TOPIC

LATTICE-BASED ACCESS-CONTROL MODELS

Ravi Sandhu

LATTICE-BASED MODELS

- **Denning's axioms**
- **Bell-LaPadula model (BLP)**
- **Biba model and its duality (or equivalence) to BLP**
- **Dynamic labels in BLP**

DENNING'S AXIOMS

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

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

DENNING'S AXIOMS

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

1 **SC is finite**

2 $\rightarrow$ **is a partial order on SC**

3 **SC has a lower bound L such that L $\rightarrow$ A for all A $\in$ SC**

4 $\oplus$ **is a least upper bound (lub) operator on SC**

Justification for 1 and 2 is stronger than for 3 and 4. In practice we may therefore end up with a partially ordered set (poset) rather than a lattice.

5

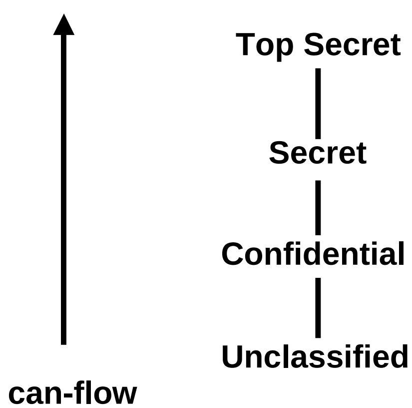
DENNING'S AXIOMS IMPLY

- **SC is a universally bounded lattice**
- **there exists a Greatest Lower Bound (glb) operator ⊗ (also called meet)**
- **there exists a highest security class H**

6

LATTICE STRUCTURES

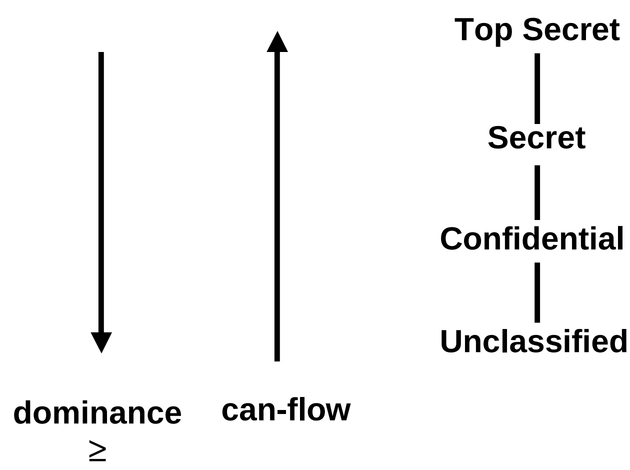
Hierarchical Classes



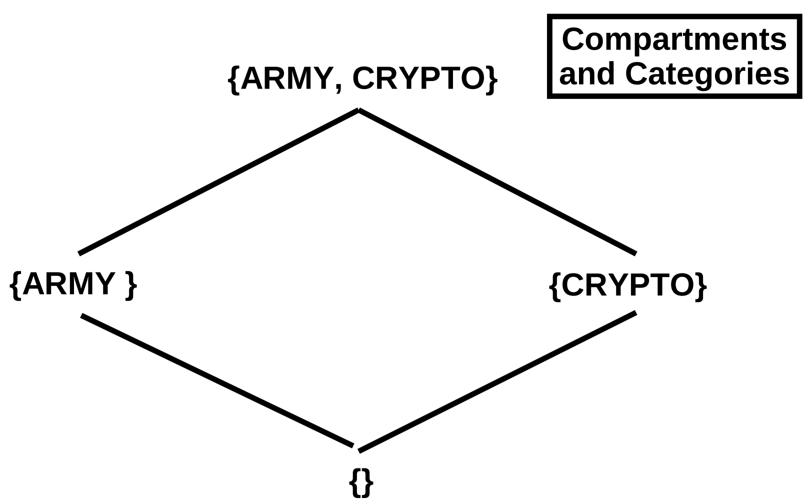
reflexive and transitive edges are implied but not shown

