vulnerabilities

- Access the password file
- Brute force attacks
- Directory attacks
- Social engineering

- Complex password policy
  - Forcing users to pick stronger passwords

The Vulnerability of Passwords

- Offline dictionary attack
- Specific account attack
- Popular password attack
- Password guessing against single user

Password Cracking of User-Chosen Passwords

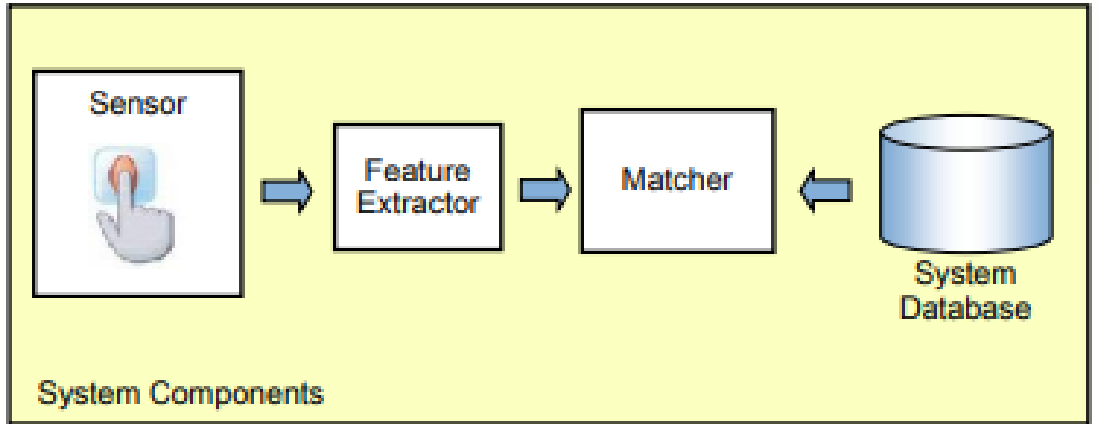
- Tradition Approach
  - Brute force.
  - Dictionary.
  - Rainbow table.
- Modern Approach.
  - Increase power of computing (GPU)
  - Sophisticated algorithms

