CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

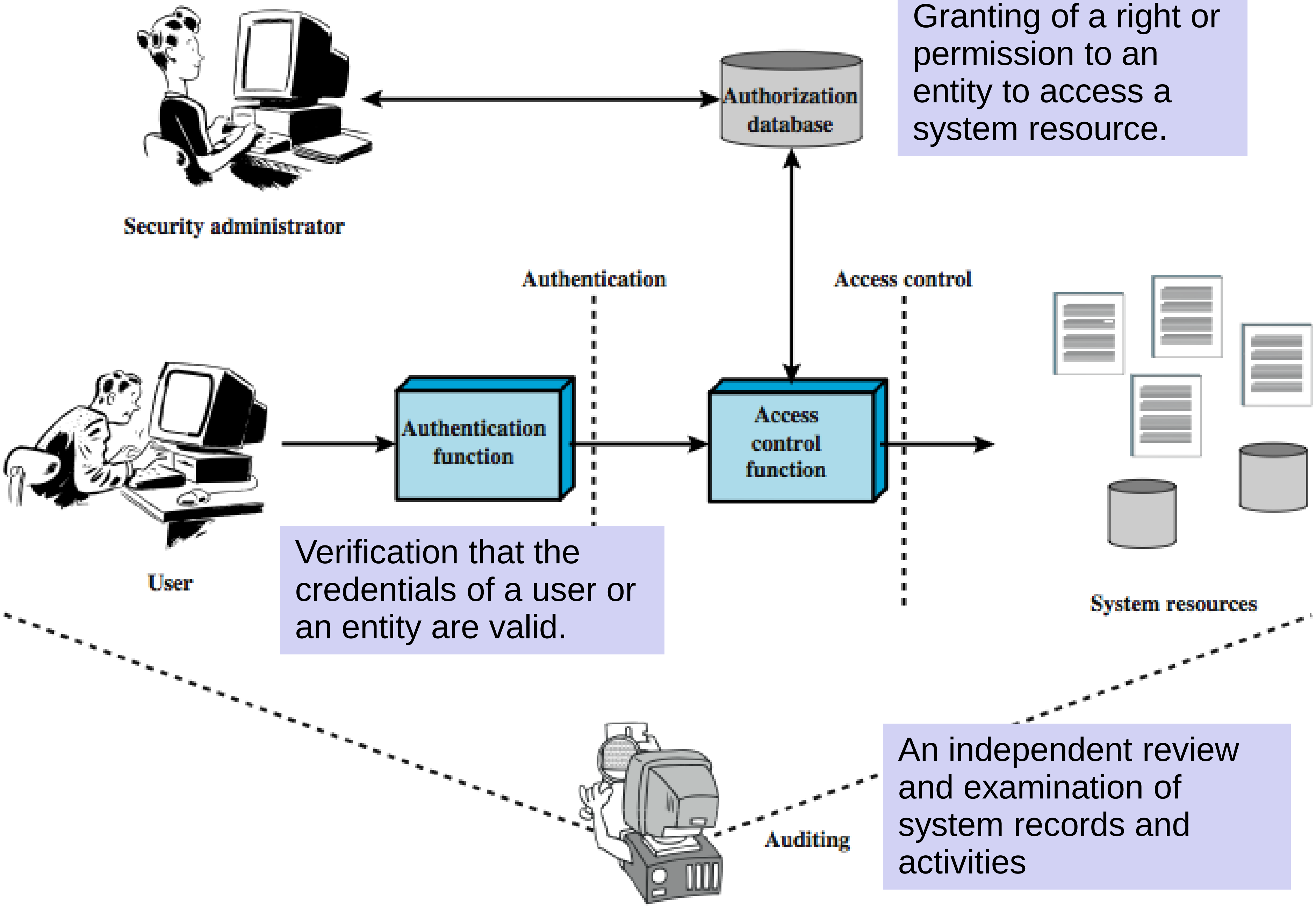
Previous Class

- Access Control
  - Discretionary Access Control

Present class

- Access Control