© 1993 Ravi Sandhu

LATTICE STRUCTURES

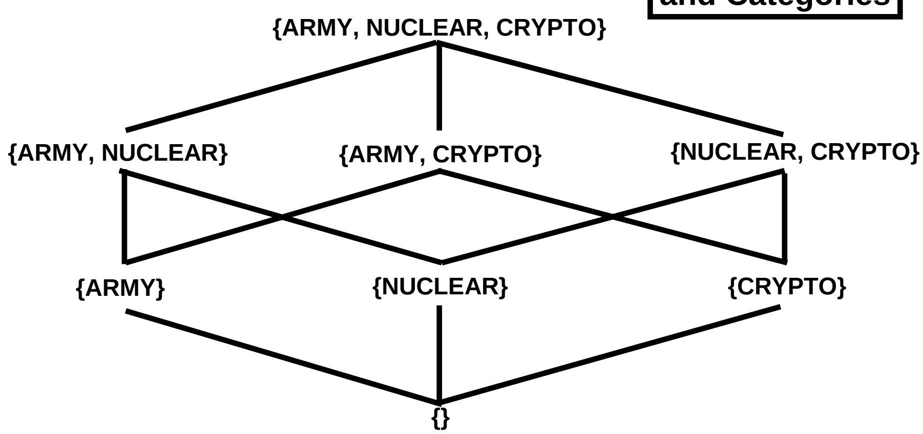


LATTICE STRUCTURES



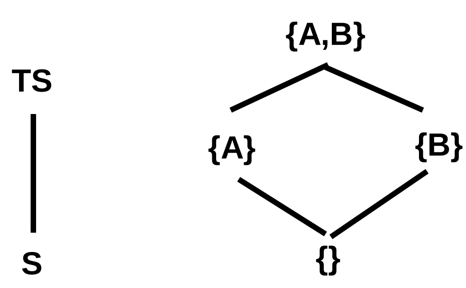
LATTICE STRUCTURES

Compartments and Categories



LATTICE STRUCTURES

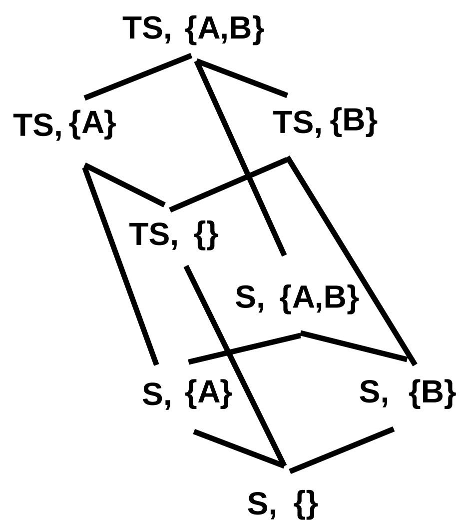
Hierarchical Classes with Compartments

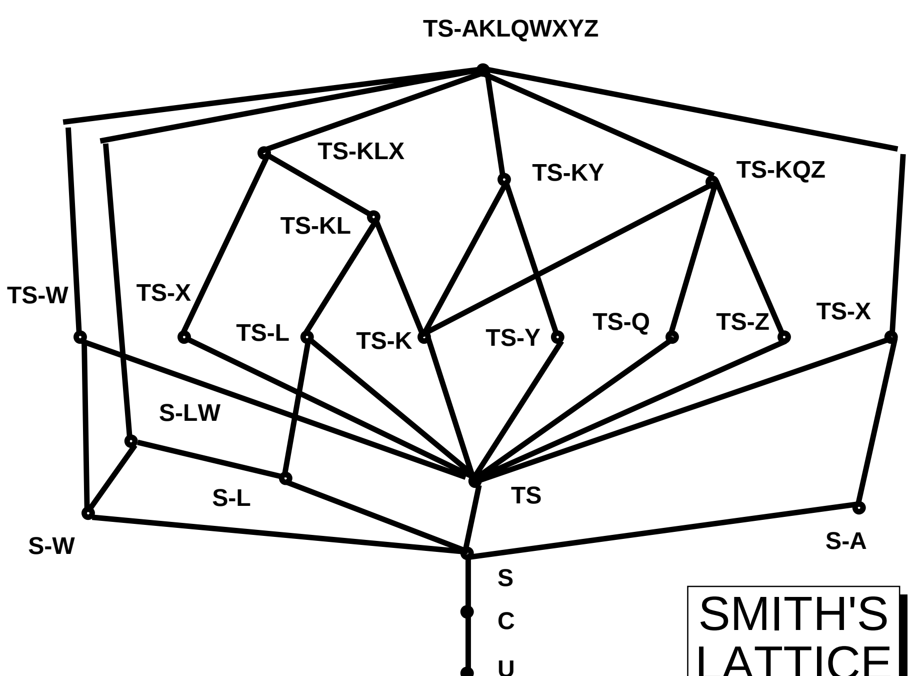


product of 2 lattices is a lattice

LATTICE STRUCTURES

Hierarchical Classes with Compartments





SMITH'S LATTICE

SMITH'S LATTICE

- **With large lattices a vanishingly small fraction of the labels will actually be used**
  - **Smith's lattice: 4 hierarchical levels, 8 compartments, therefore**

    number of possible labels = 4*2^8 = 1024

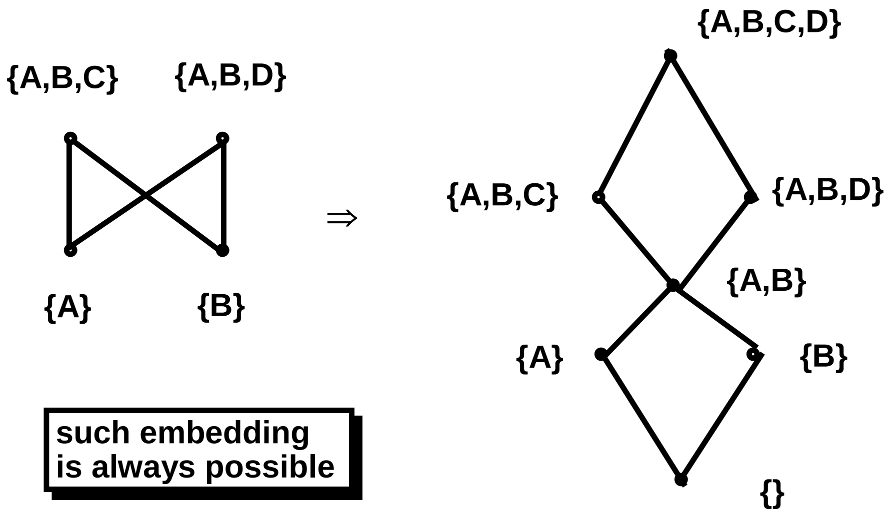
    Only 21 labels are actually used (2%)
  - **Consider 16 hierarchical levels, 64 compartments which gives 10^20 labels**

EMBEDDING A POSET IN A LATTICE