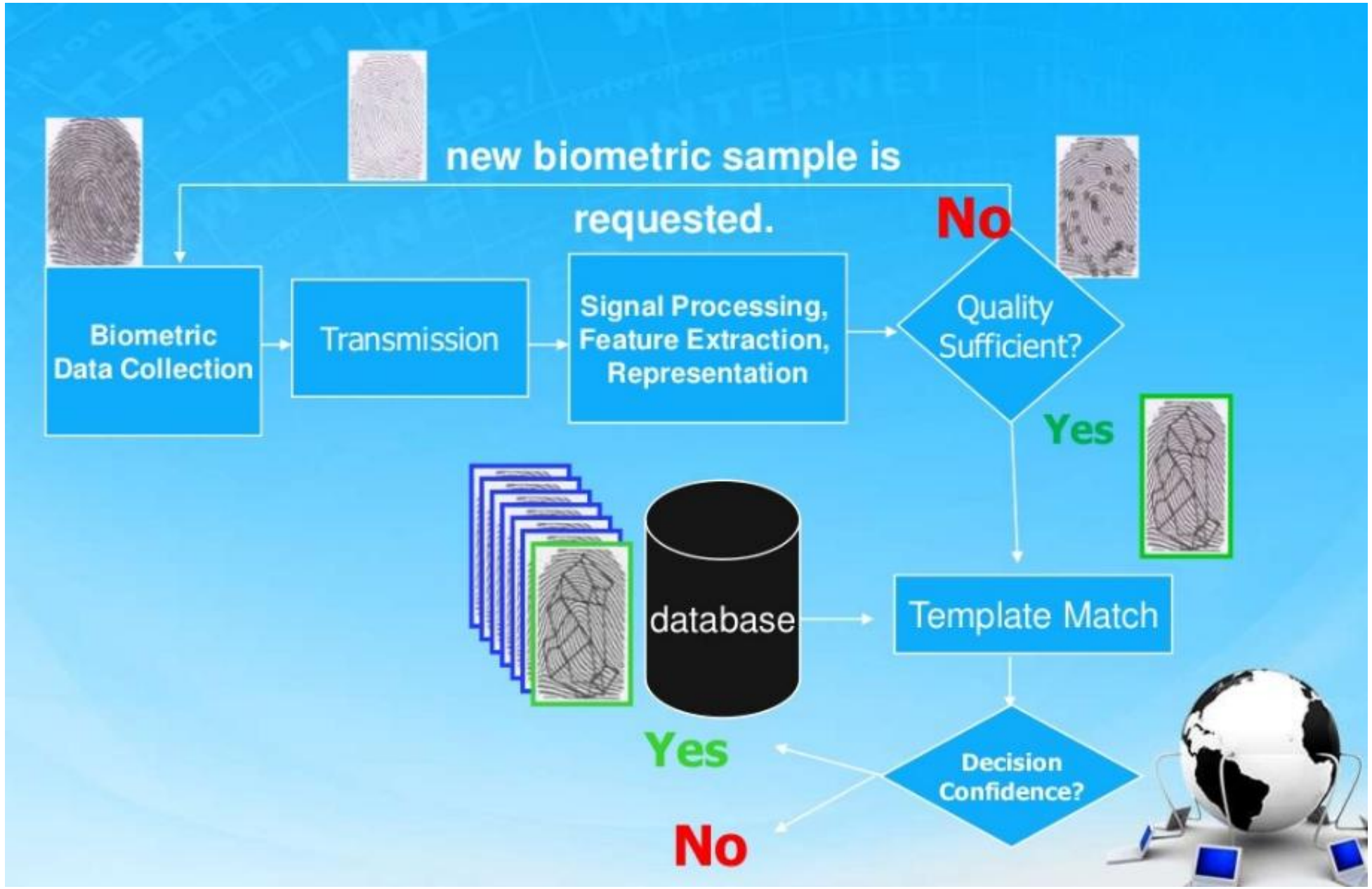
Strategies for strong passwords

- Proactive password checking
  - Users select a potential password which is tested
  - Weak passwords are not accepted
- Reactive password checking
  - SysAdmin periodically runs password cracking tools to detect weak passwords that must be replaced
- Computer-generated passwords
  - Random passwords are strong but difficult to remember

Something you are/do
(Inherence-based)

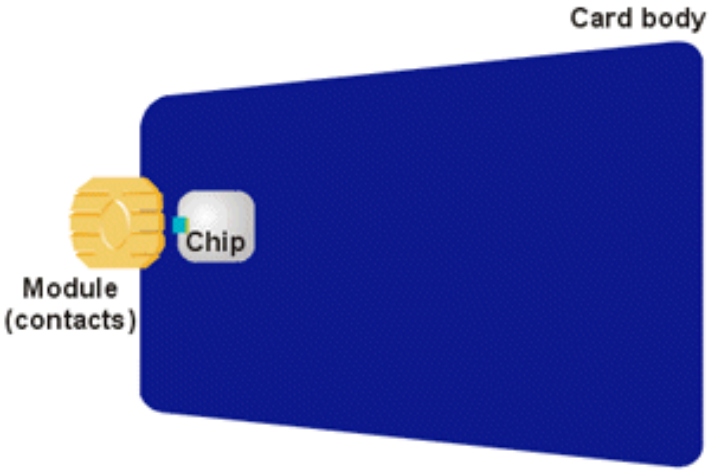
- Biometric - **"You are your key"**
- Examples:
  - Fingerprint
  - Handwritten signature
  - Facial recognition
  - Speech recognition
  - Iris
  - Voice
  - …




new biometric sample is requested.
No
Biometric Data Collection
Transmission
Signal Processing, Feature Extraction, Representation
Quality Sufficient?
Yes
database
Template Match
Yes
Decision Confidence?
No

Something you have *(Ownership-based)*

- **E-Token**: store credentials such as passwords, digital signatures and certificates, and private keys
- **RFID**: Integrated circuit(s) with an antenna that can respond to an RF signal with identity information
- **Smart card**
- **Digital Certificates** (used by Websites to authenticate themselves to customers)

