LATTICE-BASED MODELS

- **Denning's axioms and lattices**
- **Bell-LaPadula model (BLP)**
- **BIBA**
- **Integrity and information flow**

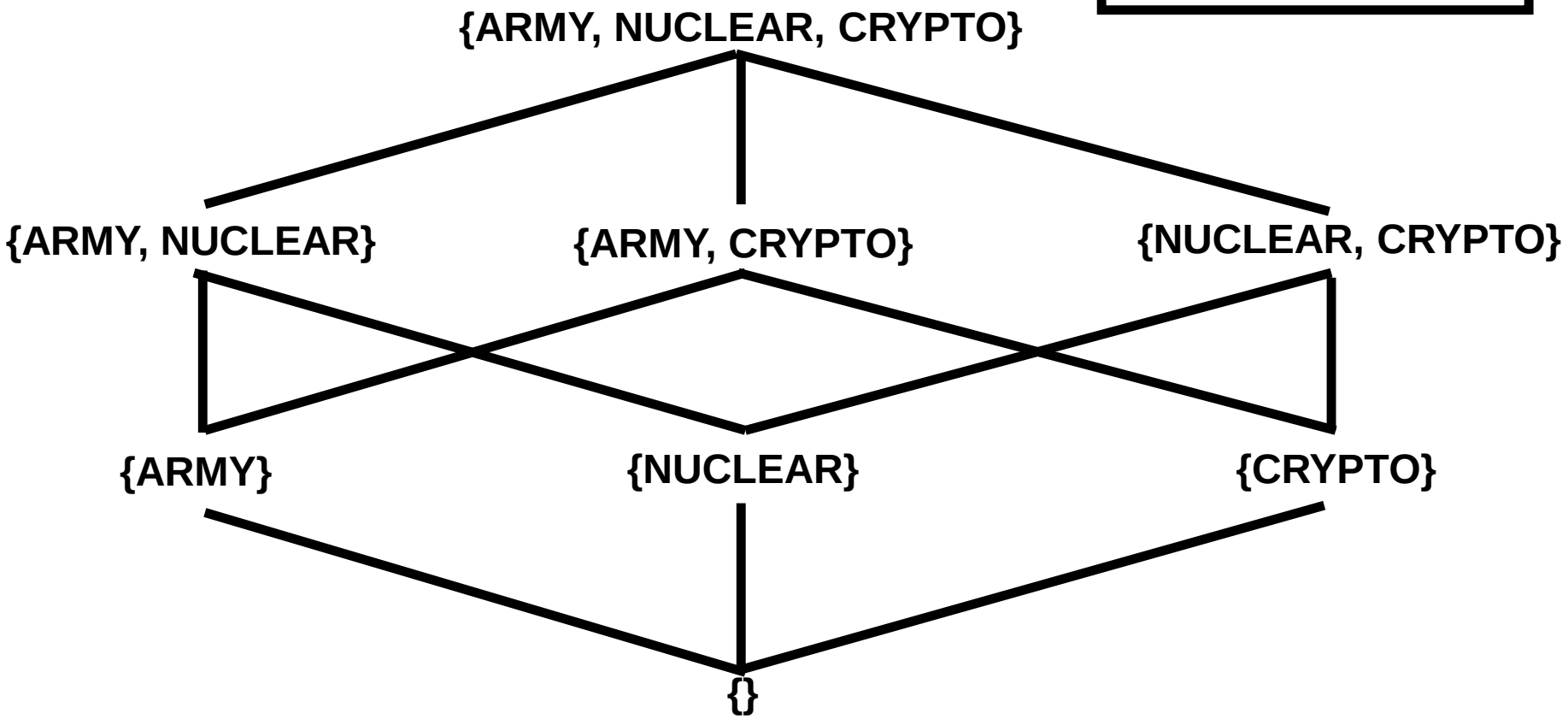
INFORMATION FLOW

$$< SC, \rightarrow, \oplus >$$

SC	**set of security classes**
$\rightarrow \subseteq$ SC X SC	**flow relation (i.e., can-flow)**
$\oplus$: SC X SC -> SC	**class-combining operator**