  - Mandatory Access Control
  - Role-Based Access Control

Access Control Principles

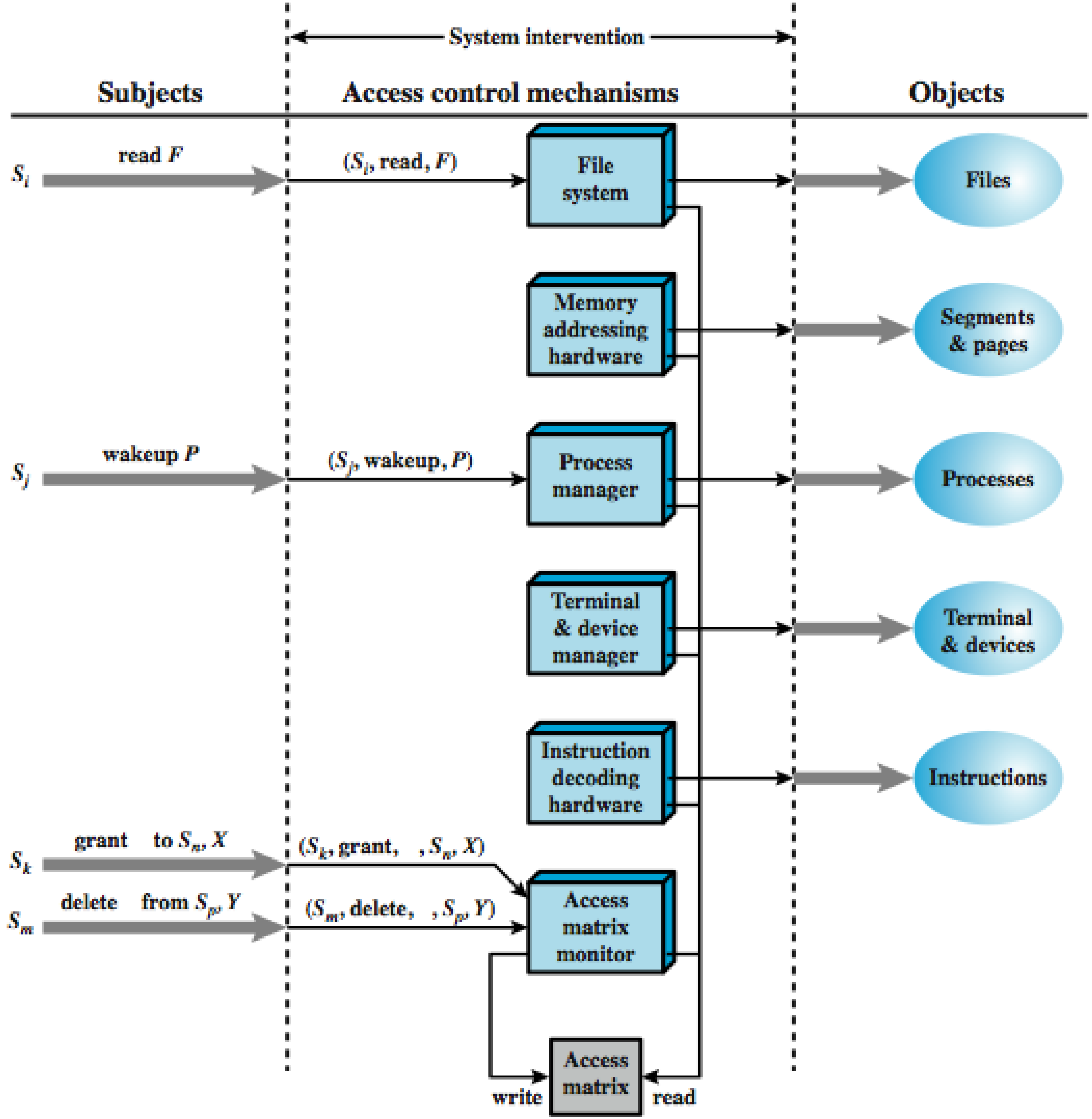


Granting of a right or permission to an entity to access a system resource.