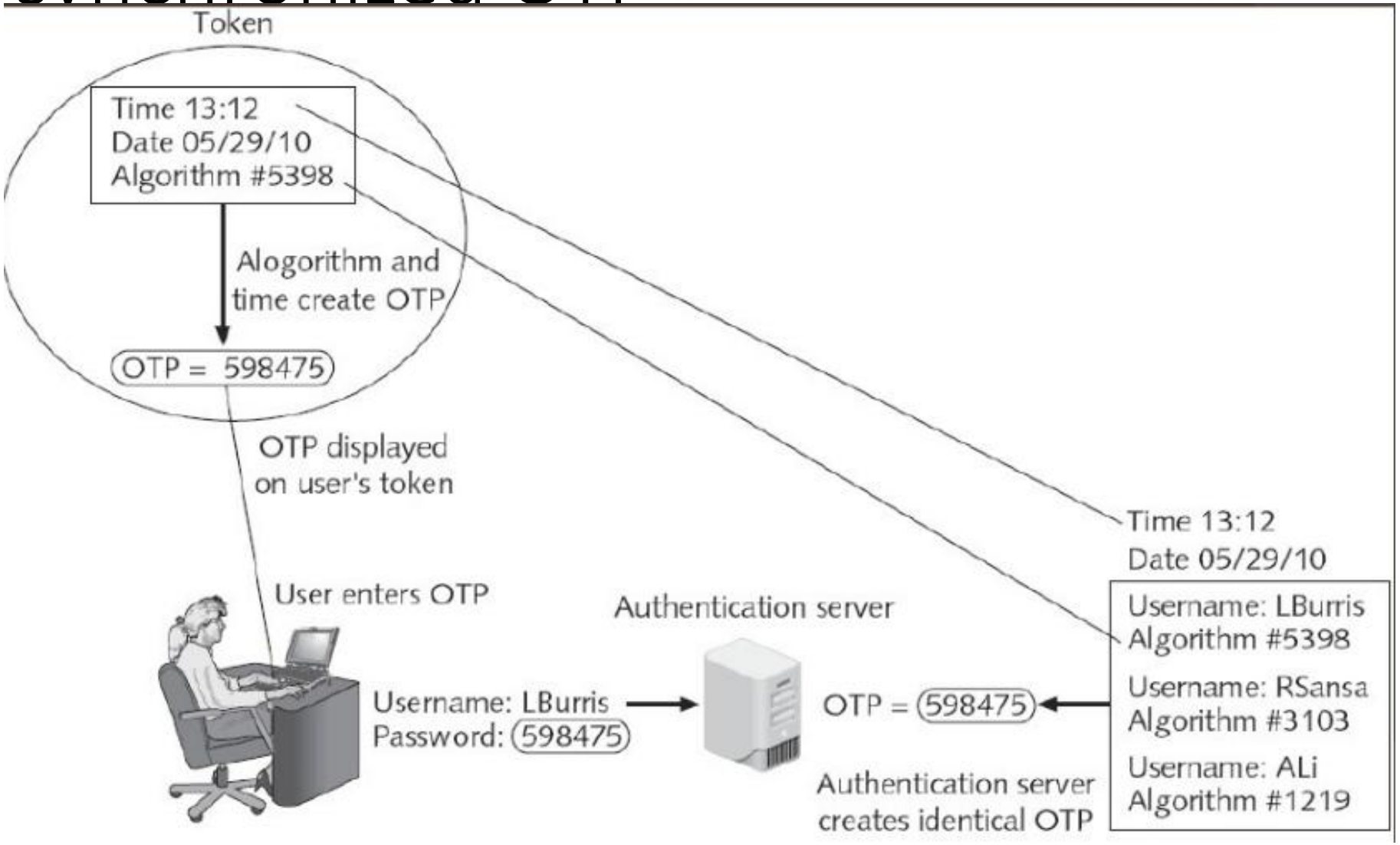


Source: Gemplus - All About Smart Cards

One Time Password

- Dynamic password that change frequently
- Systems using OTPs generate a unique password on demand that is not reusable

Time-synchronized OTP



Challenge-based OTP

- Authentication server displays a challenge (a random number) to the user
- User then enters the challenge number into the token (executes a special algorithm to generate a password)
- Because the authentication server has the same algorithm, it can also generate the password and compare it against that entered by the user.

Single Sign On

- Multiple applications, each requires login
- Provide users with the ability to login only once for usability
- Automatically propagate login to all applications

Single Sign On

- Advantages
  - Unified mechanism
  - One login/password to remember
  - New applications reuse code
- Disadvantages
  - Can weaken security
- Example: OIDC, SAML

