İTÜ

Computer Security

User Authentication and Access Control

Dr. Şerif Bahtiyar

bahtiyars@itu.edu.tr

Fall 2015

Before Starting

JP Morgan sees 76 million customer accounts hacked

http://www.bbc.com/news/business-29470381

Before Starting

Sony Pictures Entertainment hack

https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

Outline

- User Authentication (chapter 3)
- Access Control (chapter 4)

User Authentication

- Basics of Authentication
- Password-Based Authentication
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Some Attacks on Authentication Systems

User Authentication

- Authentication is the binding of an identity to a principal.
  - Message authentication is a procedure that allows communicating parties to verify that received or stored messages are authentic.
  - User authentication is the process of verifying an identity claimed by or for a system entity. (RFC2828)

- User authentication is the fundamental building block and the primary line of defense.

User Authentication

Steps of an authentication process:

- Identification: specify identifier

- Verification: bind the entity and the identifier

User Authentication

- Four means of user authentication based on individual:
  - Knows: password, PIN
  - Possesses (token): electronic keycards, smart cards, physical keys
  - Is (static biometrics): fingerprint, retina, face
  - Does (dynamic biometrics): voice pattern, handwriting characteristic
  - Location

- Each of these methods has problems.

User Authentication (Password Based)

- Widely used user authentication method
  - User provides name and password
  - System compares name and password

- Authenticate identifier (ID) of user logging
  - User is authorized to access system
  - Determines user's privileges

User Authentication (Password Based)

Vulnerabilities of passwords and counter measures-1

- Offline dictionary attack – prevent unauthorized access to the password file, IDS measures
- Specific account attack – account lockout mechanism

- Popular password attack – policies, scanning IP address and cookies
- Password guessing against single user – training and enforcement of policies

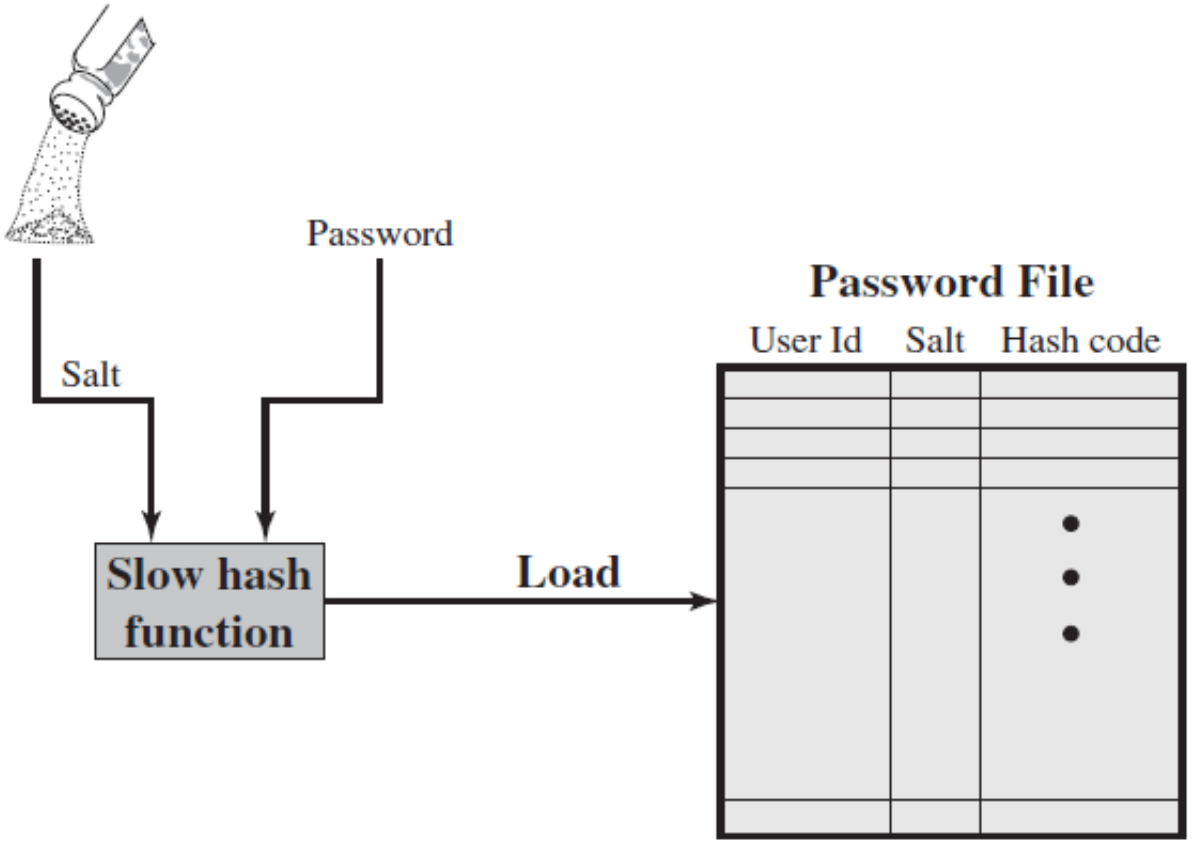
User Authentication (Password Based)

Vulnerabilities of passwords and countermeasures-2

- Workstation hijacking - IDS
- Exploiting user mistakes – training, IDS, combined with other means
- Exploiting multiple password use – policy
- Electronic monitoring – encrypted links

User Authentication (Password Based)

Hash based authentication: Loading a new password



(a) Loading a new password

User Authentication (Password Based)