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

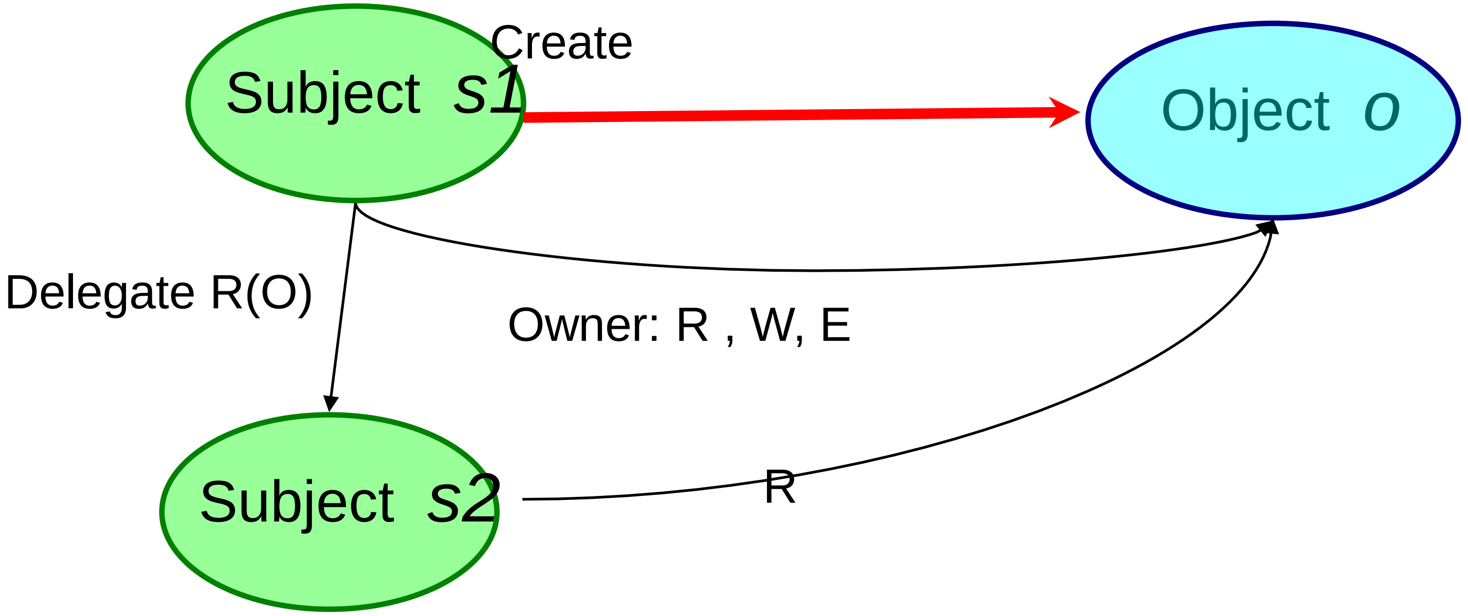
An independent review and examination of system records and activities

Access Control Function



Access Control Models: DAC

- DAC model enforces access control based on user identities, object ownership and permission delegation. The owner of an object may delegate the permission of the object to another user.



Access Control Lists (ACLs) in UNIX

- modern UNIX systems support ACLs
  - FreeBSD, OpenBSD, Linux, Solaris
- FreeBSD
  - `Setfacl` assigns a list of UNIX user IDs and groups
  - any number of users and groups can be associated with a file
  - read, write, execute protection bits
  - a file does not need to have an ACL
  - includes an additional protection bit that indicates whether the file has an extended ACL

Access Control Lists (ACLs) in UNIX

- when a process requests access to a file system object two steps are performed:
  - *step 1*: selects the most appropriate ACL
    - owner, named users, owning / named groups, others
  - *step 2*: checks if the matching entry contains sufficient permissions

DAC Pattern Advantages

advantages:

- Users can self manage access privileges.
- The burden of security administrators is significantly reduced, as resource users and administrators jointly manage permission.
- Per-user granularity for individual access decisions as well as coarse-grained access for groups are supported.
- It is easy to change privileges.
- Supporting new privileges is easy.