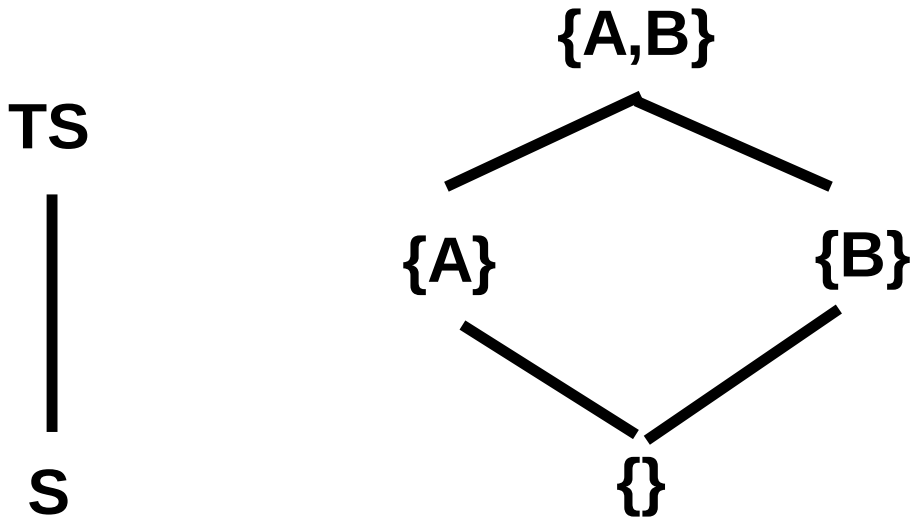
LATTICE STRUCTURES

Compartments and Categories



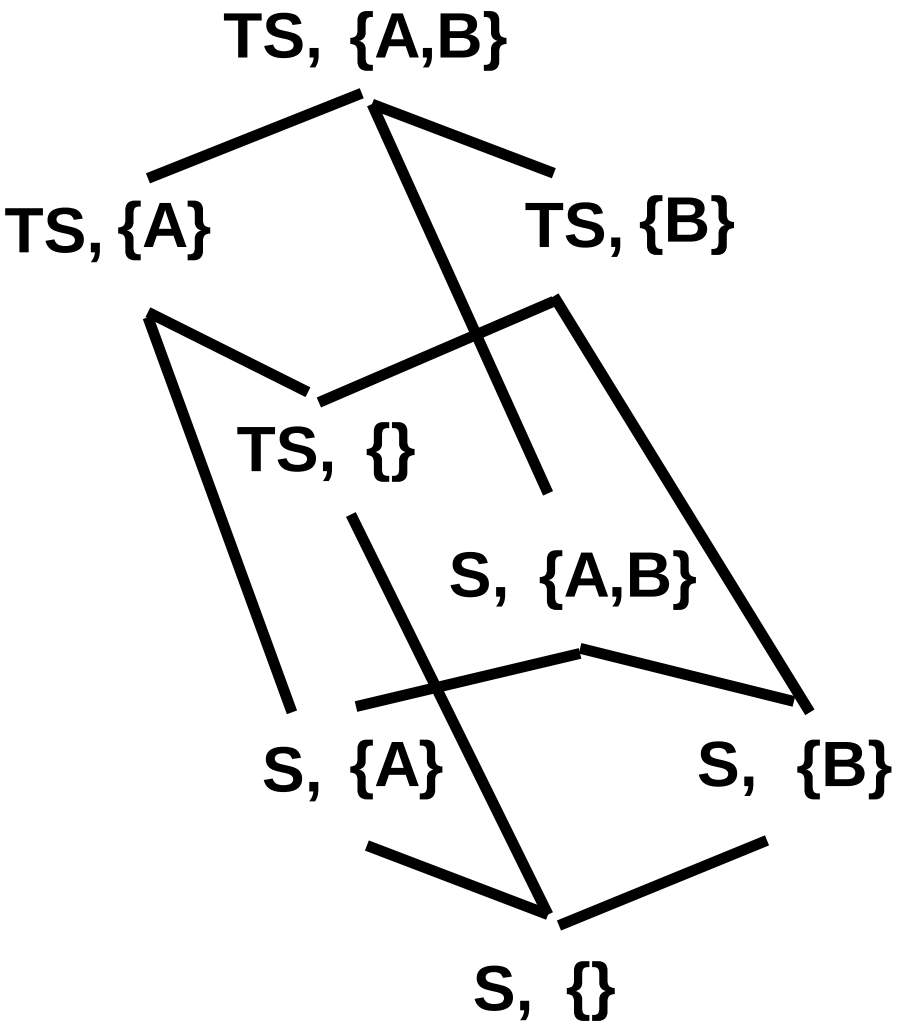
LATTICE STRUCTURES

Hierarchical Classes with Compartments



product of 2 lattices is a lattice

LATTICE STRUCTURES



Hierarchical Classes with Compartments

BELL LAPADULA (BLP) MODEL

SIMPLE-SECURITY RULE **(no read up)**

Subject S can read object O only if

- **label(S) dominates label(O) i.e. $\lambda(S) \geq \lambda(O)$**
- **information can flow from label(O) to label(S)**

STAR-PROPERTY

Subject S can write object O only if (no write down)

- **label(O) dominates label(S) i.e. $\lambda(S) \leq \lambda(O)$**
- **information can flow from label(S) to label(O)**