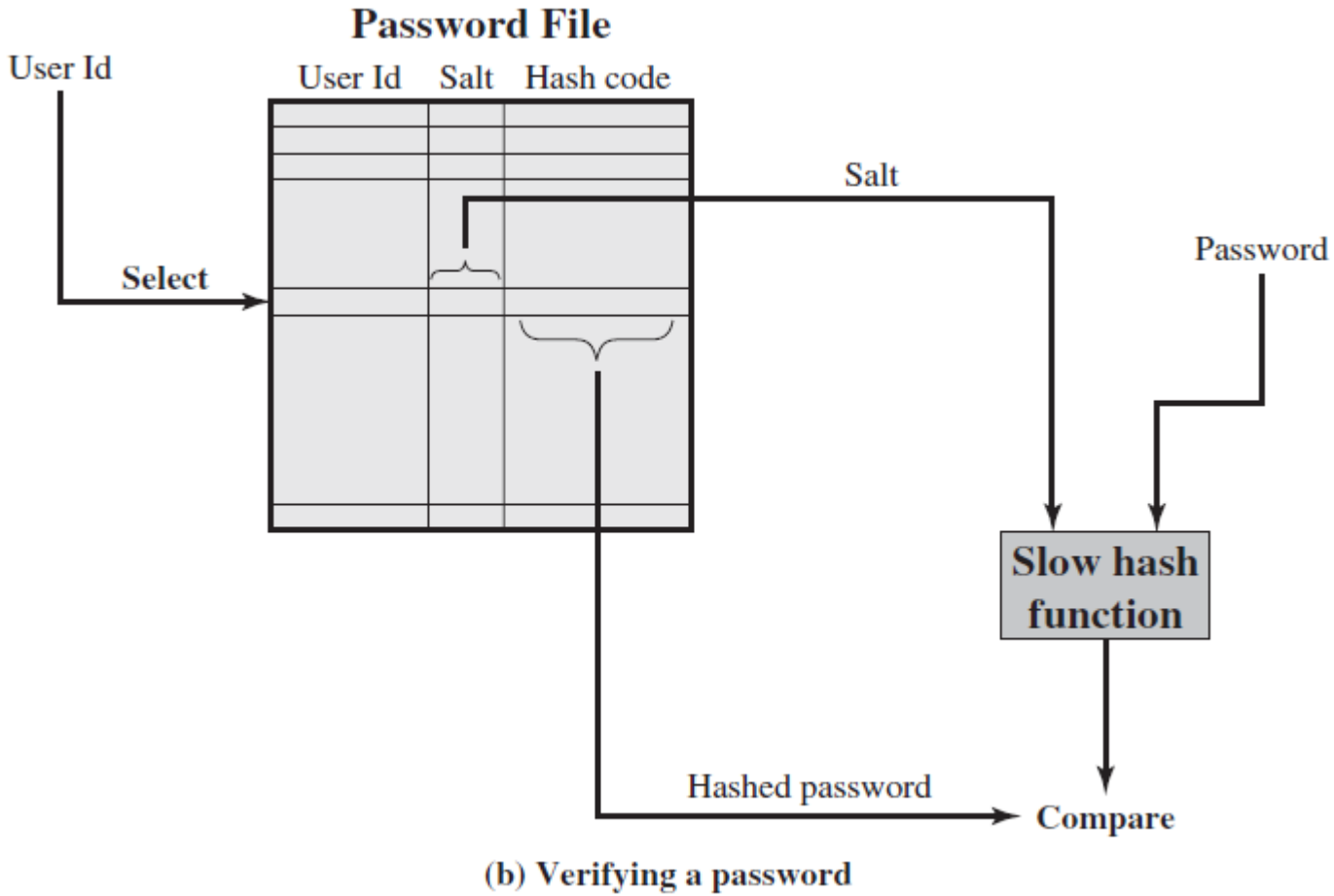
Salt and Its Benefits

Salt: A fixed-length value.

- Prevent duplicate password in the password file
- Increase the difficulty of offline dictionary attack
- Nearly impossible to find out the same password in many systems for a specific user

User Authentication (Password Based)

Hash based authentication: Verifying a password



(b) Verifying a password

User Authentication (Password Based)

Password cracking

- Dictionary attacks : try each word then obvious variants in large dictionary against hash in password file
- Rainbow table attacks
  - Pre-compute tables of hash values
  - a table of hash values, hash chains
  - e.g. 1.4GB table cracks 99.9% of alphanumeric Windows passwords in 13.8 secs
  - not feasible if larger salt values used

User Authentication (Password Based)

Password selection strategies

- User education
- Computer generated passwords
- Reactive password checking: system periodically runs its password cracker to find guessable passwords.
- Proactive password checking: a user is allowed to select password if the password complies with system requirements at the time of selection.

User Authentication (Token Based)

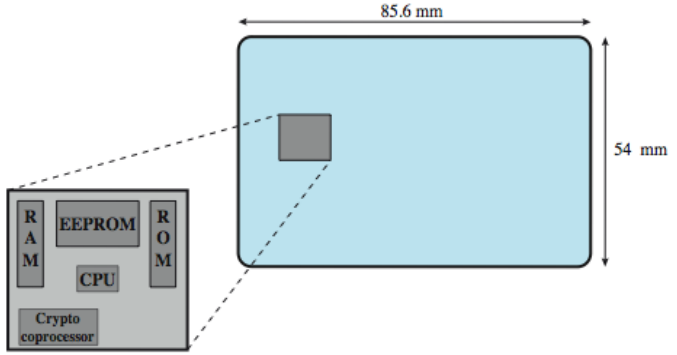
Objects that a user possesses for the purpose of user authentication are called tokens.

User Authentication (Token Based)

Some cards used as tokens

- Memory
  - Memory cards can store but not process data.
  - Store only a simple security code.

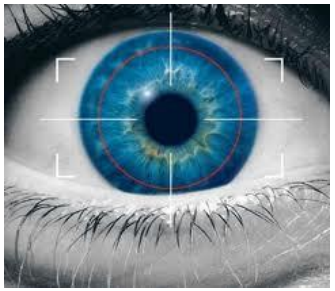
- Smart Card
  - Electronic memory and processor inside
  - Authentication protocol
    - Static
    - Dynamic password generator
    - Challenge-response

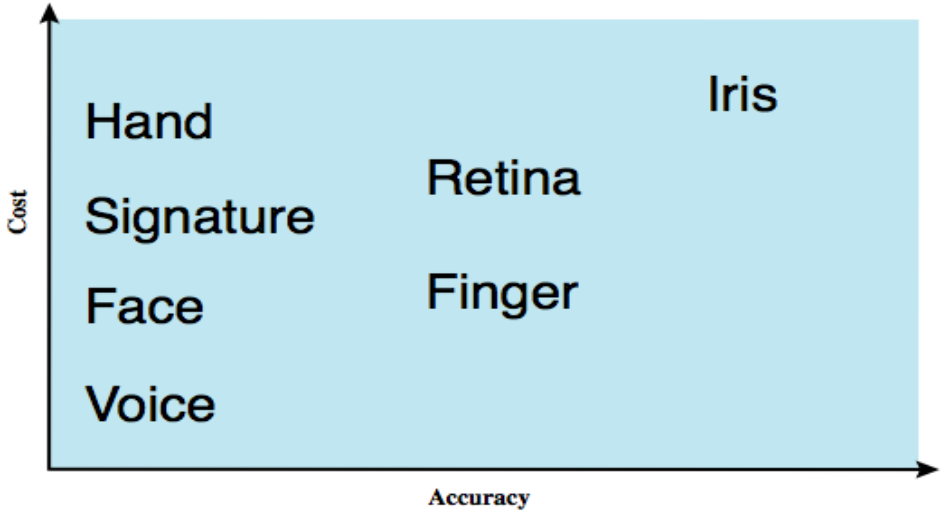


typical chip layout

User Authentication (Biometric Based)