Implementing authentication

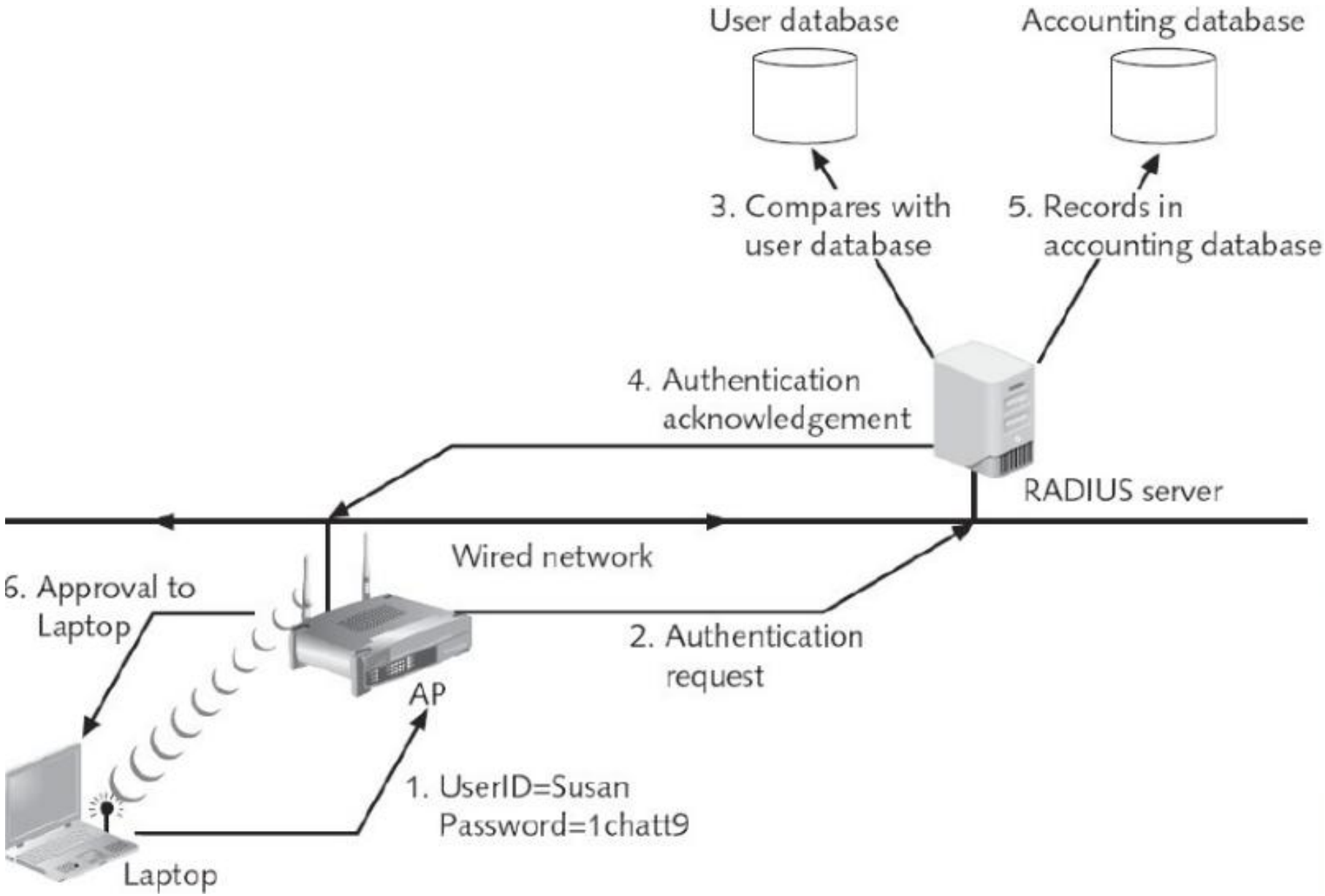
- Local authentication
- Network authentication

Authentication Server

- Radius
- Kerberos
- TACACS+
- LDAP

RADIUS

- Wired and Wireless LANs
- Radius clients: server, switch, AP
- Radius server authenticates and authorized the radius client requests


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgement
RADIUS server
Wired network
6. Approval to Laptop
2. Authentication request
AP
1. UserID=Susan Password=1chatt9
Laptop

Authorization

- Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.
- Grating access rights to subjects should be based on the level of trust a company has in a subject and the subject's need to know.
- Is a core component and established whether a user is authorized to access a particular resource and what actions he is permitted to perform on the resource.

Subjects, Objects, and Access Rights

- A subject is an entity capable of accessing objects
  - Owner: This may be the creator of a resource, such as a file. For system resources, ownership may belong to a system administrator. For project resources, a project administrator or leader may be assigned ownership.
  - Group: In addition to the privileges assigned to an owner, a named group of users may 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.

Subjects, Objects, and Access Rights

- An object is a resource to which access is controlled.
- access right describes the way in which a subject may access an object. Access rights could include the following:
  - Read
  - Write
  - Execute
  - Delete
  - Create
  - Search