BELL LAPADULA (BLP) MODEL

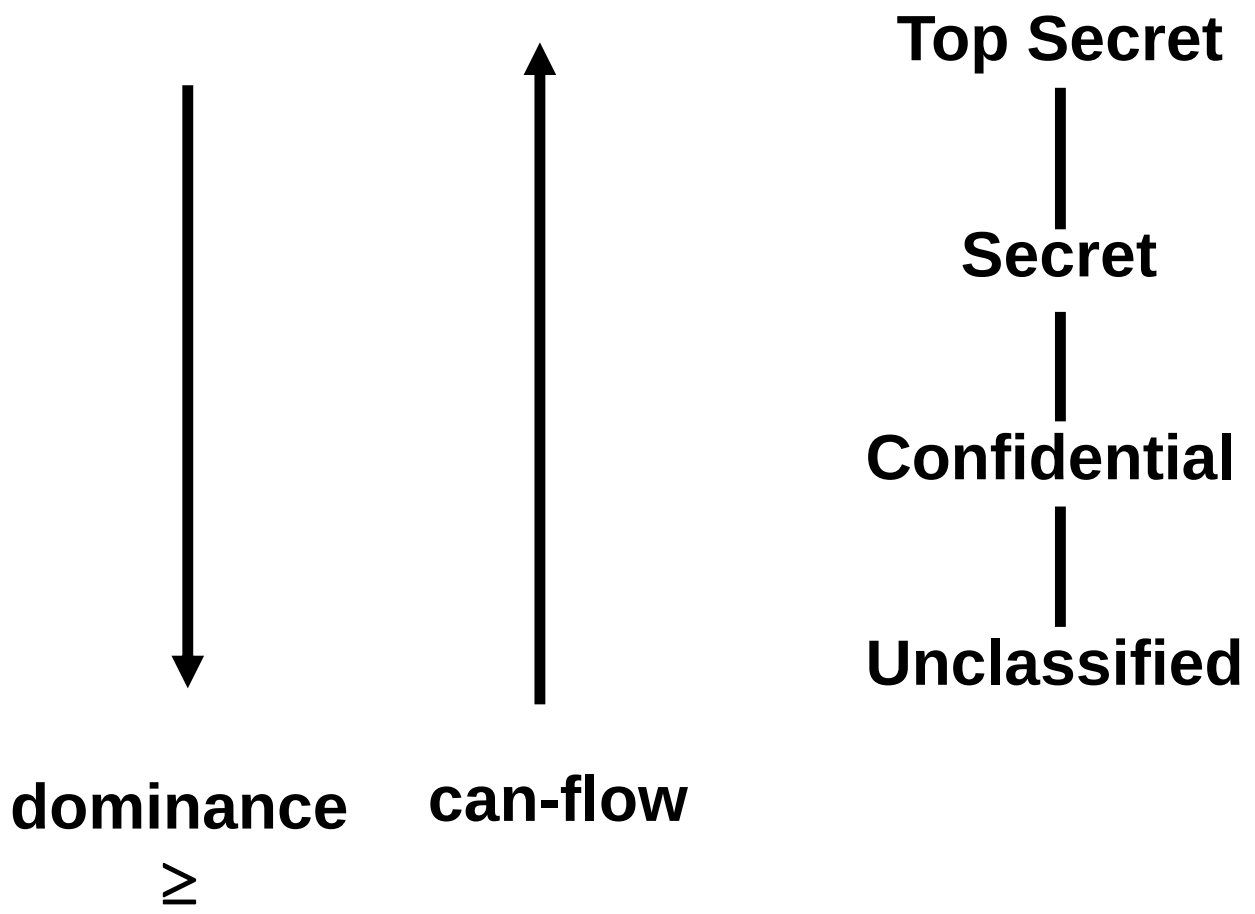
STAR-PROPERTY

Subject S can write object O only if (no write down)

- **label(O) dominates label(S) i.e. $\lambda(S) \leq \lambda(O)$**
- **information can flow from label(S) to label(O)**
- **The $*$-property allows secret data be destroyed or damaged by unclassified subjects. To prevent this the $*$-property is sometimes used in the form**

  S is allowed to write O only if $\lambda(S) = \lambda(O)$

BLP MODEL


Top Secret
Secret
Confidential
Unclassified
dominance
≥
can-flow

BIBA MODEL

SIMPLE-INTEGRITY RULE

Subject S can read object O only if

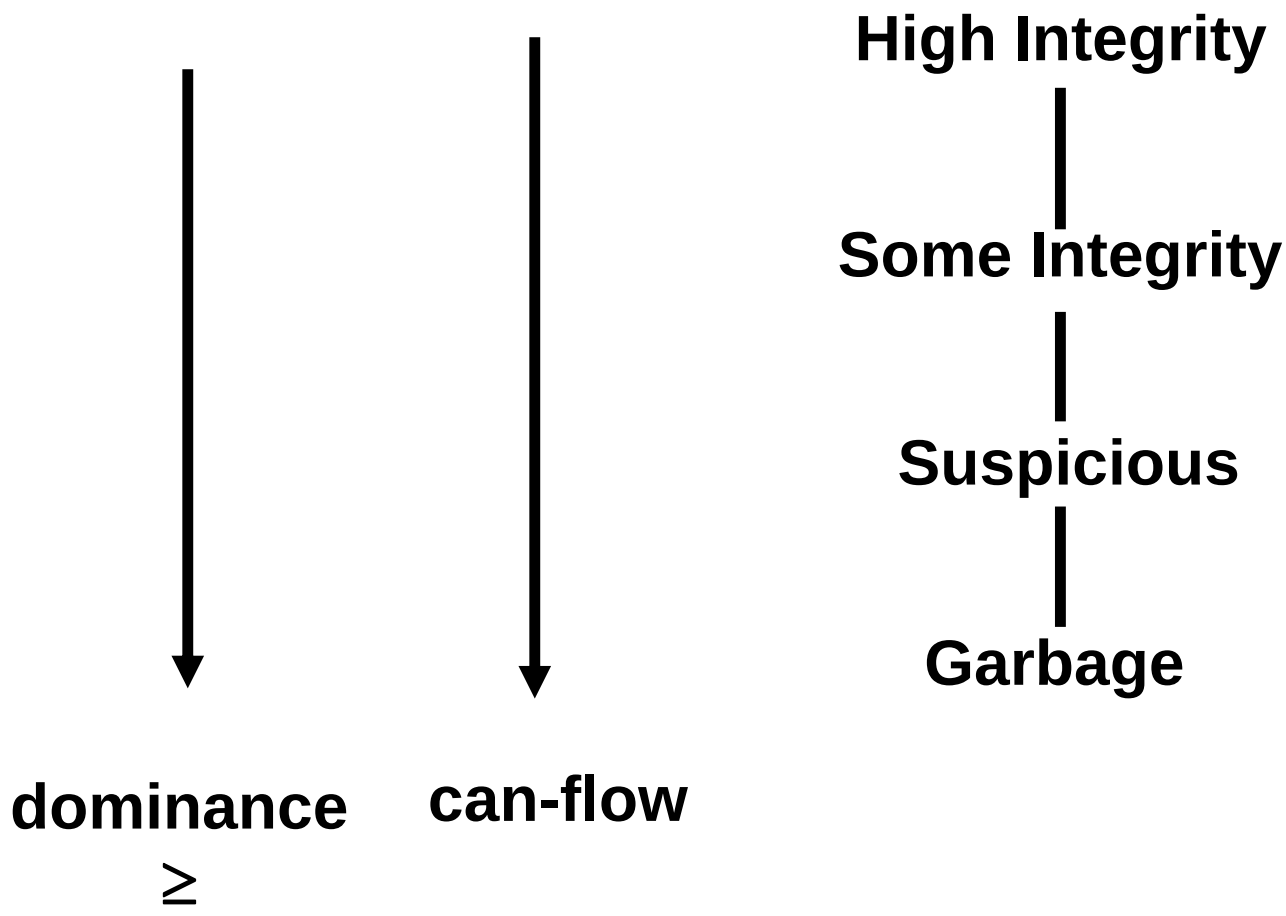
- **label(O) dominates label(S) i.e. $\omega(S) \leq \omega(O)$**
- **information can flow from label(O) to label(S)**