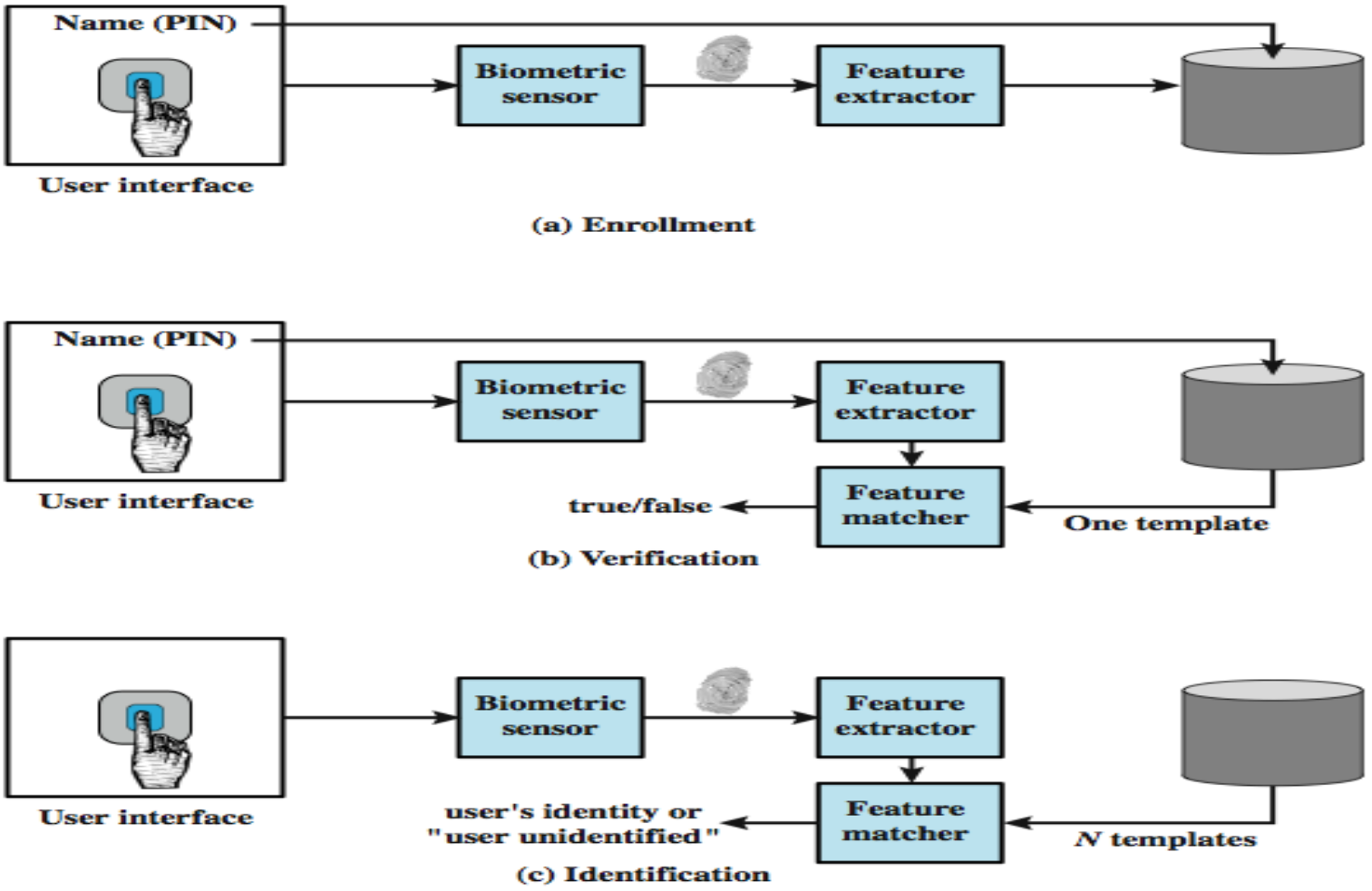
- Authenticates an individual based on one of its physical characteristic.
- Based on pattern recognition
- Technically complex and expensive





User Authentication (Biometric Based)