- **Smith's subset of 21 labels do form a lattice. In general, however, selecting a subset of labels from a given lattice**
  - **may not yield a lattice, but**
  - **is guaranteed to yield a partial ordering**
- **Given a partial ordering we can always add extra labels to make it a lattice**

15

EMBEDDING A POSET IN A LATTICE



such embedding is always possible

16

BLP BASIC ASSUMPTIONS

- **SUB = {S1, S2, ..., Sm}, a fixed set of subjects**
- **OBJ = {O1, O2, ..., On}, a fixed set of objects**
- **R $\supseteq$ {r, w}, a fixed set of rights**
- **D, an m $\times$ n discretionary access matrix with D[i,j] $\subseteq$ R**
- **M, an m $\times$ n current access matrix with M[i,j] $\subseteq$ {r, w}**

17

BLP MODEL

- **Lattice of confidentiality labels**

$$\Lambda = \{\lambda 1, \lambda 2, ..., \lambda \mathbf{p}\}$$

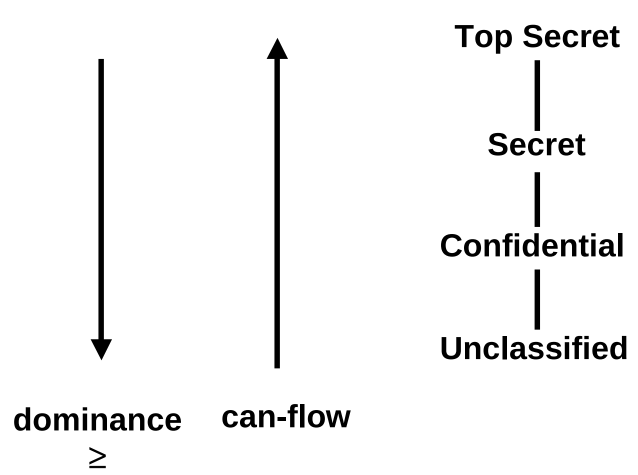
- **Static assignment of confidentiality labels**

