CS 556 – Computer Security
Spring 2018

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA

Mandatory Access Control for Integrity

Biba Model

- Counterpart of the BLP model for Integrity purposes
- Used to enforce integrity of system resources

Biba Simple Integrity

- A subject, S, is allowed a read access to an object, O, only if the access class of the subject S is dominated by the access class of object O
  - That is AC(S) $\leq$ AC(O)
    - No read down

Biba * (Star) Property - Integrity Confinement

- A subject, S, is allowed to write to an object, O, only if the access class of subject S dominates the access class of object O
  - That is AC(O) $\leq$ AC(S)
    - No write up

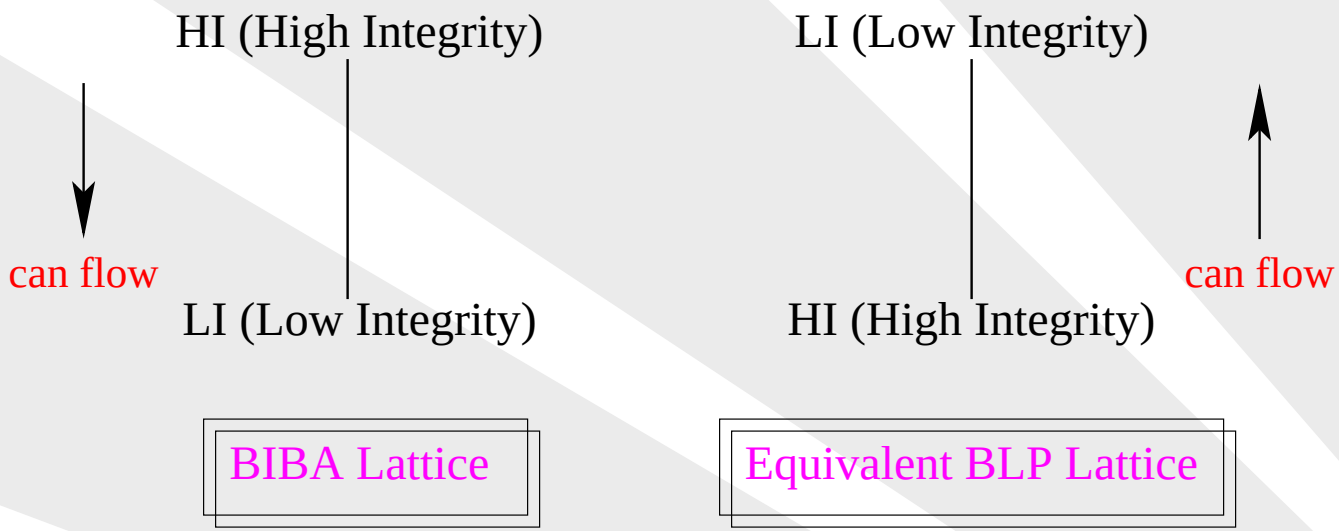
Information Flow Models

- BLP and Biba are two examples of information flow policies
- Information usually flows from one object to another
- Whenever information flows from one object A to another object B, there is also information flow from the security class of A to the security class of B

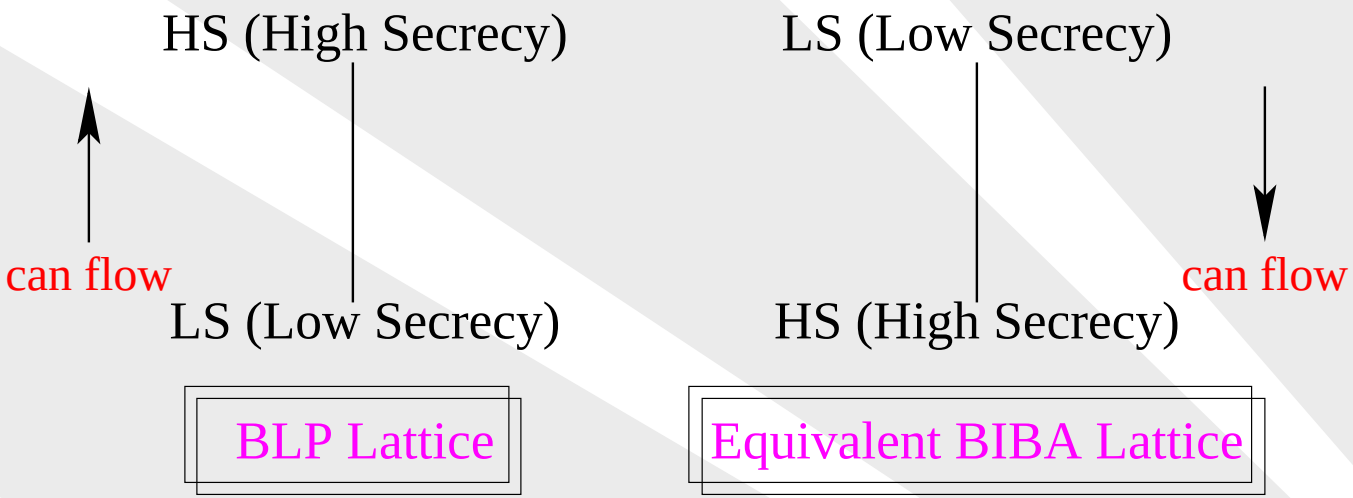
BLP, Biba Revisited

- BLP and Biba models are fundamentally equivalent
  - Information flow in the Biba model is from top to bottom
  - Information flow in the BLP model is from bottom to top
  - Since top and bottom are relative terms, the two models are fundamentally equivalent