STAR-PROPERTY

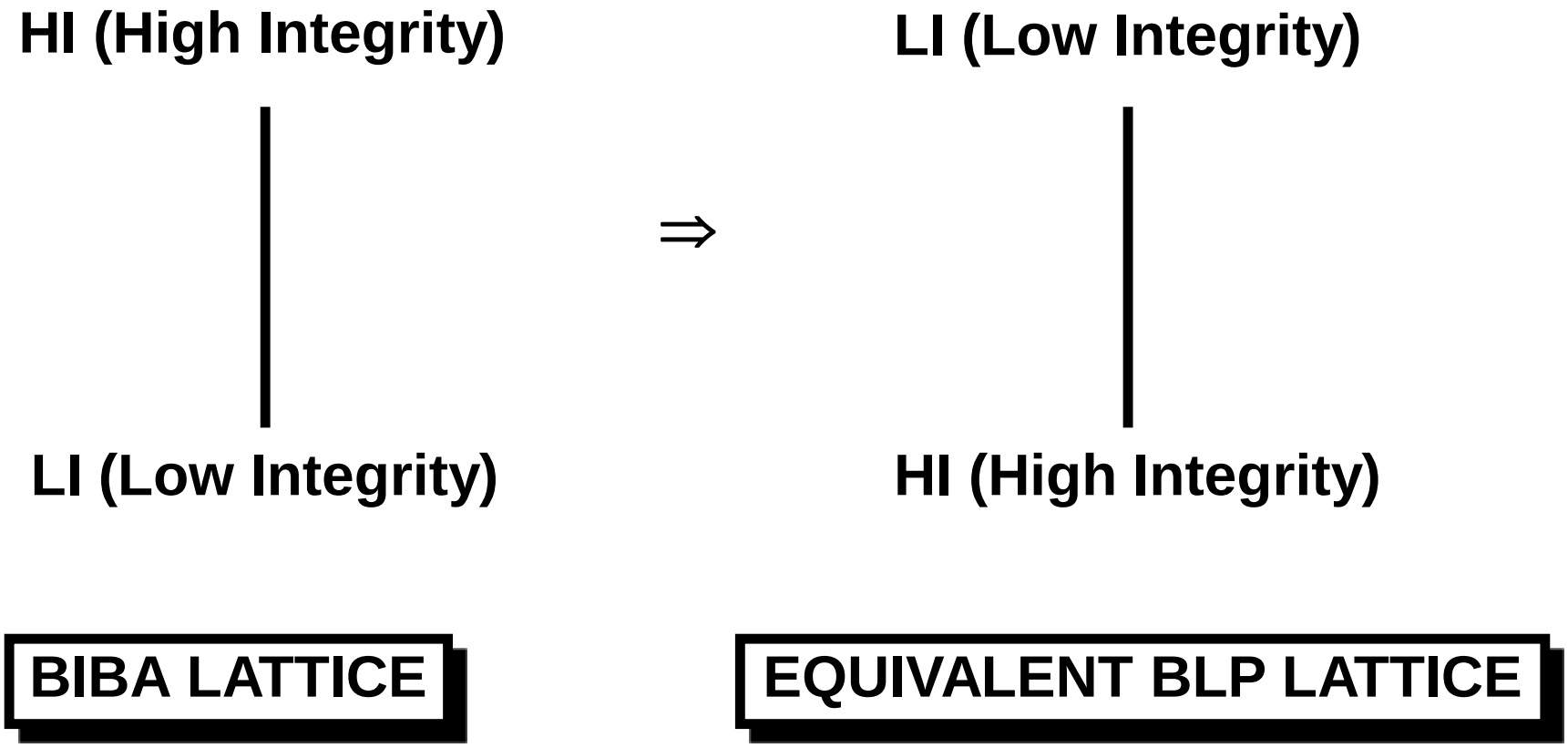
Subject S can write object O only if

- **label(S) dominates label(O) i.e. $\omega(S) \geq \omega(O)$**
- **information can flow from label(S) to label(O)**