$$\lambda\text{: } \mathbf{SUB} \cup \mathbf{OBJ} \rightarrow \Lambda$$

- **M, an m $\times$ n current access matrix with**
  - **r $\in$ M[i,j] $\Rightarrow$ r $\in$ D[i,j] $\wedge$ λ(Si) $\geq$ λ (Oj)** **simple security**
  - **w $\in$ M[i,j] $\Rightarrow$ w $\in$ D[i,j] $\wedge$ λ(Si) $\leq$ λ (Oj)** **star-property**

18

BLP MODEL



STAR-PROPERTY

- **applies to subjects not to users**
- **users are trusted (must be trusted) not to disclose secret information outside of the computer system**
- **subjects are not trusted because they may have Trojan Horses embedded in the code they execute**
- **star-property prevents overt leakage of information and does not address the covert channel problem**

BIBA MODEL

- **Lattice of integrity labels**

$$\Omega = \{\omega 1, \omega 2, ..., \omega \mathbf{q}\}$$

- **Assignment of integrity labels**

$$\omega\text{: } \mathbf{SUB} \cup \mathbf{OBJ} \rightarrow \Omega$$

- **M, an m $\times$ n current access matrix with**
  - **r $\in$ M[i,j] $\Rightarrow$ r $\in$ D[i,j] $\wedge$ ω(Si) $\leq$ ω (Oj)** — **simple integrity**
  - **w $\in$ M[i,j] $\Rightarrow$ w $\in$ D[i,j] $\wedge$ ω(Si) $\geq$ ω(Oj)** — **integrity confinement**

EQUIVALENCE OF BLP AND BIBA

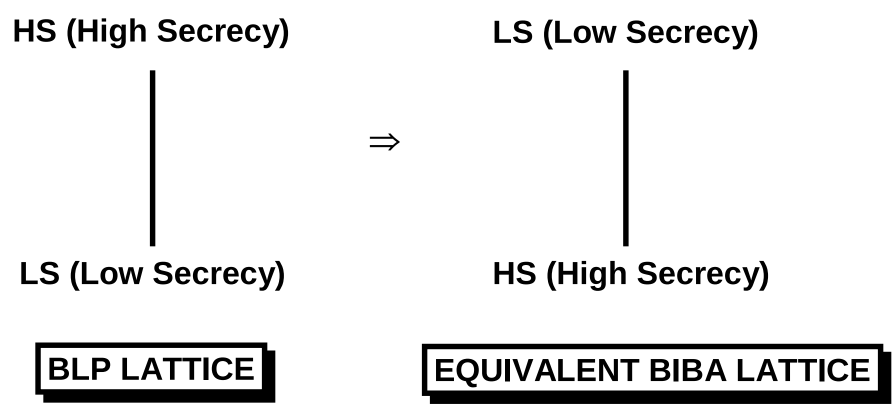
- **Information flow in the Biba model is from top to bottom**
- **Information flow in the BLP model is from bottom to top**
- **Since top and bottom are relative terms, the two models are fundamentally equivalent**

EQUIVALENCE OF BLP AND BIBA

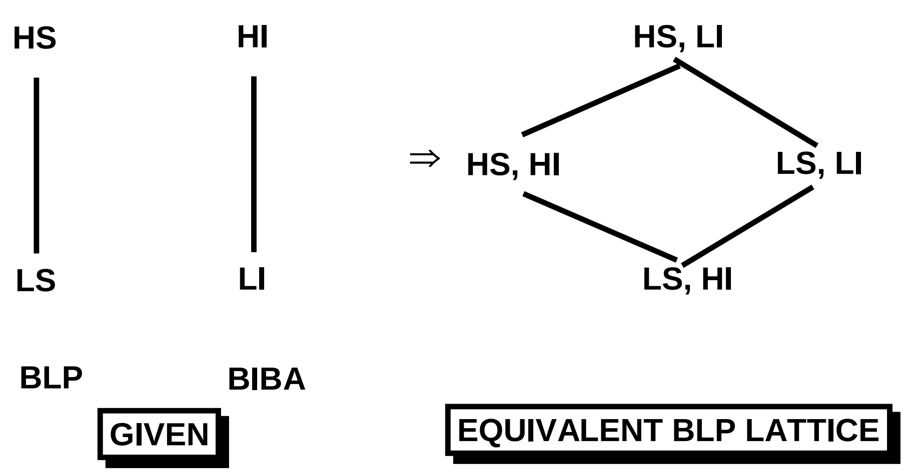
BIBA LATTICE		EQUIVALENT BLP LATTICE
HI (High Integrity)		**LI (Low Integrity)**
|	⇒	|
LI (Low Integrity)		**HI (High Integrity)**