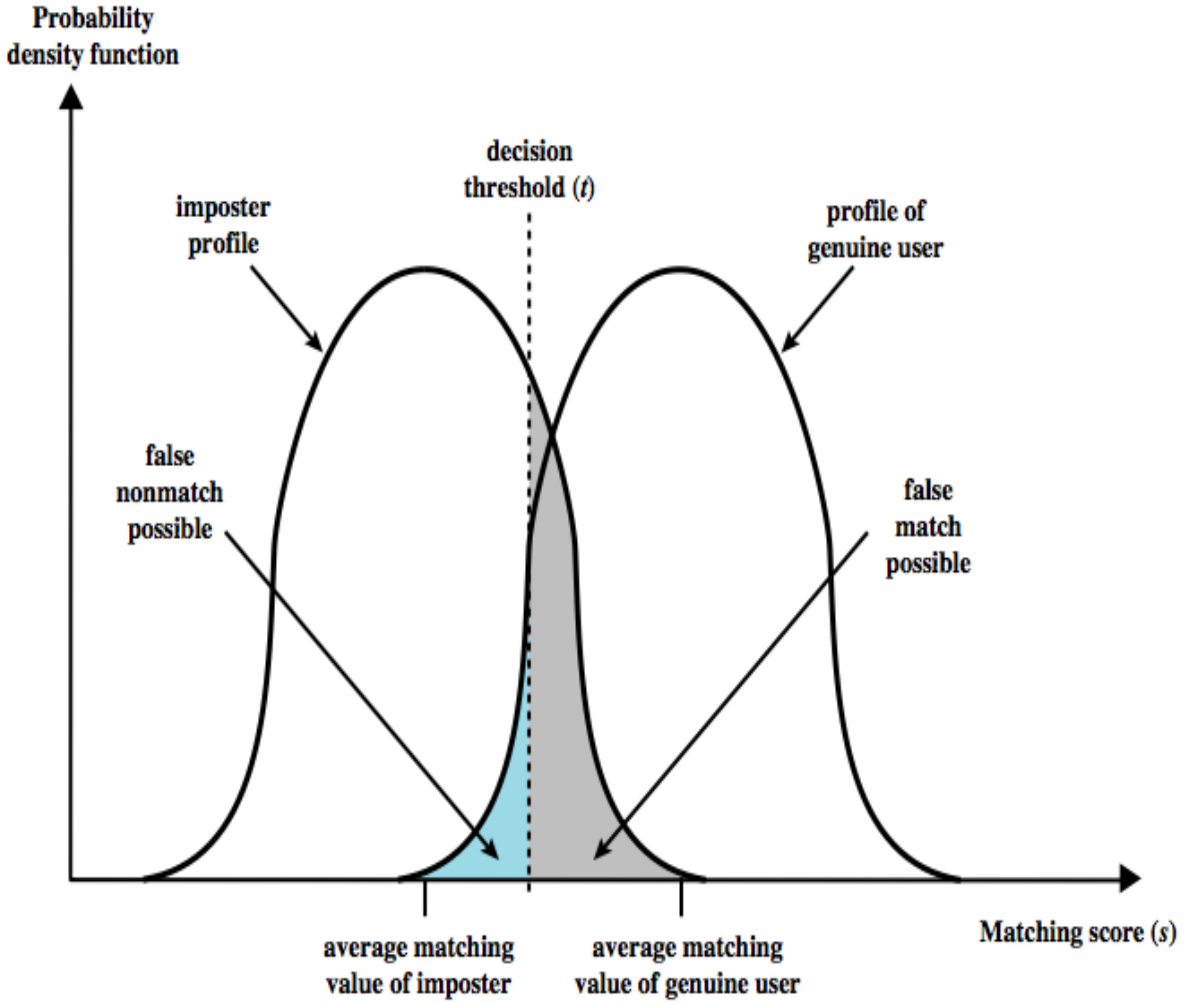
Operations



User Authentication (Biometric Based)

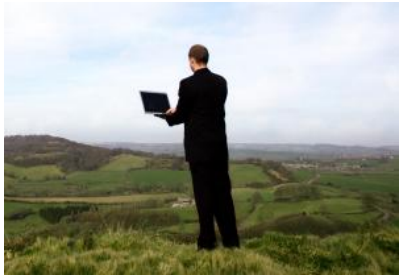
Accuracy

- never get identical templates
- problems of false match / false non-match



User Authentication (Remote User Authentication)

- Authentication over a network or communication link.
- Problems: complex, eavesdropping, replay



- Challenge-response protocol

1. User sends identity
2. Host responds with a random number
3. User computes f(r, h(P)) and sends back
4. Host compares values from user with own computed value, if mach user authenticated

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{r, h(), f()\}$	random number h(), f(), functions
P' password r', return of r	$f(r', h(P')) \rightarrow$	
	$\leftarrow$ yes/no	if $f(r', h(P')) = f(r, h(P(U)))$ then yes else no

(a) Protocol for a password

User Authentication (Some Attacks)

- Client attacks
  - Password guessing, exhaustive search for tokens,..
  - Limited attempts, large entropy,…
- Host attacks
  - Plaintext theft, passcode theft, template theft,..
  - Hashing, large entropy, protection of password database, OTP,..
- Eavesdropping
  - Shoulder surfing, theft, Copying (spoofing) biometric,..
  - Multifactor authentication, tamper resistant token, ..
- Replay, Trojan Horse, Denial-of-service, …

Access Control

- Definition of Access Control
- Access Control Functions, Policies, and Requirements
- Elements of Access Control
- Discretionary Access Control
- Role-Based Access Control

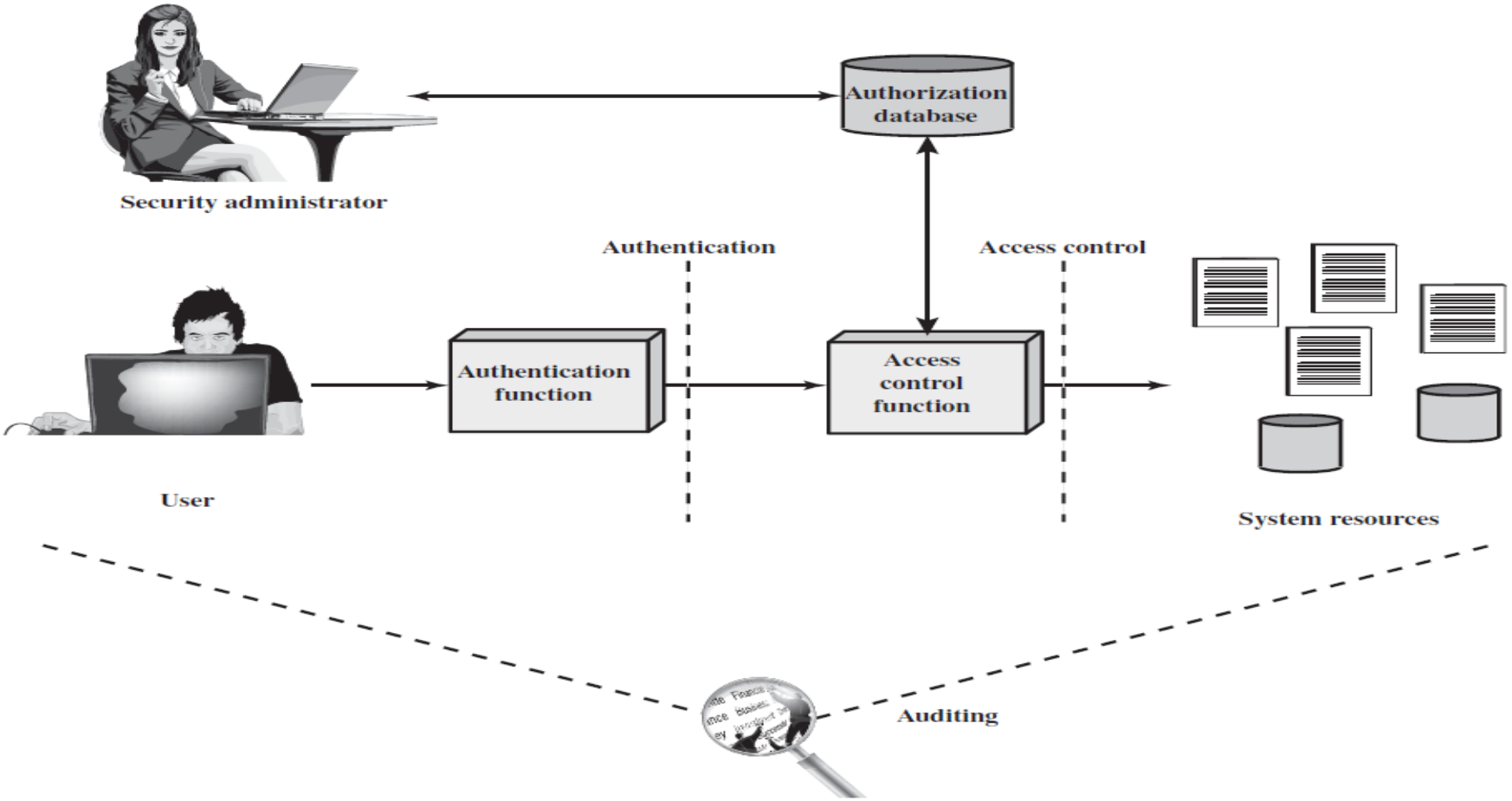
Access Control

- Access Control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

- Central element of computer security
- We consider user groups, not networked environment.
- All systems need access control.
- Access control mechanisms mediate between a user and system resources.