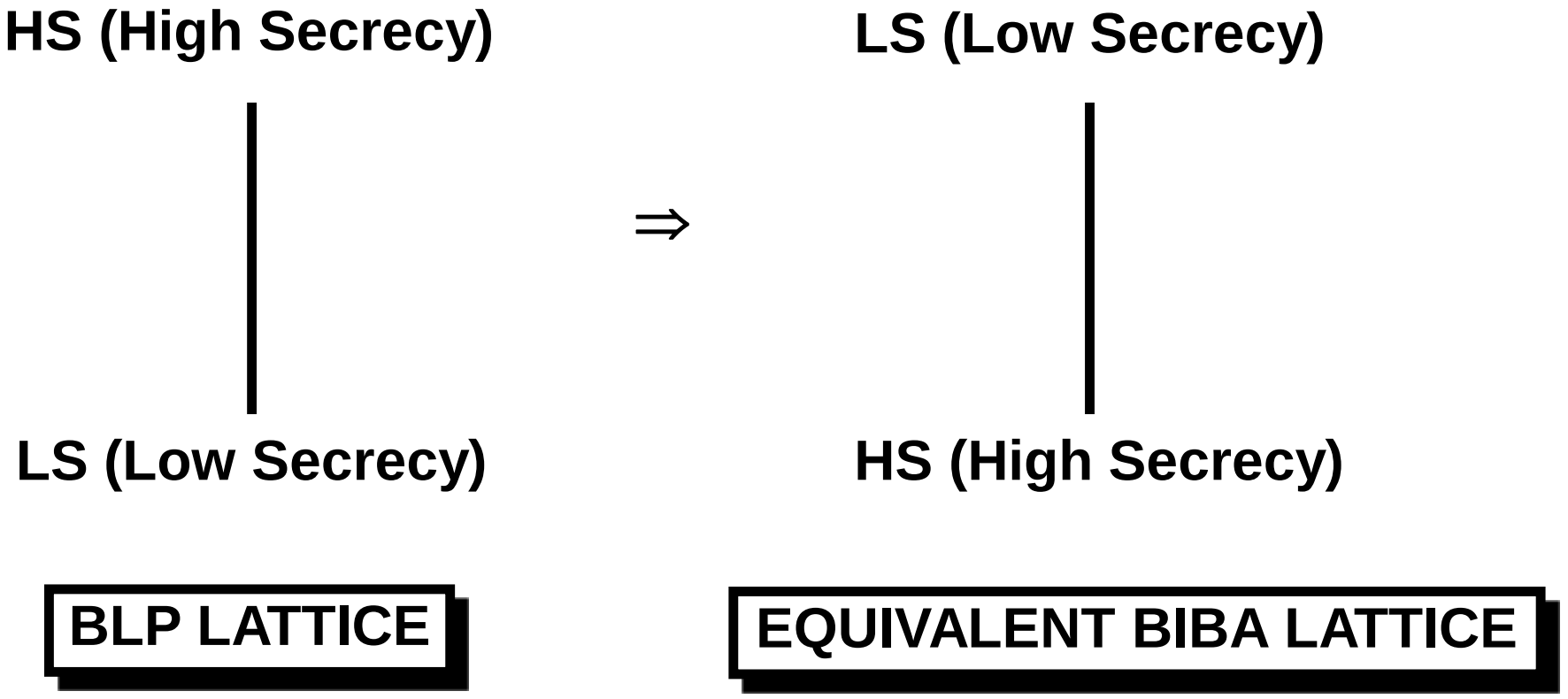
BIBA MODEL


High Integrity
Some Integrity
Suspicious
Garbage
dominance
≥
can-flow

EQUIVALENCE OF BLP AND BIBA

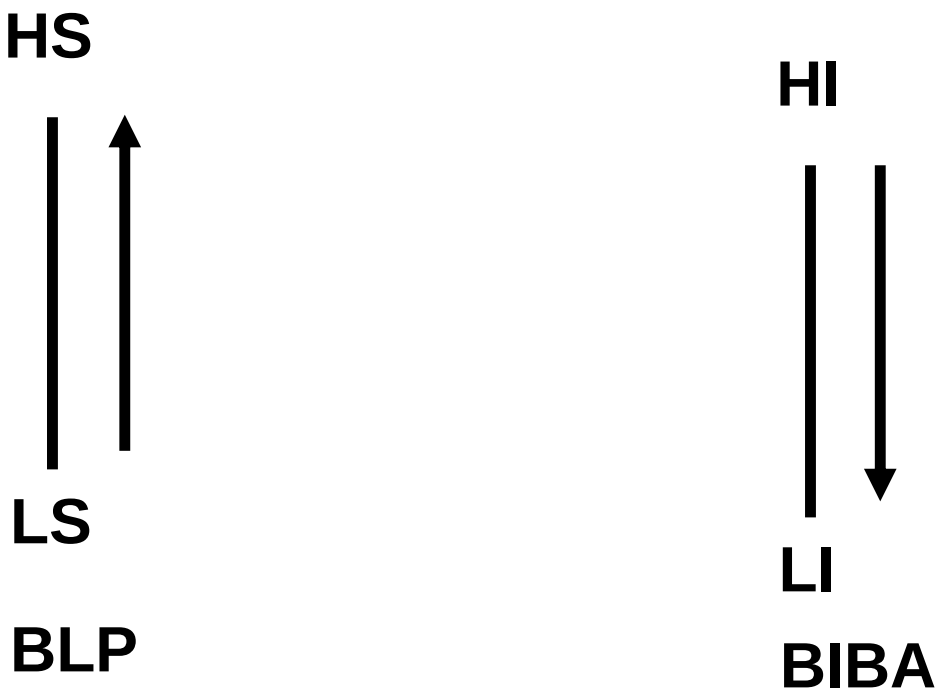


EQUIVALENCE OF BLP AND BIBA



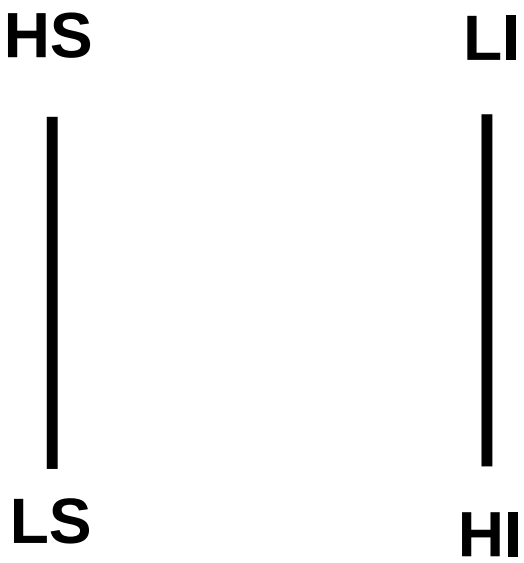
COMBINATION – BLP&BIBA

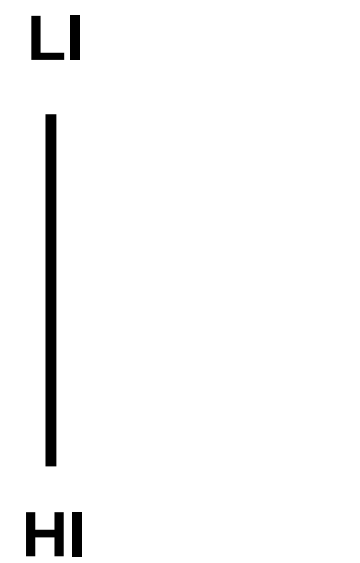
Case 1

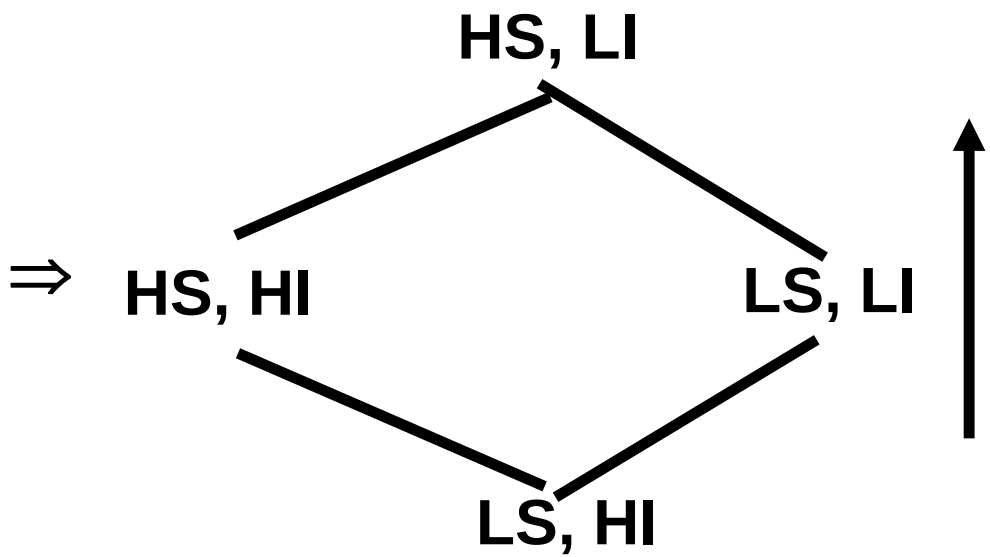