Access Control models

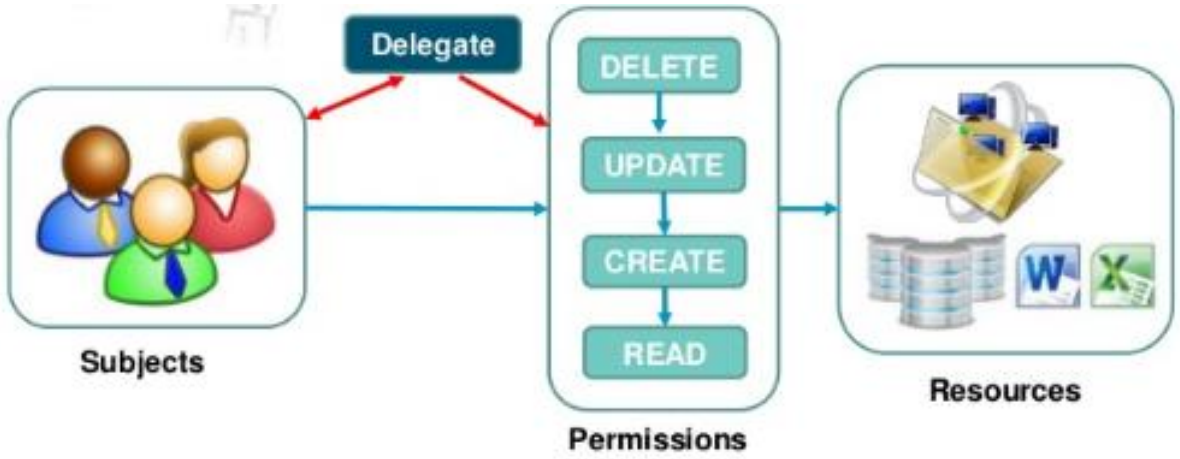
- How does someone grant the right level of permission to an individual so that they can perform their duties? Access control models define how permissions are assigned.
- Access control model – hardware and software predefined *framework* that custodian can use for controlling access
- Access control models have four flavors:
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-Based access control
  - Rule-Based access control
  - Attribute-based access control

Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.

Mandatory Access Control (MAC)

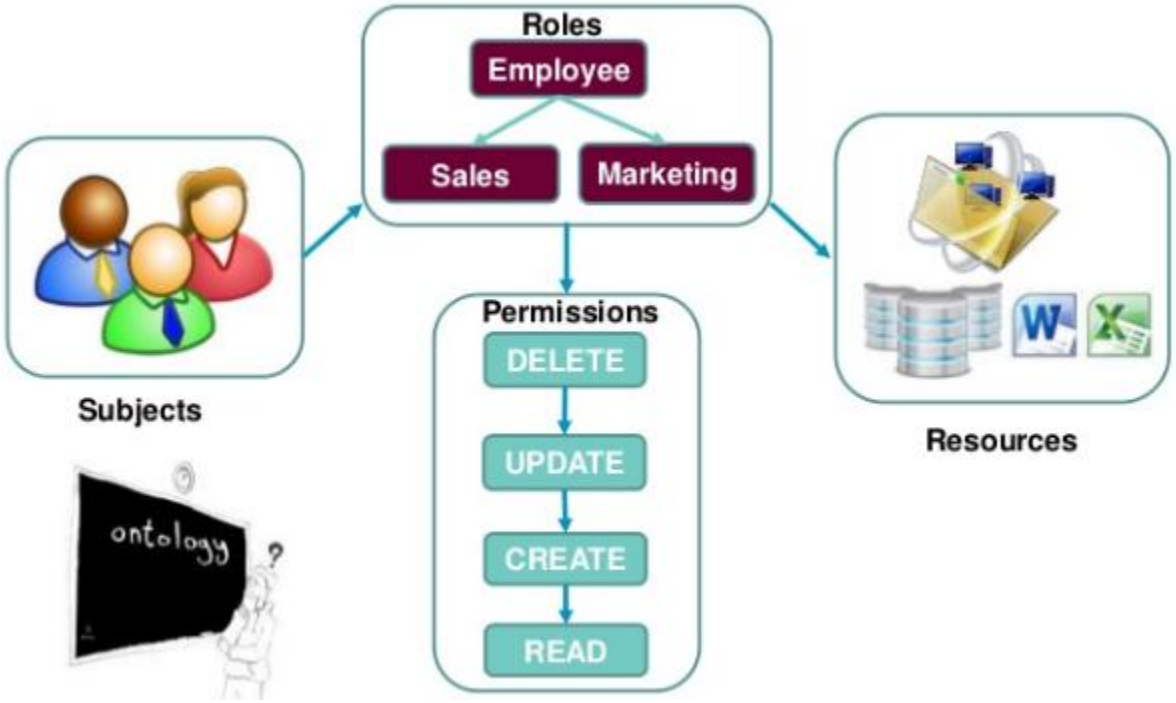
- This is a security model in which access rights are regulated by a central authority based on multiple levels of security.
- This means the end user has no control over any settings that provide any privileges to anyone.