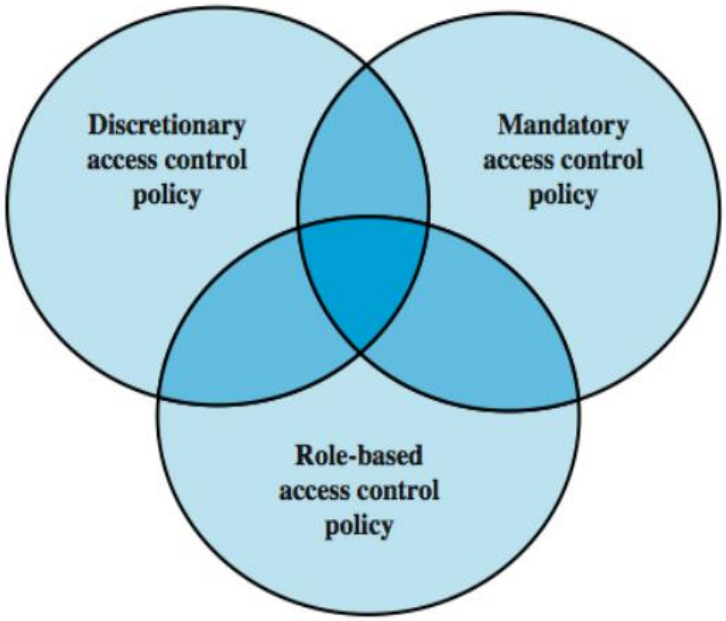
Access Control (Access control principles)

Authentication, Authorization, Audit



Access Control (Access control policies)

- Discretionary Access Control (DAC):
  - Access based on the identity of the requestor and on access rules
  - An entity may enable another entity to access resources
- Mandatory Access Control (MAC):
  - Access based on comparing security labels
  - An entity cannot enable another entity to access resources
- Role-Based Access Control (RBAC):
  - Access based on roles of users



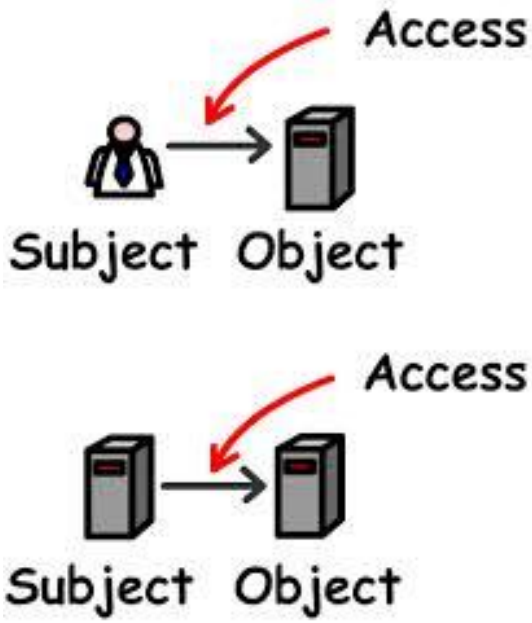
Access Control
(Access control requirements)

- Reliable input (authentication)
- Fine and coarse specifications
- Least privilege
- Separation of duty
- Open and closed policies
- Policy combinations, conflict resolution
- Administrative policies
- Dual control

Access Control (Access control elements)

Subject: is an entity capable of accessing objects.

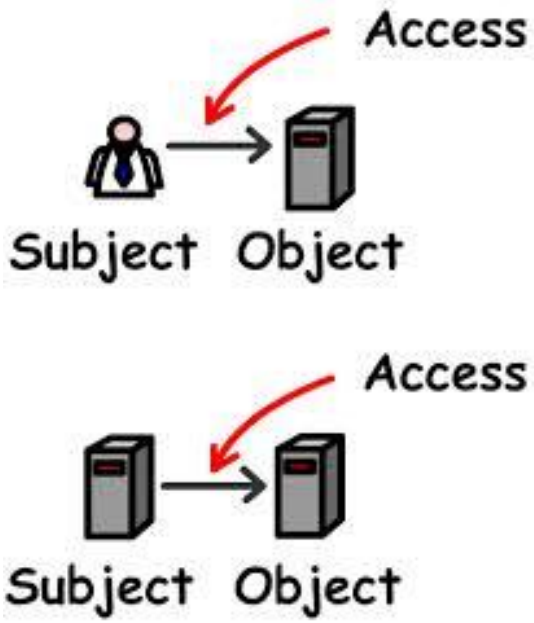
- A process representing user or application
- Often have three classes: owner, group, world



Access Control (Access control elements)

Object: a resource to which access is controlled.

