CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous *Class*

- Protection in General-Purpose Operating Systems
  - Segmentation and Paging
  - Dual Mode Protection
  - User Authentication

Present Class

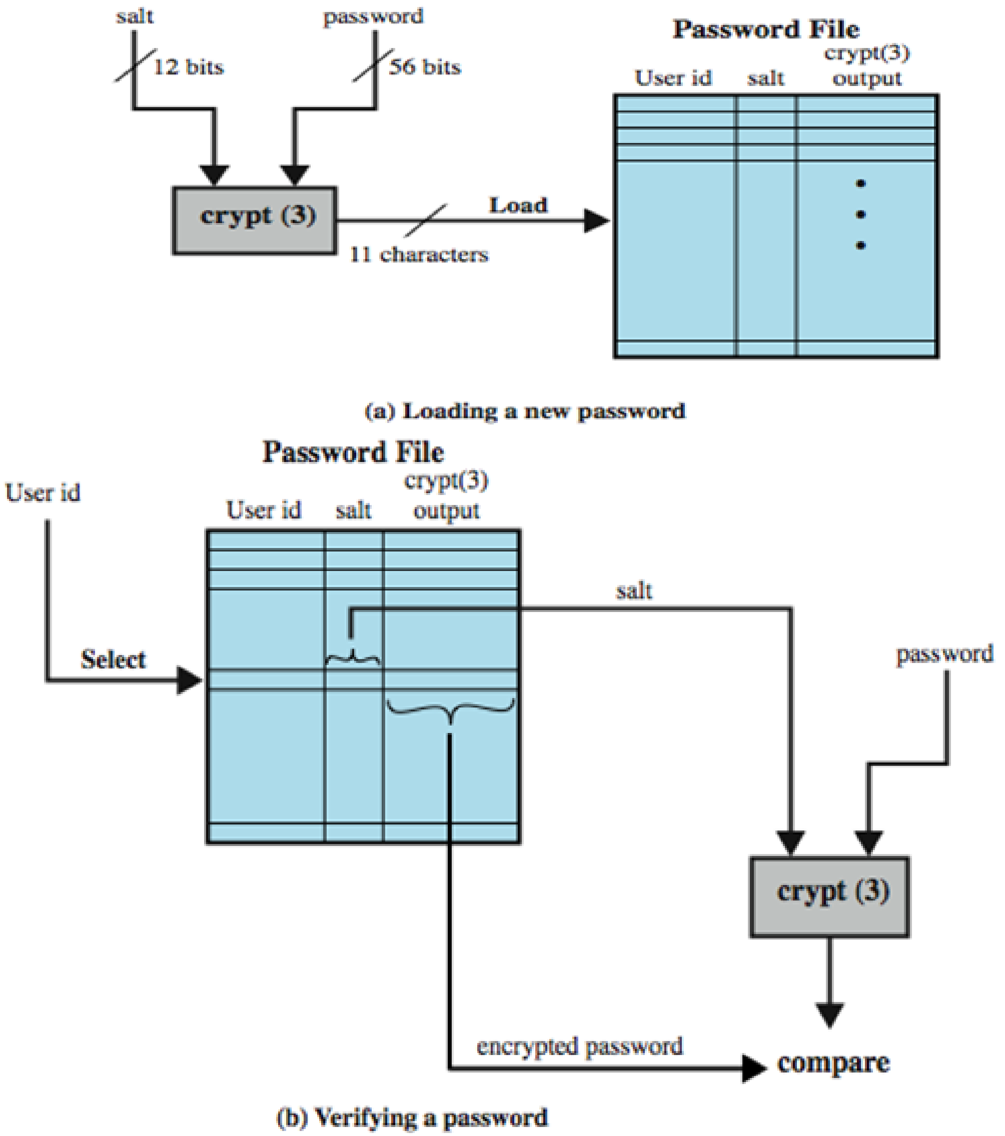
- Access Control
  - DAC
    - Linux File System
  - MAC

User Authentication

- Use of Hashed salt Passwords
  Prevents duplicate passwords

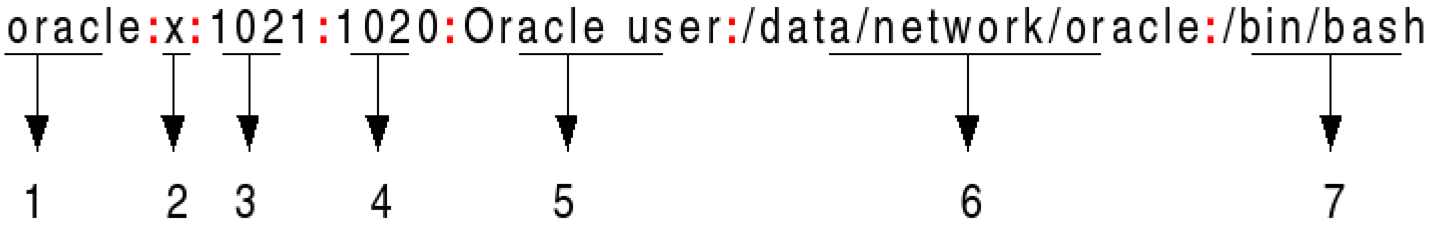
- Increases the difficulty of offline dictionary attacks.

- becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.



Linux password

- /etc/passwd



```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

  - Username, x, UID,GID, Full name, homeDirectory, Login shell