Discretionary Access Control (DAC)

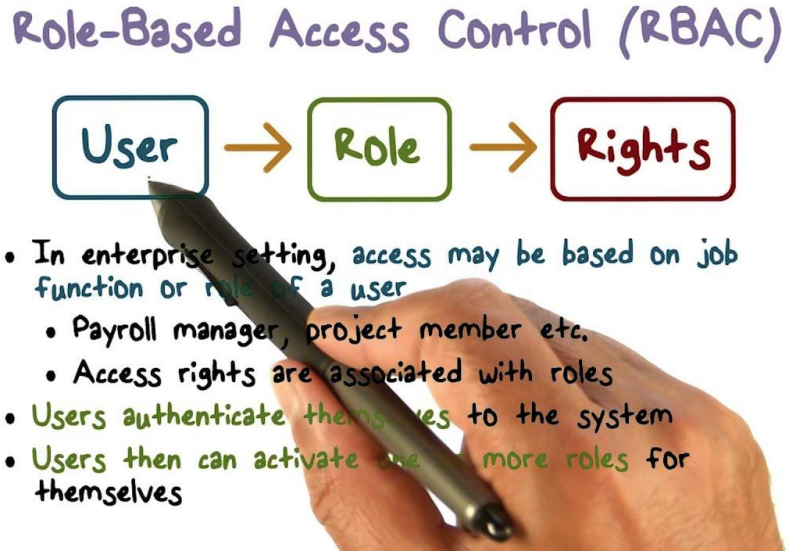


- DAC allows an individual complete control over any objects they own along with the programs associated with those objects.

Role-Based Access Control (RBAC)



- Provides access control based on the position an individual fills in an organization.



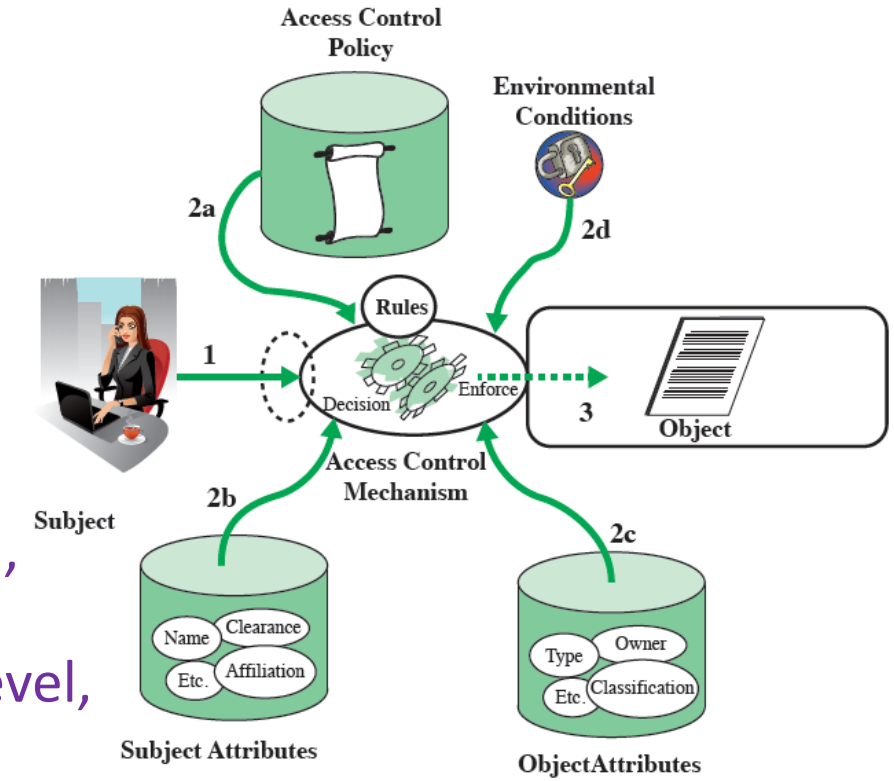
- Restricts access to computer resources based on individuals or groups with defined business functions.

Rule-Based Access Control

- This is a security model in which the system administrator defines the rules that govern access to resource objects.
- These rules are based on conditions, such as time of day or location.
- For example: if someone is only allowed access to files during certain hours of the day, Rule-Based Access Control would be the tool of choice.