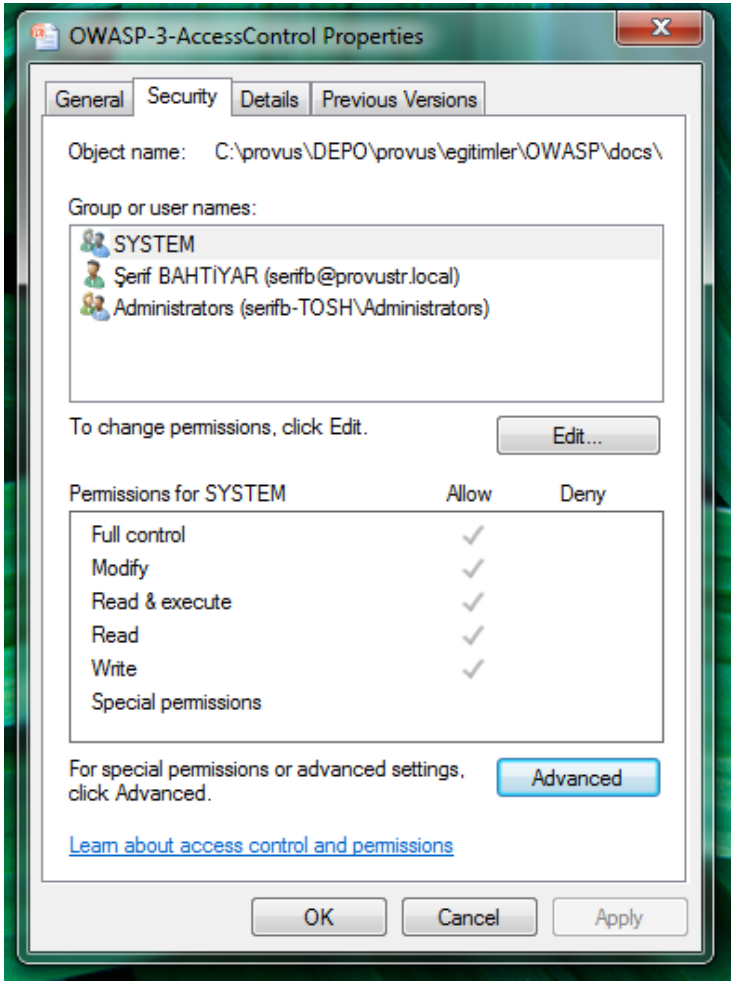
- Files, records, directories, programs, …
- Number and type depend on environment



Access Control (Access control elements)

Access right: describes the way in which a subject may access an object.

- Read, write, execute, delete, search, create



Access Control (Discretionary Access Control)

Generally provided with access control matrix

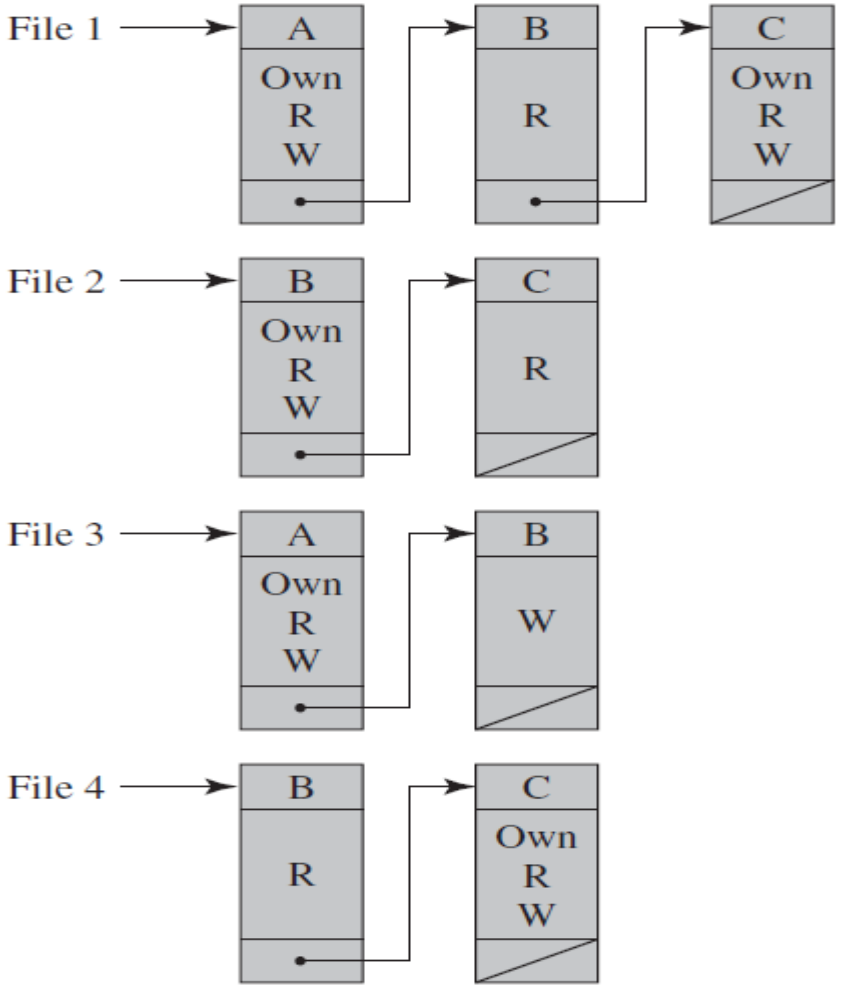
- lists subjects in one dimension (rows)
- lists objects in the other dimension (columns)
- each entry specifies access rights of the specified subject to object
- is often sparse

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

Access Control (Discretionary Access Control)

Access control list (ACL)

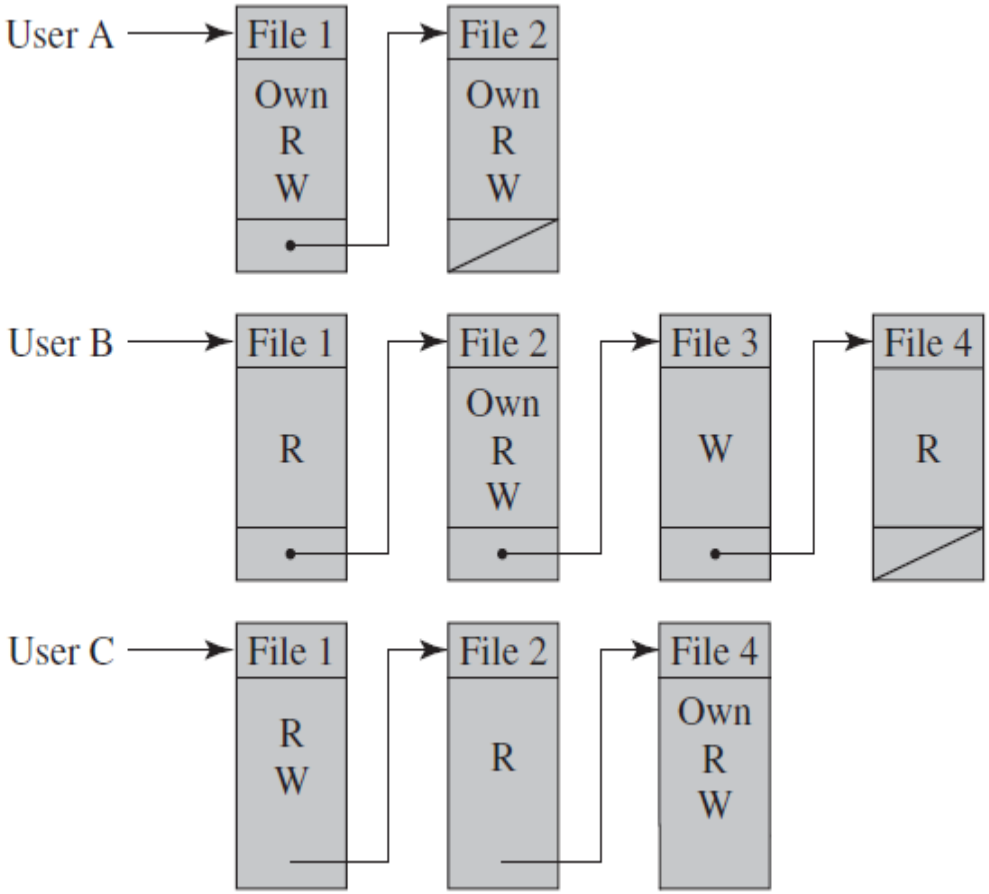
- Matrix decomposition by columns
- Convenient from subject side
- Inconvenient for determining access rights to a specific user