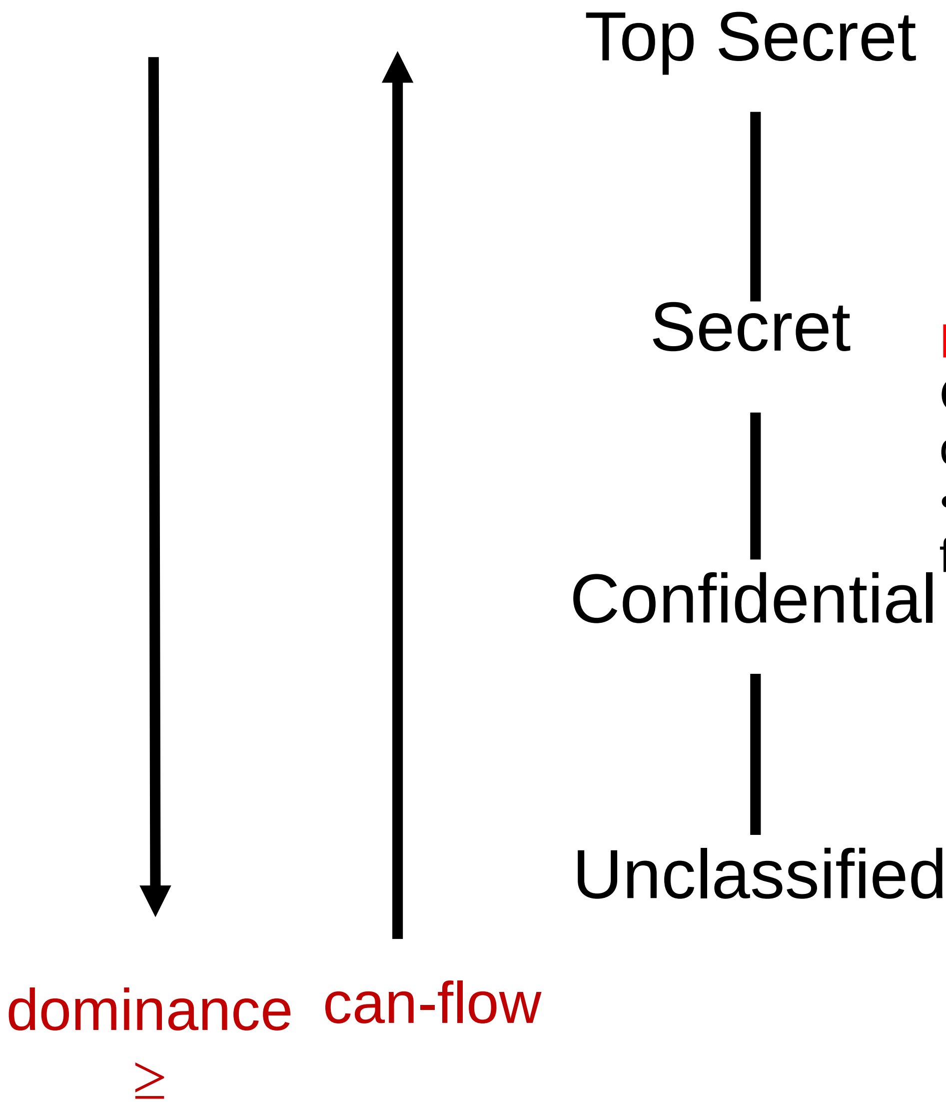
DAC

- What is wrong with DAC?
  - Difficult to enforce a system-wide security policy, e.g.: A user can leak classified documents to a unclassified users.
- Only based user's identity and ownership, Ignoring security relevant info such as
  - User's role, Function of the program, Trustworthiness of the program
- Compromised program can change access to the user's objects
- It is difficult to judge the "reasonable rights" for a user or group.
- Inconsistencies in policies are possible due to individual delegation of permission.

Mandatory Access Control (MAC)

- Defined by three major properties:
  - Administratively-defined security policy
  - Control over all subjects (process) and objects (files, sockets, network interfaces)
  - Decisions based on all security-relevant info
- MAC
  - by assigning security levels to users and objects'
  - Access to an object is granted only if the security levels of the subject and the object satisfy certain constraints.
- The MAC pattern is also known as multilevel security model and lattice-based access control.

Mandatory Access Control (MAC)



Labeling Mechanism is used

Prevent any illegal flow of information through the enforcement of multilevel security

Military Security

Classification involves sensitivity levels, compartments

- Do not let classified information leak to unclassified files

Require a strict classification of subjects and objects in security levels

Drawback of being too rigid

Applicable only to very few environments

Bell-LaPadula Model: Multi-level Security

- Introduced in 1973
- Air Force was concerned with security in time-sharing systems
  - Many OS bugs
  - Accidental misuse
- Main Objective:
  - Enable one to formally show that a computer system can securely process classified information