COMBINATION – BLP&BIBA

Case 1



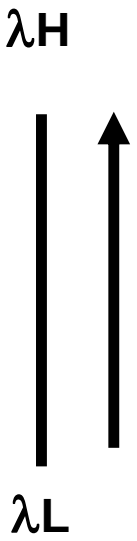




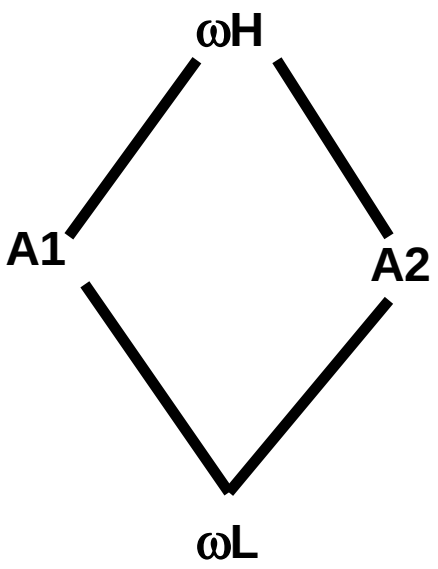
COMBINATION BLP&BIBA

COMBINATION – BLP&BIBA

Case 2



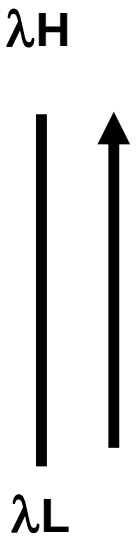
BLP



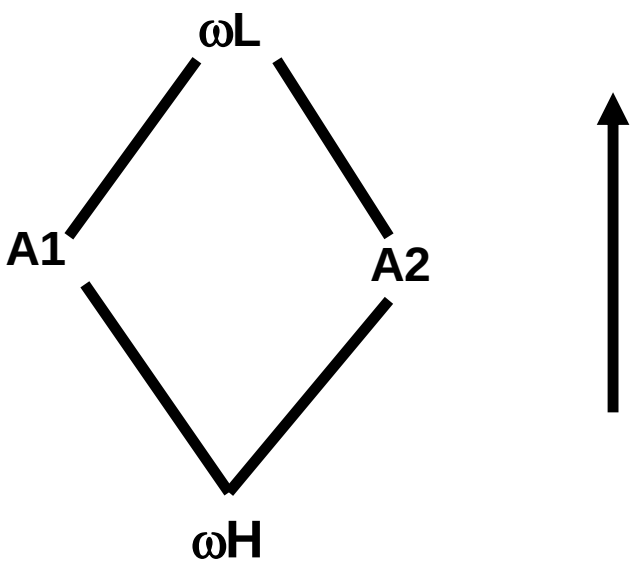
BIBA

COMBINATION – BLP&BIBA

Case 2



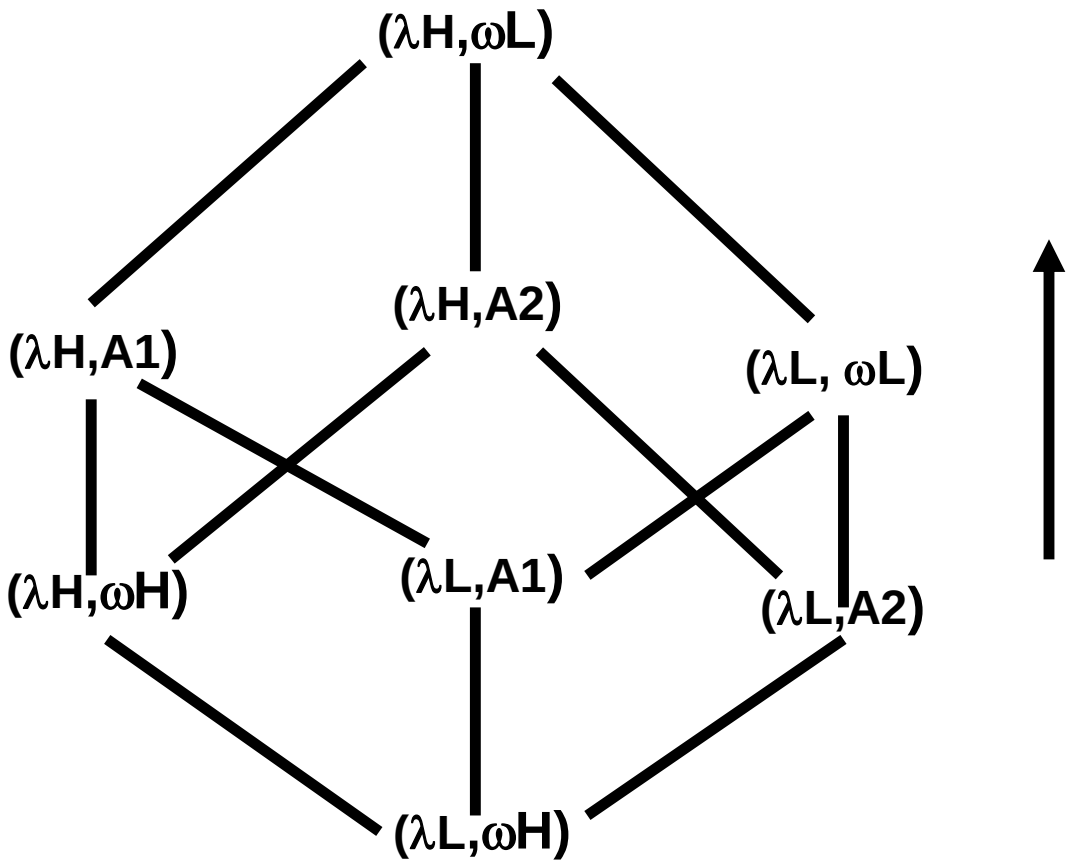
BLP



BIBA

COMBINATION – BLP&BIBA