Attribute-based Access Control (ABAC)

- Define authorizations that express conditions on properties of both the resource and the subject
- Types of attributes
  - Subject attributes: Name, Organization, Job title
  - Object attributes: Title, Author, Date
  - Environment attributes: Describe the operational, technical, and even situational environment or context in which the information access occurs: Current date, Network security level, Current virus/hacker activities



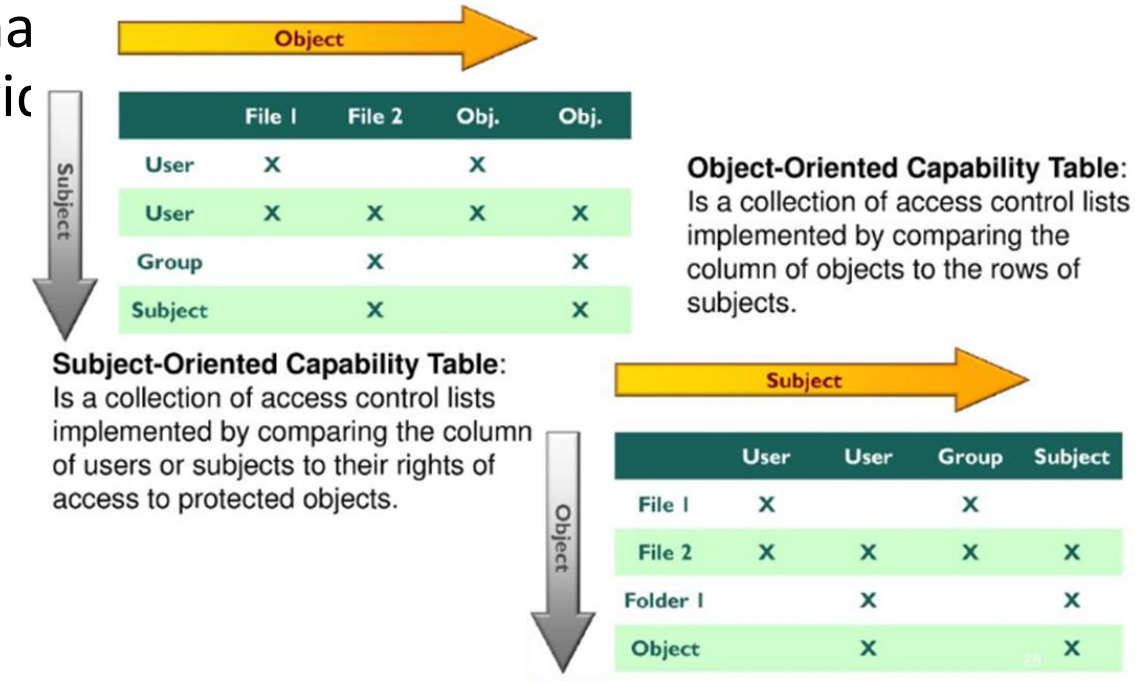
Implementing Access Control

- Access control is a process that is integrated into an organization's IT environment. It can involve identity management and access management systems.
- These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.
- When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.
- Access control requirement: **least privilege**

Access Control Matrix

- Is a table of subjects and objects indicating wha actions individual subjects can take upon indivic objects

- Two types:
  - Capability table (bound to a subject)
  - Access control List (bound to an object)



Ex1: Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it.

a. Create the corresponding access control matrix.

	alicerc	bobrc	cyndyrc
Alice	--xo	r---	----
Bob	r---	--xo	----
Cyndy	r---	rw--	rwxo

b. Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix.

	alicerc	bobrc	cyndyrc
Alice	--xo	r---	r---
Bob	----	--xo	----
Cyndy	r---	rw--	rwxo

Ex2: Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z

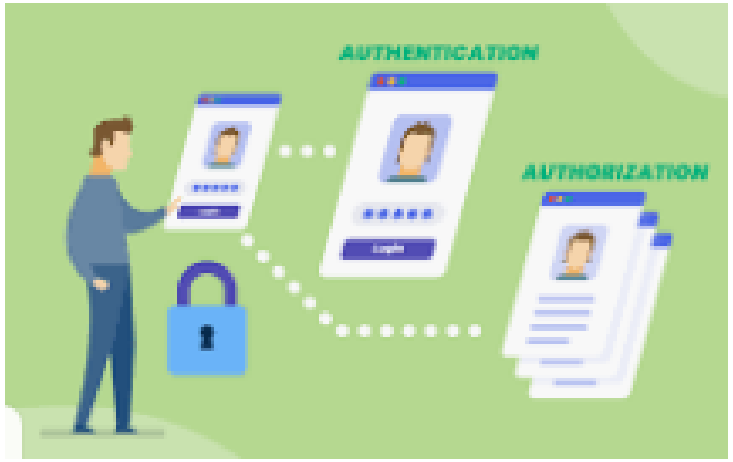
a) Write a set of **access control lists** for this situation. Which list is associated with which file?
b) Write a set of **capability lists** for this situation. With what is each list associated?