Access Control (Discretionary Access Control)

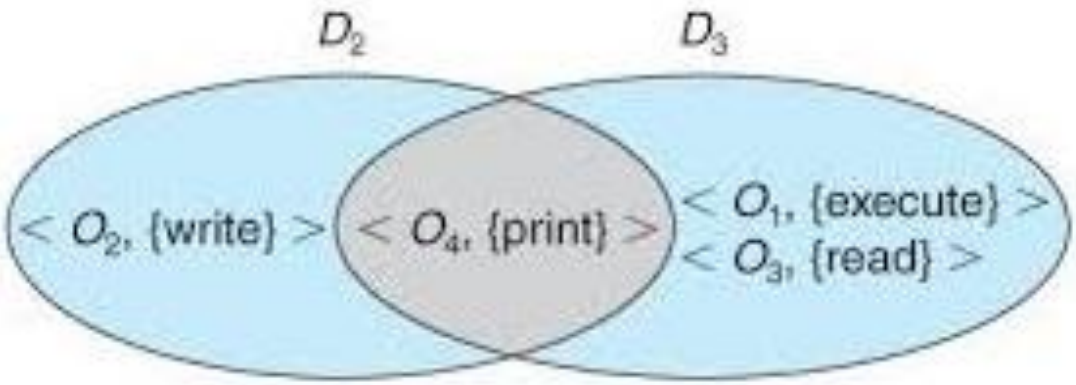
Capability tickets

- Matrix decomposition by rows
- Appropriate for use in distributed environment
- Convenient and inconvenient aspects are opposite of ACL

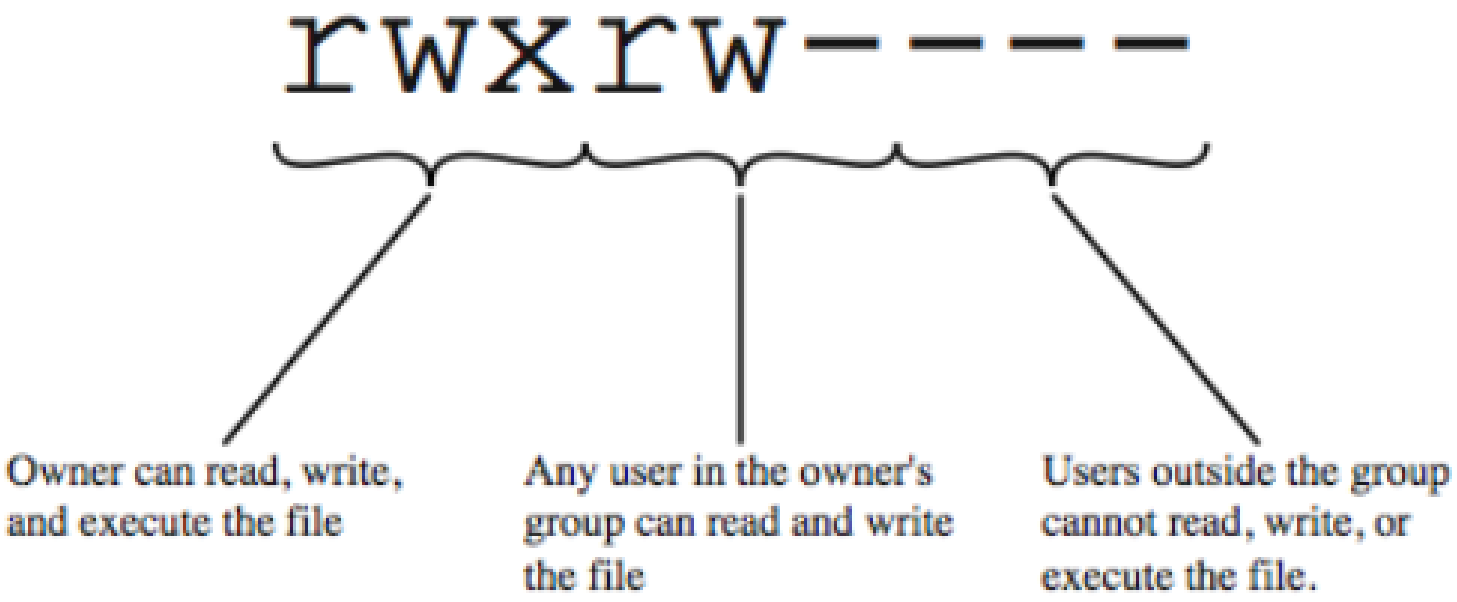


Access Control (Protection Domain)

- Set of objects with associated rights
- In access matrix view, each row is a protection domain
  - But not necessarily just a user
  - May a limited subset of user's access rights
  - Applied to a more restricted process
- May be static or dynamic