- $ sudo cat /etc/shadow/
- som:$6$ABCD1234$JnCx/.NCi4315V0AONxuVpUIRvPivoQjLzY0M28iYkOJU/FwVhXE4Me2f72fldvGEOpnTAB7IuVrsVfwpT/XT/:38478:0:99999:5:::
- username
- $6$ Algorithm used for hashing. 6 (sha-512)
- $ABCD1234$ string salt which is used for hashing..
- $JnCx/.NCi4315V0AON .....fwpT/XT/ Value after the third $ sign represents actual hashed password.
- password change date, expiry date etc. in colon (:)

Windows system

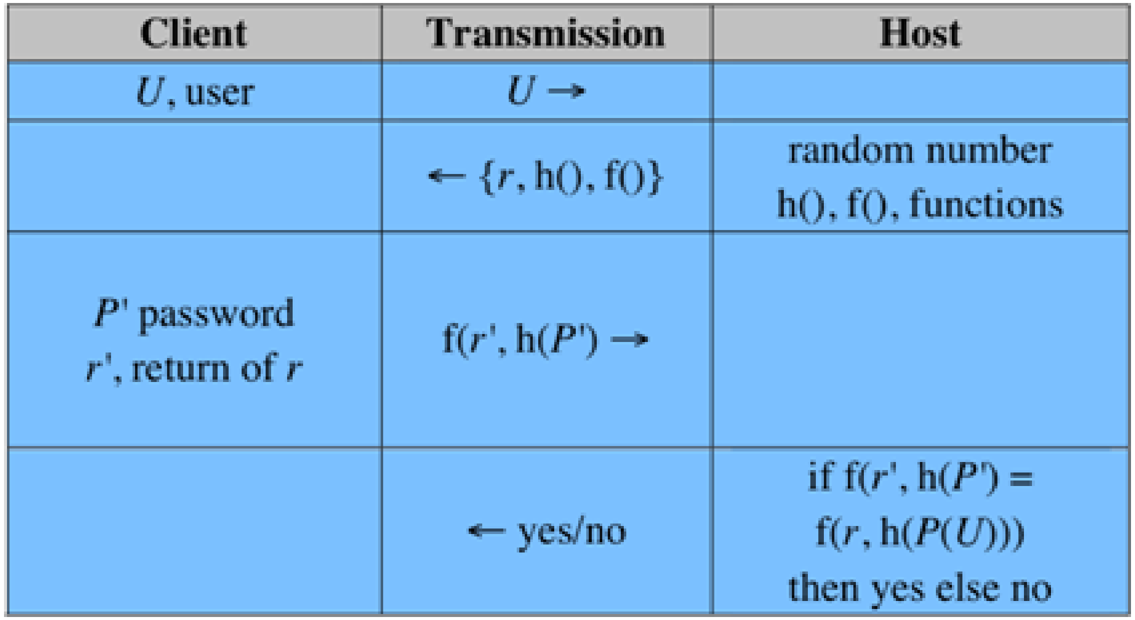
- password hashes are stored **Security Accounts Manager (SAM)** file,
  - C:\windows\\system32\\config\\SAM
  - not accessible to regular users while the operating system is running.