Set of access control lists. They are object focused so each list is associated with a file.
ACL(FileX) = Alice: {read, write}, Bob: {read}
ACL(FileY) = Alice: {read}, Bob: {read, write}
ACL(FileZ) = Alice: {execute}, Bob: {}

Set of capability lists. They are subject focused, so each list is associated with a user.
CList(Alice) = FileX: {read, write}, FileY: {read}, FileZ: {execute}
CList(Bob) = FileX: {read}, FileY: {read, write}, FileZ: {}

Authorization

- **Problems in controlling access to assess:**
  - Different levels of users with different levels of access
  - Resources may be classified differently
  - Diverse identity of data
  - Corporate environments keep changing



- **Solutions that enterprise wide and single sign on solutions**
  - User provisioning
  - Password synchronization and reset
  - Centralized auditing and reporting
  - Integrated workflow (increase in productivity)
  - Regulatory compliance

Identity, Credential, and Access Management

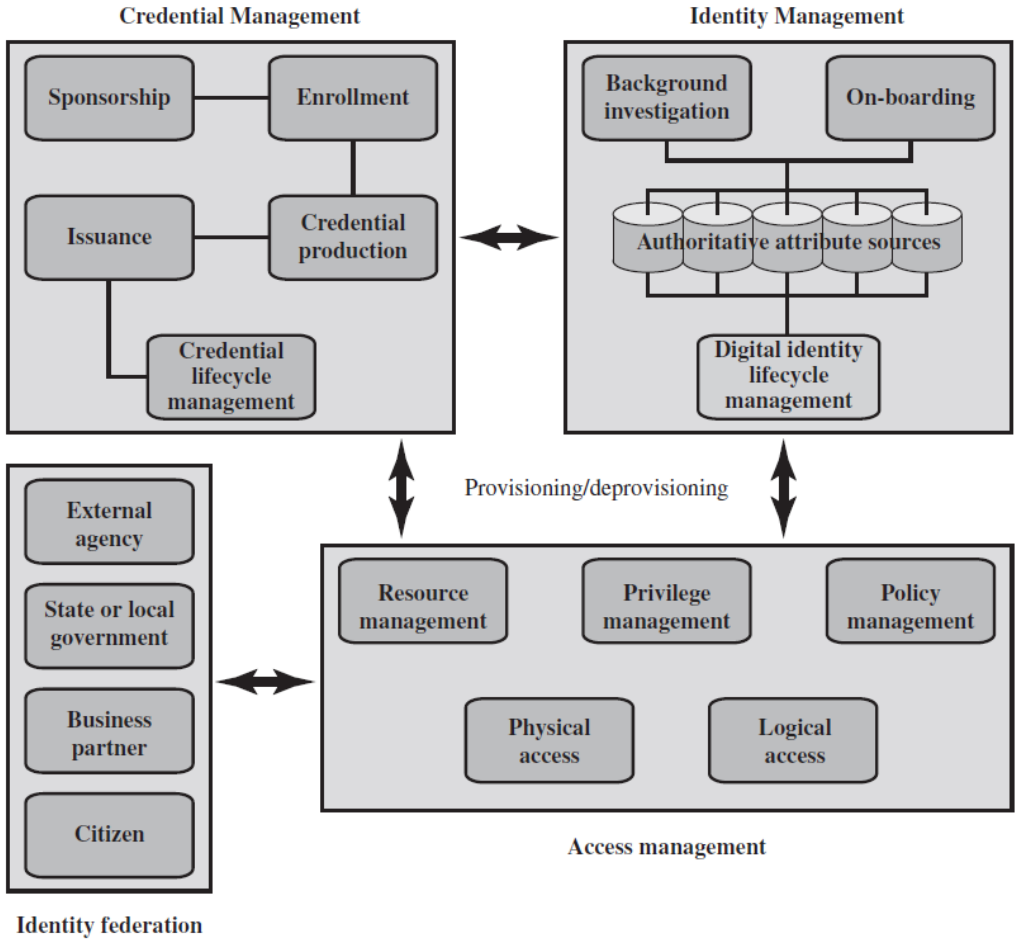


Figure 4.12 **Identity, Credential, and Access Management (ICAM)**

IdentityManagement

- Identity management is concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE.
- A final element of identity management is lifecycle management, which includes the following:
  - 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 Manager

- a credential is an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a subscriber
- Credential management is the management of the life cycle of the credential.
    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. This step may also involve incorporating authoritative attribute data, maintained by the identity management component.
    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.

Access Manager

- The access management component deals with the management and control of the ways entities are granted access to resources.
  - Resource management: This element is concerned with defining rules for a resource that requires access control.
  - Privilege management: This element is concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual’s access profile.
  - Policy management: This element governs what is allowable and unallowable in an access transaction.

Identity Federation

- Identity federation addresses two questions:
  - How do you trust identities of individuals from external organizations who need access to your systems?
  - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations?