CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Access Control
  - Discretionary Access Control

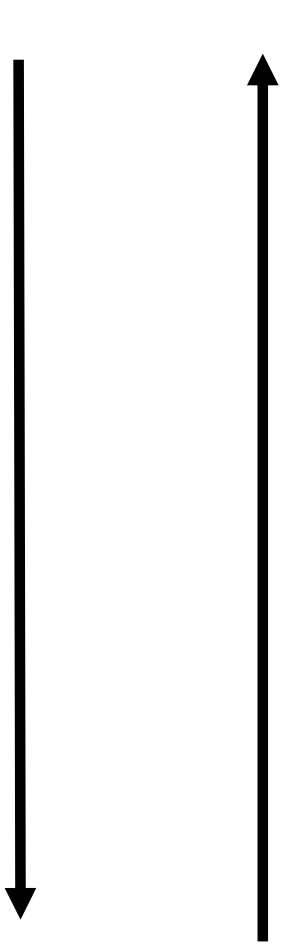
Present class

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

Mandatory Access Control (MAC)

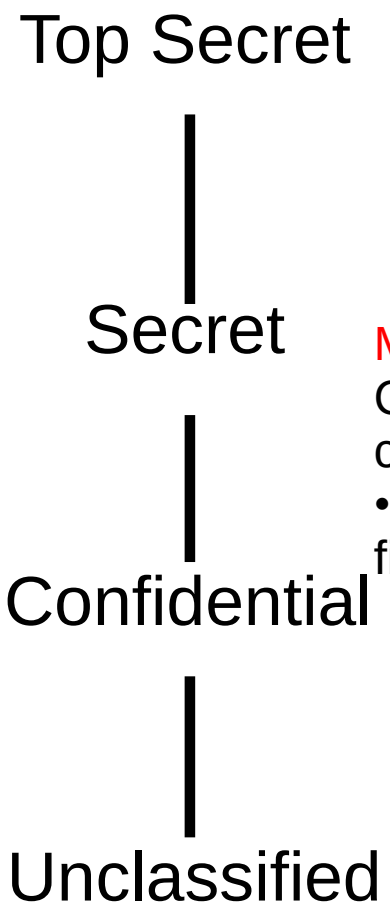
- Defined by three major properties:
  - Administratively-defined security policy
  - Control over all subjects (process) and objects (files, sockets, network interfaces)
  - Decisions based on all security-relevant info
- MAC
  - by assigning security levels to users and objects'
  - Access to an object 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)