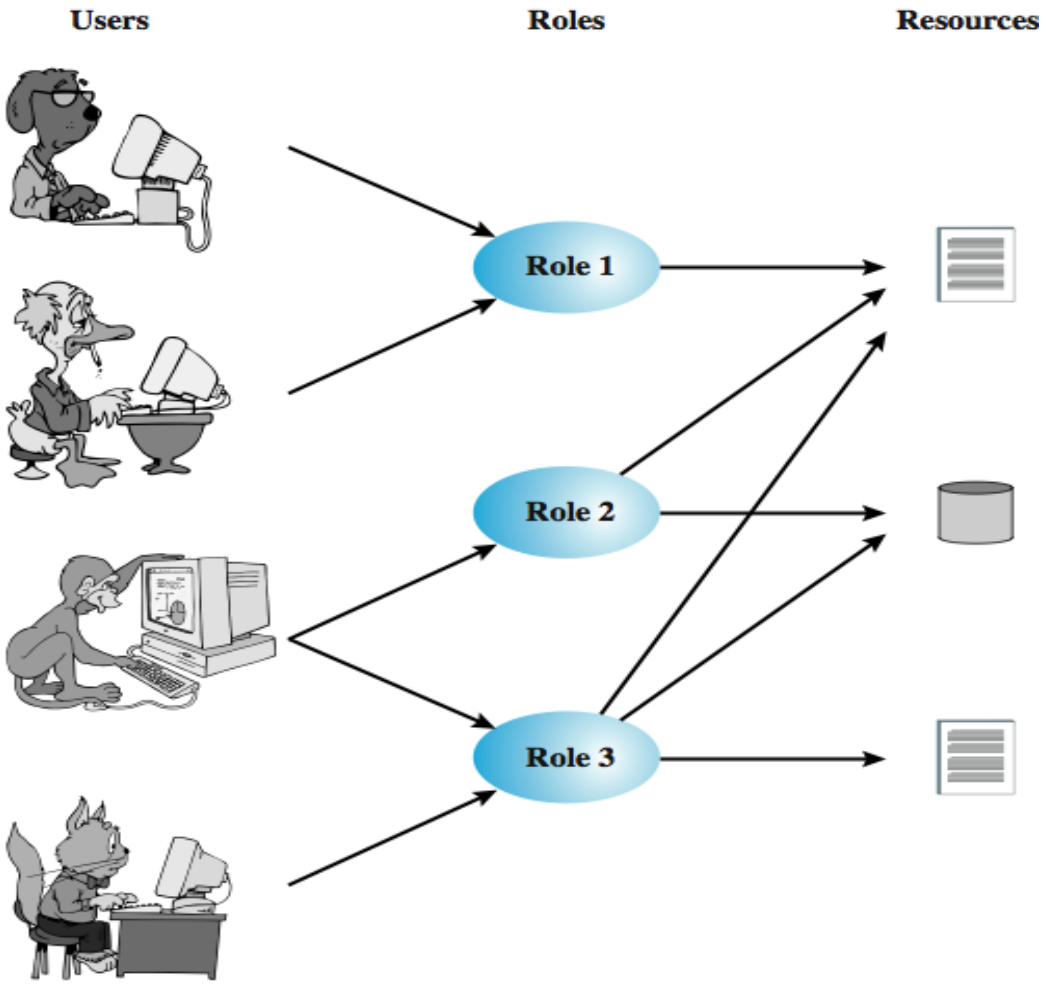


Access Control
(UNIX File Access Control)



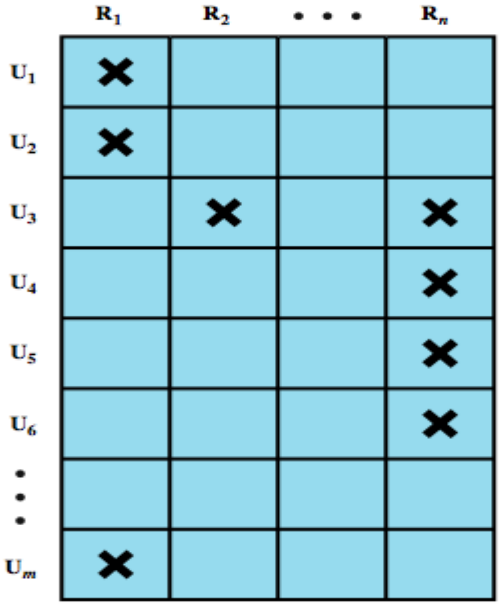
Access Control (Role-Based Access Control)

- Based on the roles that users assume in a system rather than the user's identity.
- Define a role as a job function within an organization.



Access Control (Role-Based Access Control)

- Assign access rights to roles instead of individual users.
- Users are assigned to different roles, either statically or dynamically, according to their responsibilities.

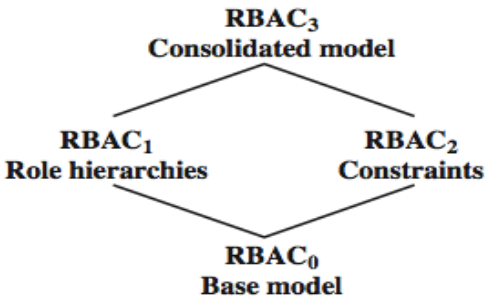


OBJECTS

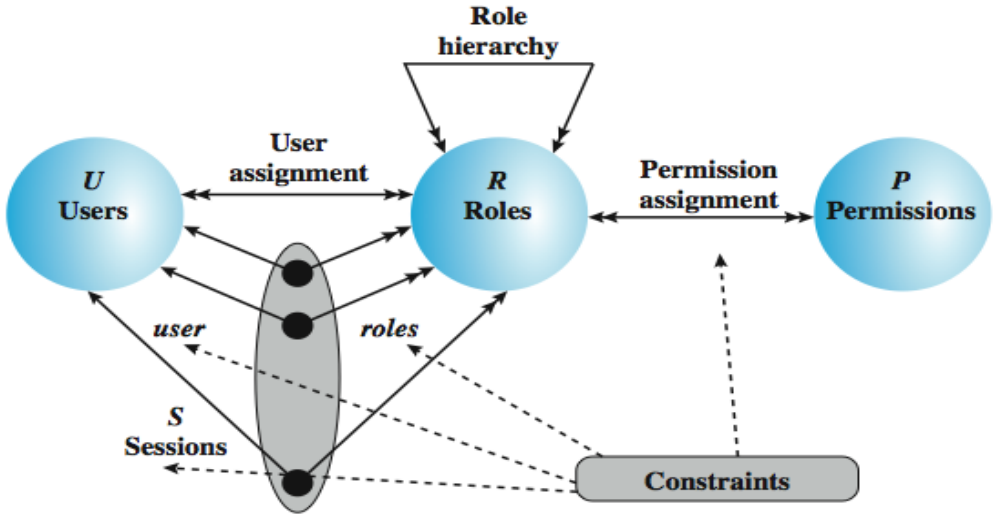
ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			

Access Control (Role-Based Access Control)

The many-to-many relationships between users and roles and between roles and permissions provide a flexibility and granularity of assignment not found in conventional DAC schemes.



(a) Relationship among RBAC models



(b) RBAC models

Summary

- Introduce user authentication
  - Password, Token, Biometrics
  - Remote user authentication
  - Security issues
- Introduce access control
  - Principles, policies, requirements
  - Elements: subject, object, access rights
  - DAC, MAC, RBAC