- Previous versions of Windows used **LAN Manager hash**, or **LM hash**,
  - Algorithm is based on DES
  - has some security weaknesses
- To avoid this weakness NTLM algorithm.
  - It uses MD4
  - It is a challenge-response protocol used for authentication by several Windows components.

Remote User Authentication

- authentication over a network, the Internet, or a communications link is more complex
  - additional security threats such as:
    - eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- generally rely on some form of a *challenge-response protocol* to counter threats

Password Protocol

- user transmits identity to remote host
- host generates a random number (nonce)
- nonce is returned to the user
- host stores a hash code of the password function in which the password hash is one of the arguments
- use of a random number helps defend against an adversary capturing the user's transmission

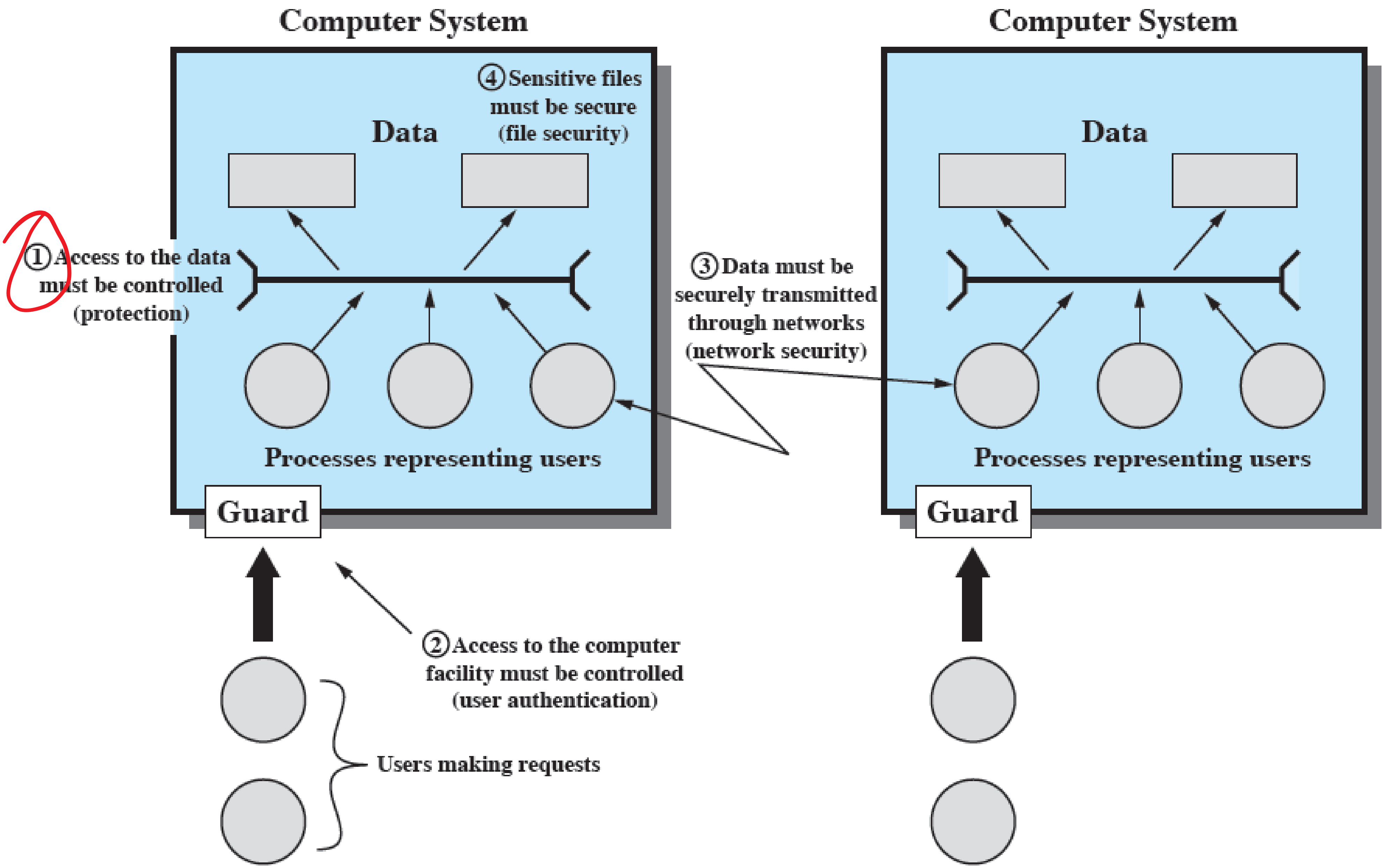


Client	Transmission	Host
U, user	U →	
	← {r, h(), f()}	random number h(), f(), functions
P' password r', return of r	f(r', h(P')) →	

	← yes/no	if f(r', h(P')) =
		f(r, h($P(U)$))
		then yes else no

(a) Protocol for a password

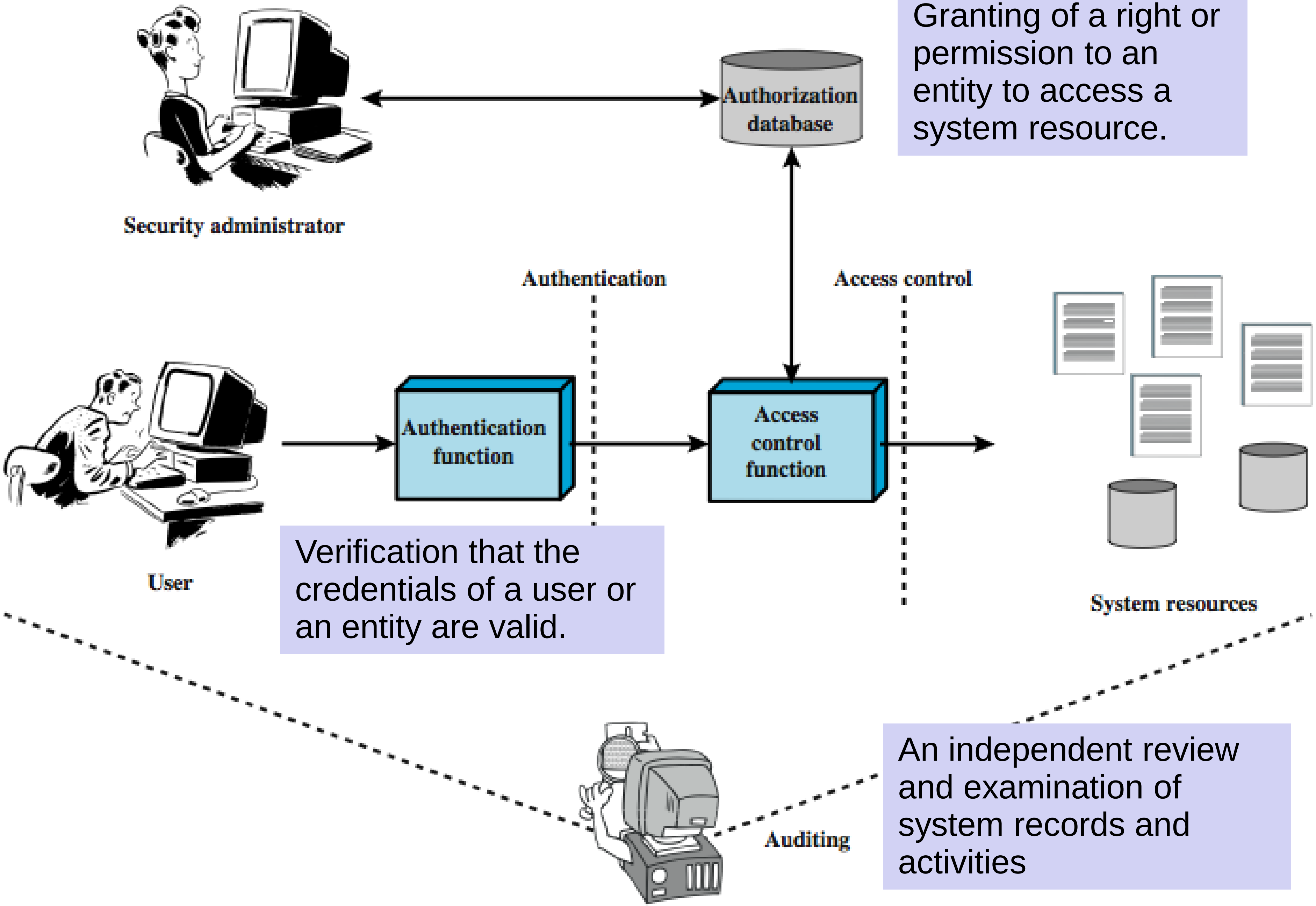
Scope of Computer Security


Computer System
Data
④ Sensitive files must be secure (file security)
① Access to the data must be controlled (protection)
Processes representing users
Guard
③ Data must be securely transmitted through networks (network security)
② Access to the computer facility must be controlled (user authentication)
Users making requests
Computer System
Data
Processes representing users
Guard

Access Control

- Many objects for which OS has to run access control
- In general, access control has three goals:
  - Check every access: Else OS might fail to notice that access has been revoked