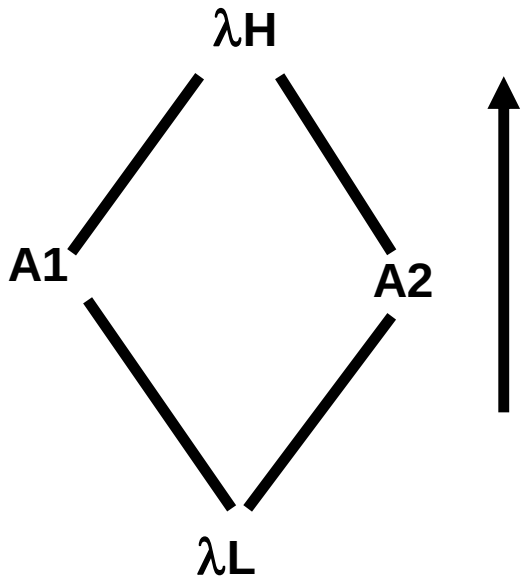
Case 2



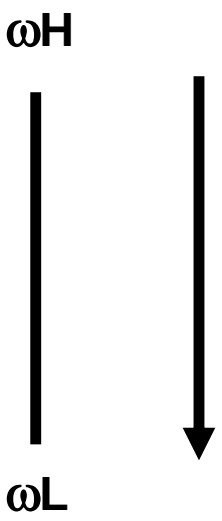
COMBINATION BLP&BIBA

COMBINATION – BLP&BIBA

Case 3



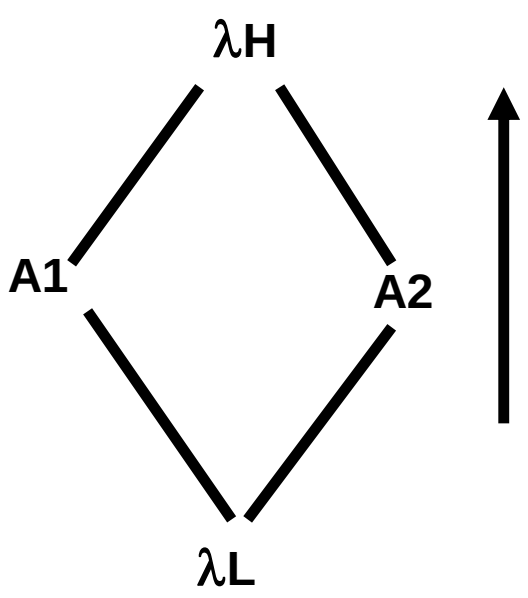
BLP



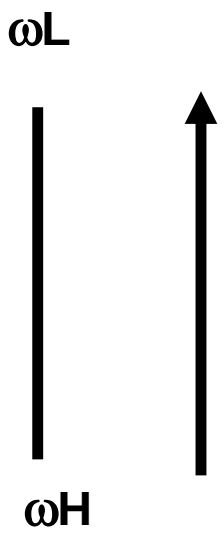
Biba

COMBINATION OF DISTINCT LATTICES

Case 3



BLP



Biba

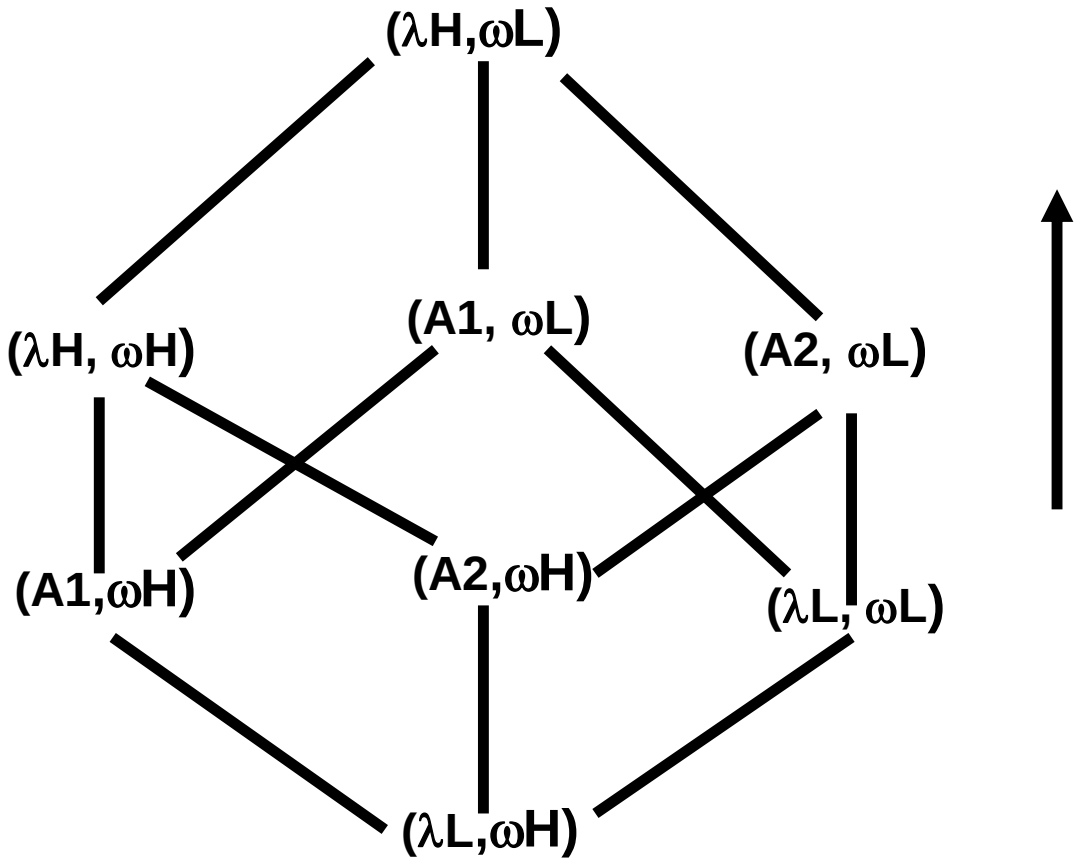
L ≤ A1 A1 ≤ H

L ≤ A2 A2 ≤ H

A1, A2 incomparable

COMBINATION – BLP&BIBA

Case 3



COMBINATION BLP&BIBA

BLP AND BIBA

- **BLP and Biba are fundamentally equivalent and interchangeable**
- **Lattice-based access control is a mechanism for enforcing one-way information flow, which can be applied to confidentiality or integrity goals**
- **We will use the BLP formulation with high confidentiality at the top of the lattice, and high integrity at the bottom**