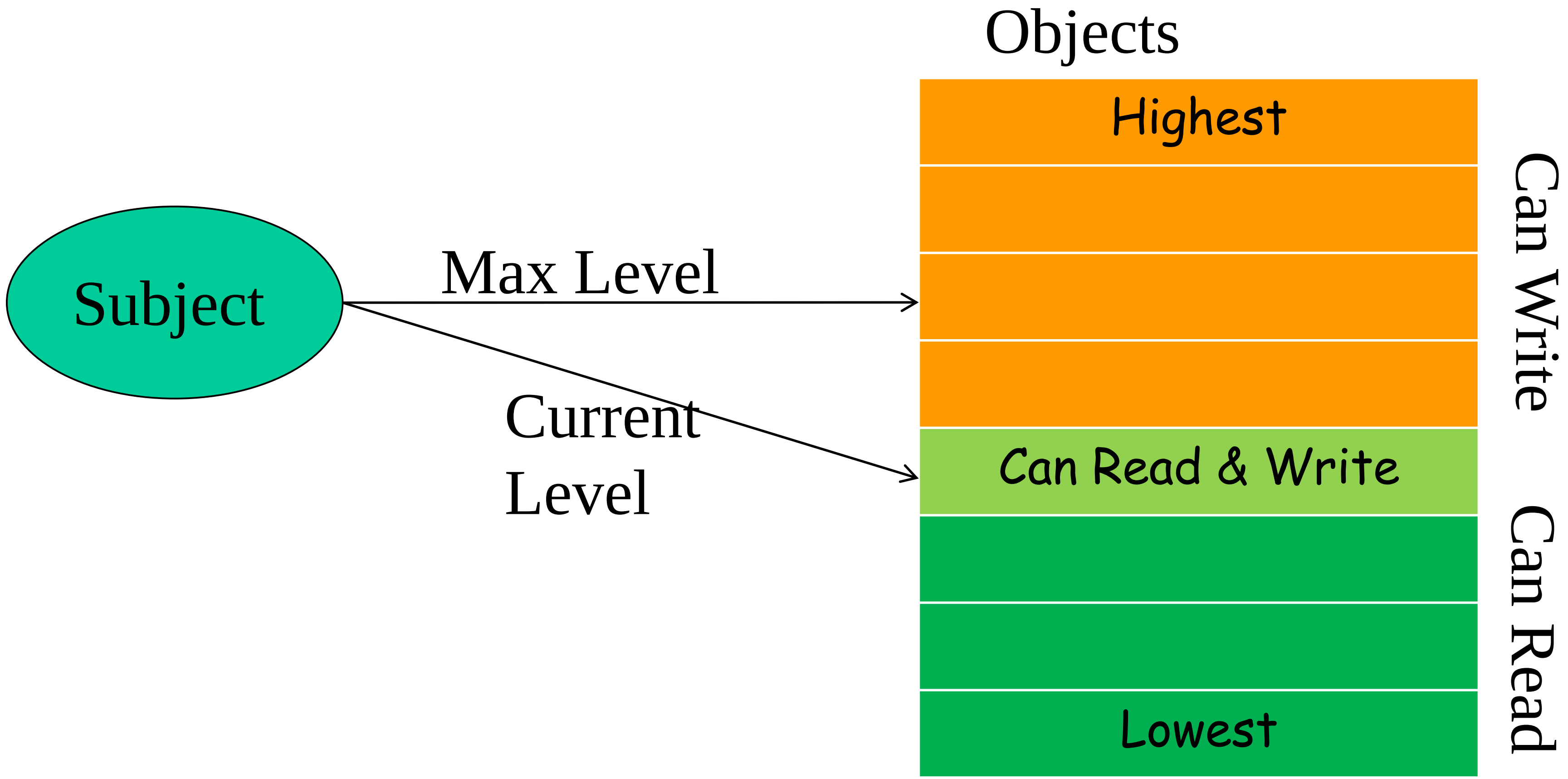
The BLP Security Model

- A computer system is modeled as a state-transition system
  - There is a set of subjects; some are designated as trusted.
  - Each state has objects, an access matrix, and the current access information.
  - There are state transition rules describing how a system can go from one state to another
  - Each subject s has a maximal sec level $L_m(s)$, and a current sec level $L_c(s)$
  - Each object has a classification level