Equivalence of BLP and Biba



Equivalence of BLP and Biba



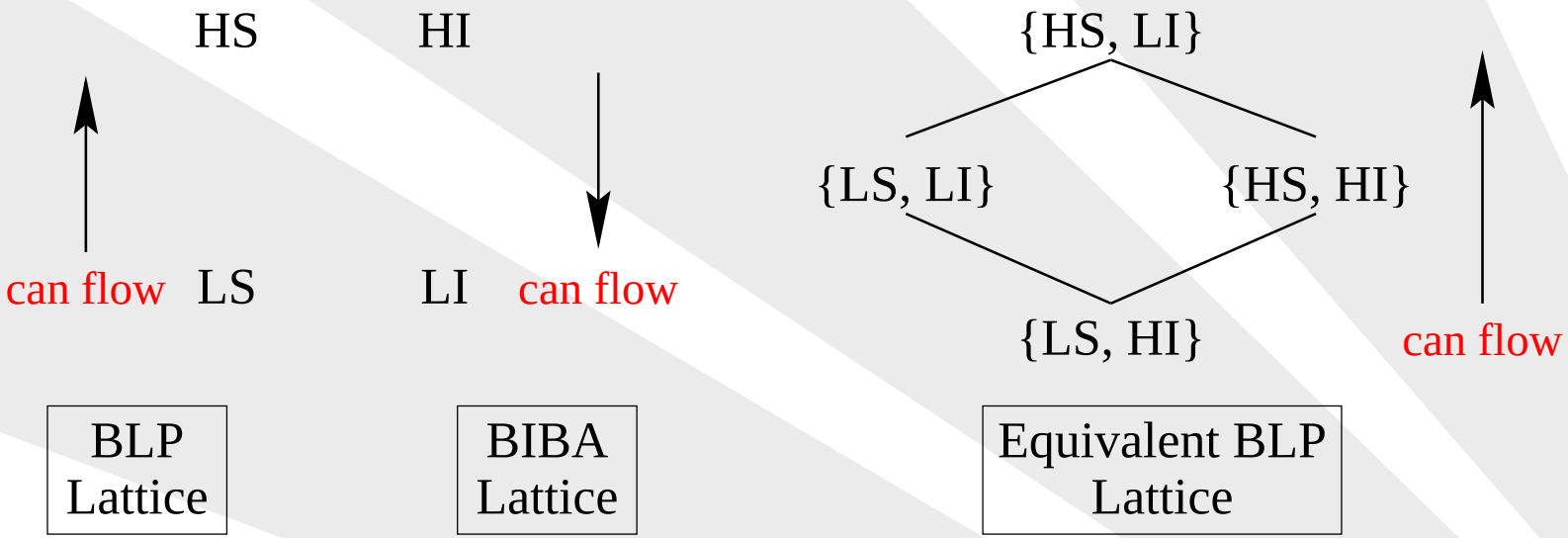
Combining the BLP and Biba Models

- If a single label is used for both confidentiality as well as integrity then the two models impose conflicting constraints
  - We fail to have information flow between security classes
  - Trivial information flow policy
- Use independent confidentiality and integrity labels
  - $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_p\}$ is a lattice of confidentiality levels
  - $\Omega = \{\omega_1, \omega_2, \ldots, \omega_p\}$ is a lattice of integrity levels

Combining the BLP and Biba Models

- The combined mandatory controls are:
  - Subject S can read object O only if $\lambda(S) \geq \lambda(O)$ and $\omega(S) \leq \omega(O)$
  - Subject S can write object O only if $\lambda(S) \leq \lambda(O)$ and $\omega(S) \geq \omega(O)$
- This is the composite model and has been implemented in several operating system

Combining BLP and Biba Models



BLP Lattice

BIBA Lattice

Equivalent BLP Lattice

Security Requirements in the Commercial Sector

Is Commercial Security Different?

- Commercial firms rarely grant access on the basis of "clearances".
  - While this can be modeled using BLP it requires a large number of categories and security levels.
  - It is difficult to control the proliferation of categories and security levels as the creation of categories and levels are decentralized.

Is Commercial Security Different?

- Problem of information aggregation is insiduos.
  - Commercial firms usually allow a limited amount of (innocuous) information to become public but keep a large amount of (sensitive) information confidential.
  - By aggregating the innocuous information one can deduce much sensitive information.
- Preventing this requires the model to track what questions have been asked.