  - Enforce least privilege: Grant program access only to smallest number of objects required to perform a task
  - Verify acceptable use: Limit types of activity that can be performed on an object

Access Control Principles



Granting of a right or permission to an entity to access a system resource.

Verification that the credentials of a user or an entity are valid.

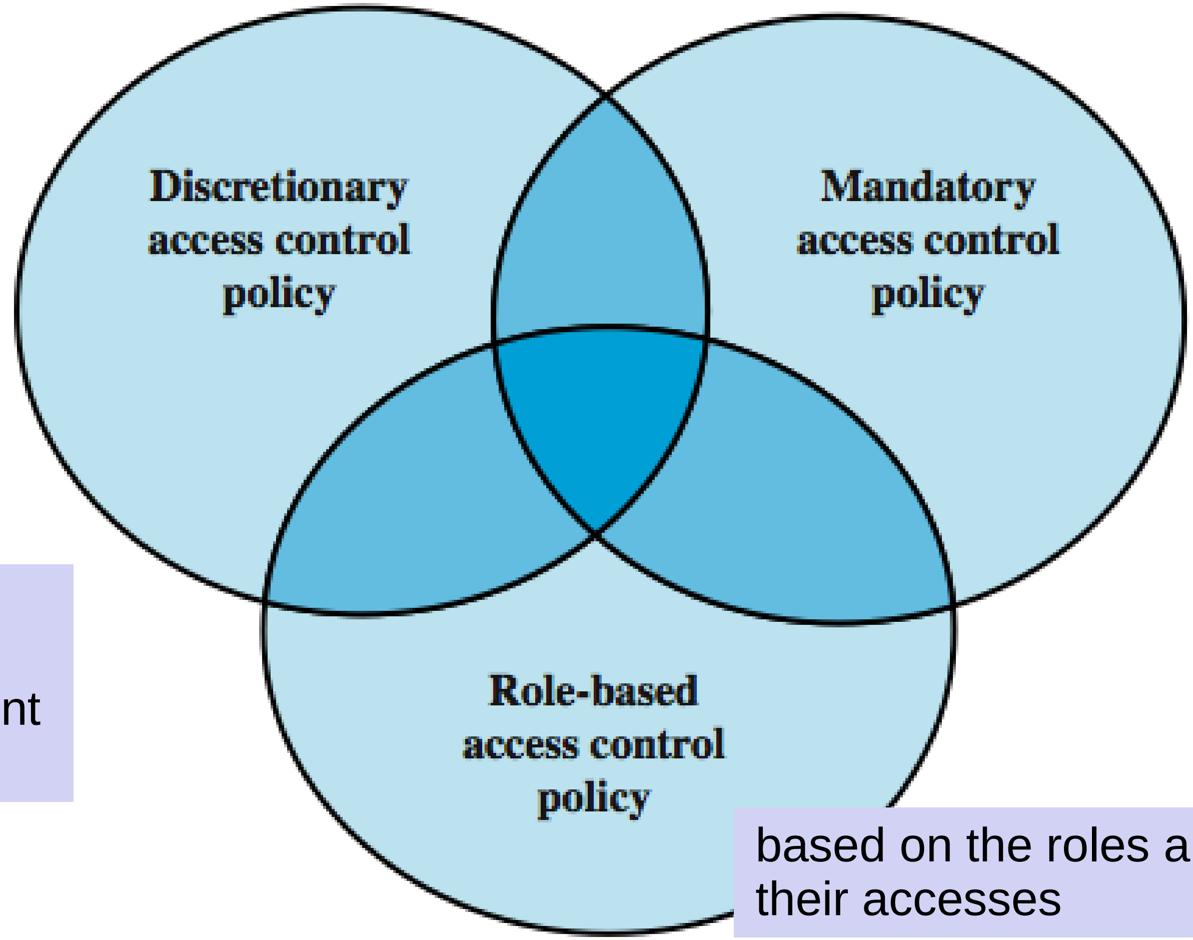
An independent review and examination of system records and activities

Access Control Policies

- dictates
  - what types of access are permitted,
  - under what circumstances,
  - by whom.

based on comparing security labels with clearances

based on the identity of the requestor and on access rules


Discretionary access control policy
Mandatory access control policy
Role-based access control policy

Attribute-based access control based on attributes of the user, the resource to be accessed, and current environmental conditions