dominance ≥

can-flow



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

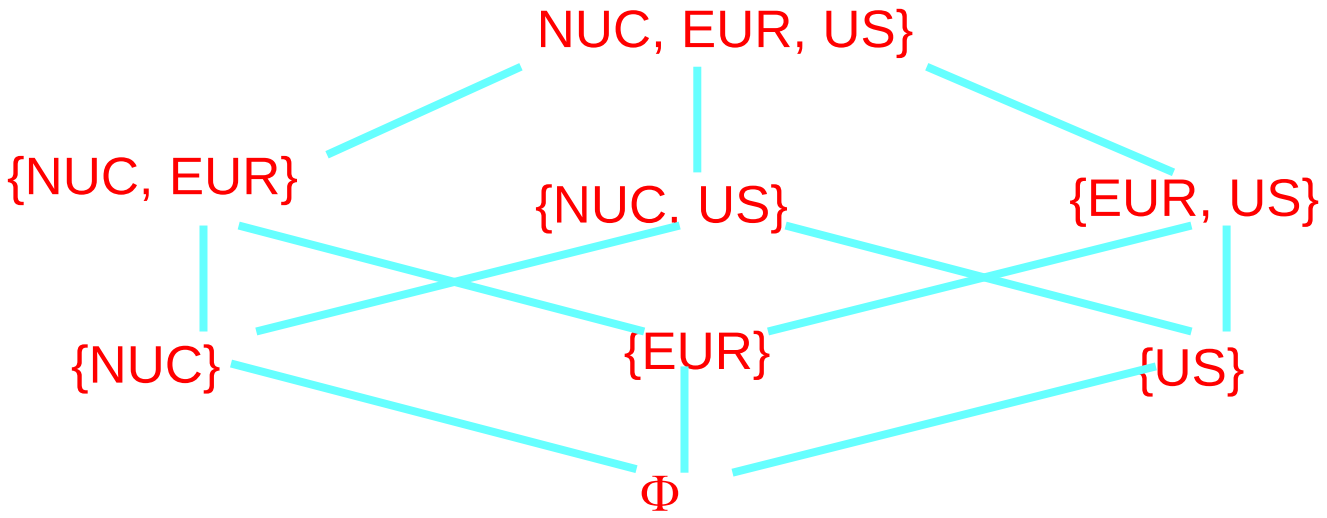
The BLP Security Policy

- 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.

Categories and Need to Know Principle

- Expand the model by adding a set of categories.
  - Each category describe a kind of information.
  - These category arise from the "need to know" principle
    - " no subject should be able to read objects unless reading them is necessary for that subject to perform its function."
- Example: three categories: NUC, EUR, US.
- Each security level and category form a security level or compartment.
- Subjects *have clearance at* (are cleared into, or are in) a security level.
- Objects are *at the level of* (or are in) a security level.

Security Lattice



- William may be cleared into level (S, {EUR})
- George into level (TS, {NUC, US}).
- A document may be classified as (C, {EUR})
- Someone with clearance at (TS, {NUC, US}) will be denied access to document with category EUR.

Dominate (dom) Relation

- The security level (L, C) dominates the security level (L', C') if and only if $L' \leq L$ and $C' \subseteq C$
- ¬Dom → dominate relation is false.
- Geroge is cleared into security level (S, {NUC, EUR})
- DocA is classified as (C, {NUC})
- DocB is classified as (S, {EUR, US})
- DocC is classified as (S, {EUR})
- George dom DocA
- George ¬ dom DocB
- George dom DocC

New Security Condition and *-Property

- Let C(S) be the category set of subject S.
- Let C(O) be the category set of object O.
- Simple Security Condition (not read up):
  S can read O if and only if S dom O and
  S has discretionary read access to O.
- *-Property (not write down):
  S can write to O if and only if O dom S and
  S has discretionary write access to O.
- Basic Security Theorem:
  Let Σ be a system with secure initial state σ_0
  Let T be the set of state transformations.
  If every element of T preserves the simple security condition, preliminary version, and the *-property, preliminary version,
  Then every state σ_i, $i \geq 0$, is secure.

Allow Write Down?

- Bell-LaPadula allows higher-level subject to write into lower level object that low level subject can read.
- A subject has a maximum security level and a current security level.
  - maximum security level must dominate current security level.
- A subject may (effectively) decrease its security level from the maximum in order to communicate with entities at lower security levels.
- Colonel's maximum security level is (S, {NUC, EUR}). She changes her current security level to (S, {EUR}). Now she can create document at Major is clearance level (S, {EUR}).

Limitations with BLP

- Deal only with confidentiality, does not deal with integrity at all

  - Addressed by integrity models (such as Biba, Clark-Wilson)

- Does not deal with information flow through covert channels

What is integrity?

- Attempt 1: Critical data do not change.
- Attempt 2: Critical data changed only in "correct ways"
  - E.g., in DB, integrity constraints are used for consistency
- Attempt 3: Critical data changed only through certain "trusted programs"
- Attempt 4: Critical data changed only as intended by authorized users.

The Biba Model

- Kenneth J. Biba: "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977.

- Motivated by the fact that BLP does not deal with integrity

Biba: Integrity Levels

- Each subject (program) has an integrity level
- Each object has an integrity level
- Integrity levels are totally ordered

- Integrity levels different from security levels in confidentiality protection
  - a highly sensitive data may have low integrity

Five Mandatory Policies in Biba

- Strict integrity policy
- Subject low-water mark policy
- Object low-water mark policy
- Low-water mark Integrity audit policy
- Ring policy

Strict Integrity Policy (BLP reversed)

- Rules:
  - s can read o iff $i(s) \leq i(o)$
    - no read down
    - stops indirect sabotage by contaminated data
  - s can write to o iff $i(s) \geq i(o)$
    - no write up
    - stops directly malicious modification

- Fixed integrity levels

- Thanks