BIBA LATTICE **EQUIVALENT BLP LATTICE**

EQUIVALENCE OF BLP AND BIBA



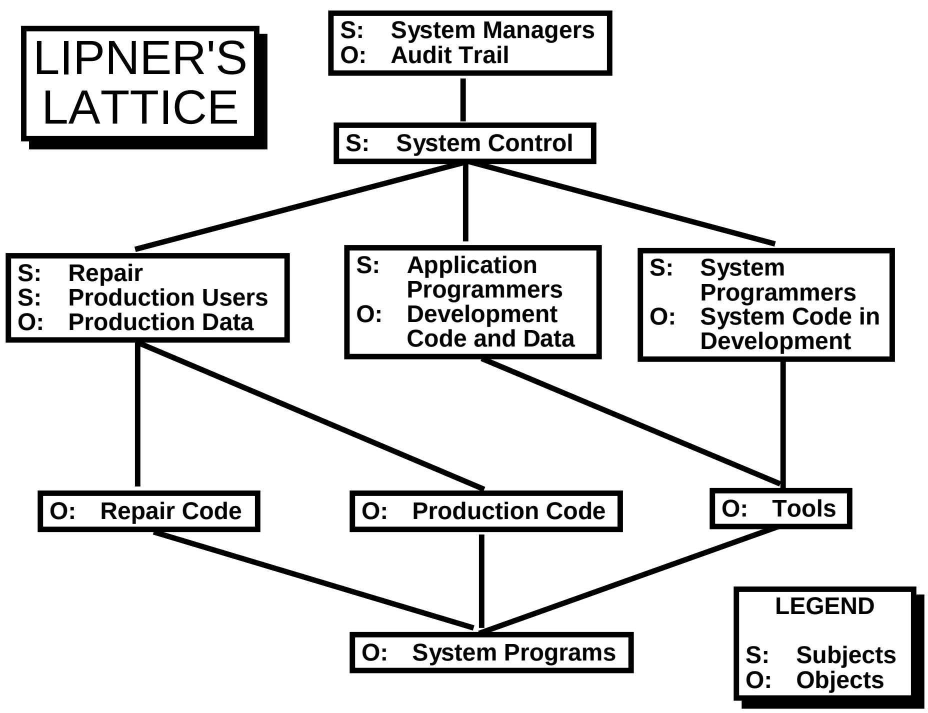
COMBINATION OF DISTINCT LATTICES



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**

LIPNER'S LATTICE



27

LIPNER'S LATTICE

- **Lipner's lattice uses 9 labels from a possible space of 192 labels (3 integrity levels, 2 integrity compartments, 2 confidentiality levels, and 3 confidentiality compartments)**
- **The single lattice shown here can be constructed directly from first principles**

28

LIPNER'S LATTICE

- **The position of the audit trail at lowest integrity demonstrates the limitation of an information flow approach to integrity**
- **System control subjects are exempted from the star-property and allowed to**
  - **write down (with respect to confidentiality)**

  or equivalently
  - **write up (with respect to integrity)**

DYNAMIC LABELS IN BLP

- **Tranquility (most common):**
  λ is static for subjects and objects
- **BLP without tranquility may be secure or insecure depending upon the specific dynamics of labelling**
- **Noninterference can be used to prove the security of BLP with dynamic labels**

DYNAMIC LABELS IN BLP

- **High water mark on subjects:**
  λ is static for objects
  λ may increase but not decrease for subjects

  Is secure and is useful
- **High water mark on objects:**
  λ is static for subjects
  λ may increase but not decrease for subjects

  Is insecure due to disappearing object signaling channel

REFERENCES

- **Ravi Sandhu, "Lattice-Based Access Control Models." Manuscript handed out in class**

© 1993 Ravi Sandhu