based on the roles and their accesses

Access Control Basic Elements

subject
entity capable of accessing objects

- concept equates with that of process
- typically held accountable for the actions they initiate
- often have three classes: owner, group, world

object
resource to which access is controlled

- entity used to contain and/or receive information
- protection depends on the environment in which access control operates

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

- e.g. read, write, execute, delete, create, search

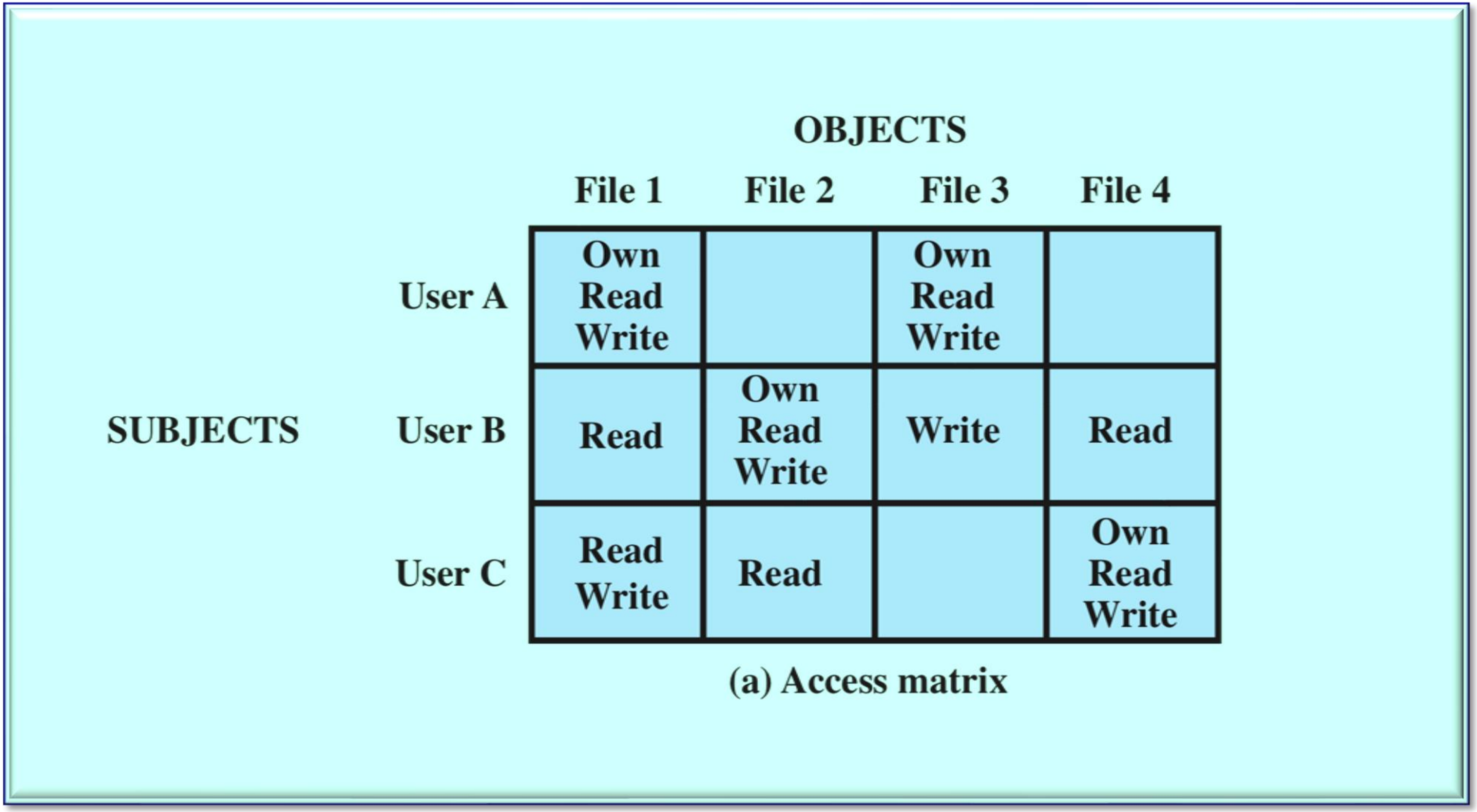
Protection Domains

- Protection Domain: set of objects together with access rights to those objects in terms of the access matrix, a row defines a protection domain
  - any process spawned by the user have access rights defined by the same protection domain
  - user can spawn processes with a subset of the access rights of the user, defined as a new protection domain
- association between a process and a domain can be static or dynamic
- Many O.S has different mode
  - in ***user mode*** certain areas of memory are protected from use and certain instructions may not be executed
  - in ***kernel mode*** privileged instructions may be executed and protected areas of memory may be accessed

Discretionary Access Control

- scheme in which an entity may enable another entity to access some resource
  - often provided using an access matrix
    - one dimension consists of identified subjects that may attempt data access to the resources
    - the other dimension lists the objects that may be accessed
  - each entry in the matrix indicates the access rights of a particular subject for a particular object

Access Matrix



		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

(a) Access matrix