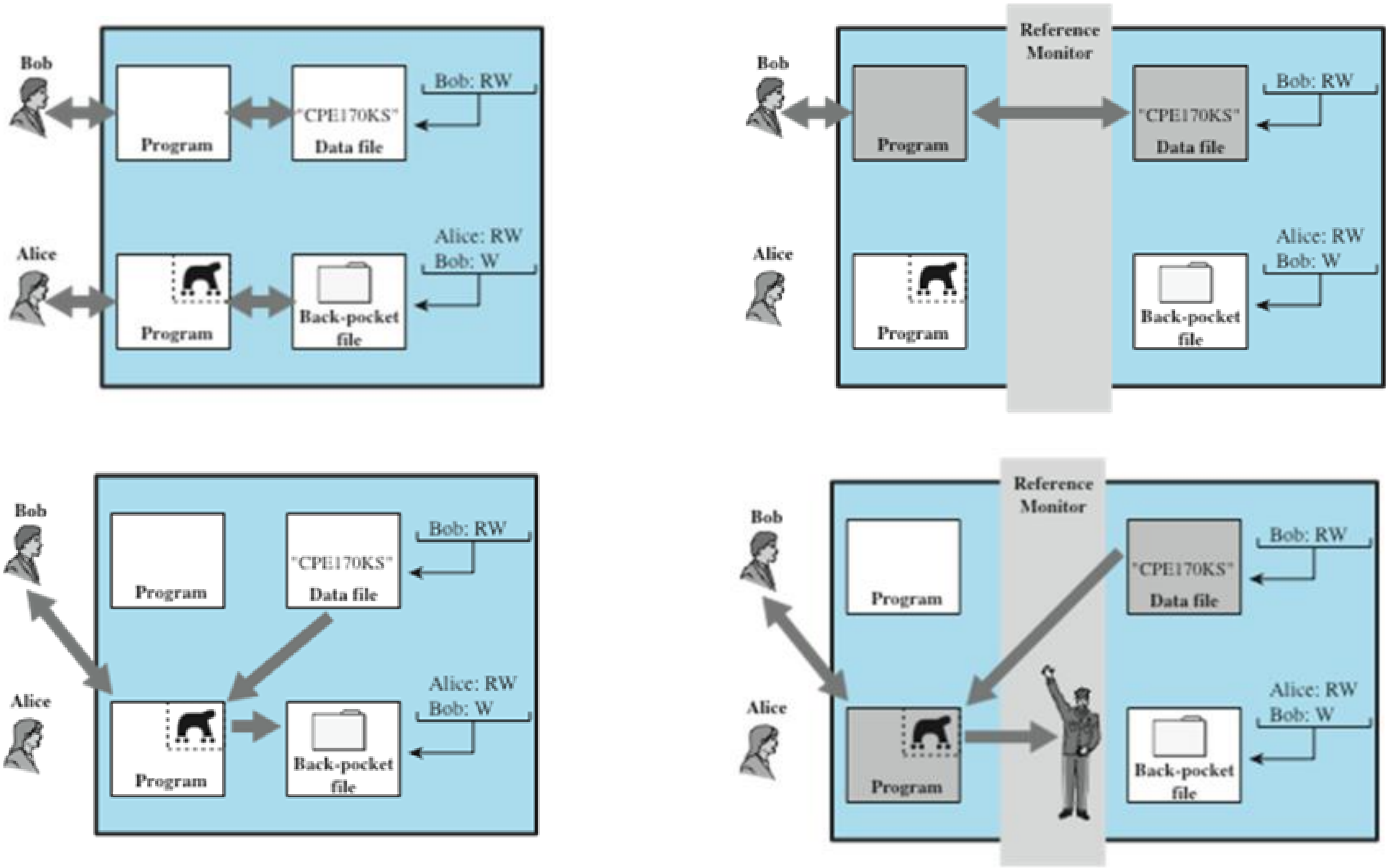
The BLP Security Policy

- A state is secure if it satisfies
  - Simple Security Condition (no read up):
    - S can read O iff $L_m(S) \geq L(O)$
  - The Star Property (no write down): for any S that is not trusted
    - S can read O iff $L_c(S) \geq L(O)$ (no read up)
    - S can write O iff $L_c(S) \leq L(O)$ (no write down)
  - Discretionary-security property
    - every access is allowed by the access matrix
- A system is secure if and only if every reachable state is secure.

Implication of the BLP Policy



Trojan Horse Defense



- Thanks