1

TOPIC

LATTICE-BASED
ACCESS-CONTROL MODELS

Ravi Sandhu

2

LATTICE-BASED MODELS

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

3

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**

4

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.

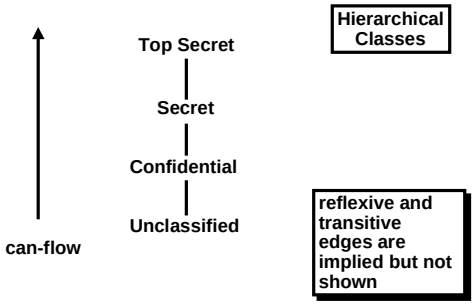
5

DENNING'S AXIOMS IMPLY

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

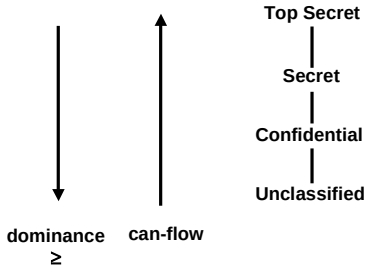
6

LATTICE STRUCTURES



7

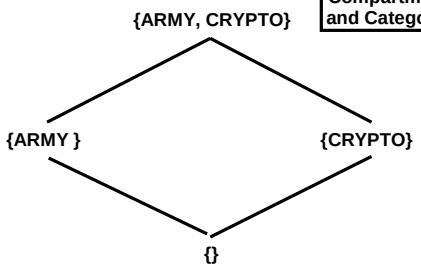
LATTICE STRUCTURES



8

LATTICE STRUCTURES

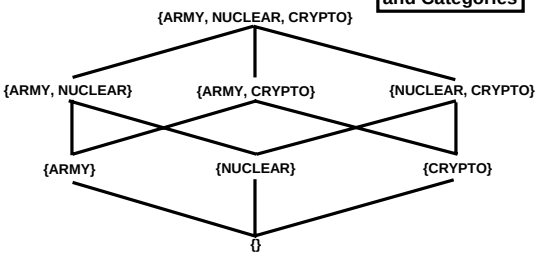
Compartments and Categories



9

LATTICE STRUCTURES

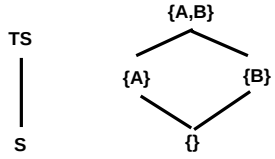
Compartments and Categories



10

LATTICE STRUCTURES

Hierarchical Classes with Compartments

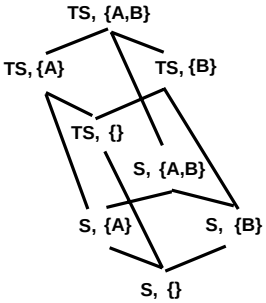


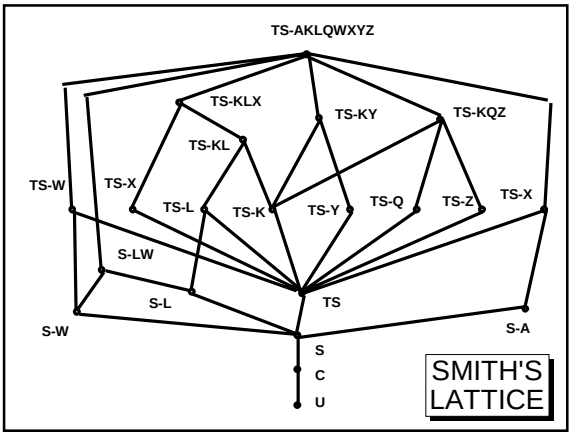
product of 2 lattices is a lattice

11

LATTICE STRUCTURES

Hierarchical Classes with Compartments





13

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

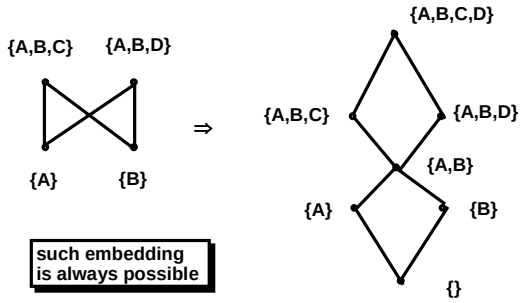
14

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 ⊇ {r, w}, a fixed set of rights
- D, an m × n discretionary access matrix with D[i,j] ⊆ R
- M, an m × n current access matrix with M[i,j] ⊆ {r, w}

17

BLP MODEL

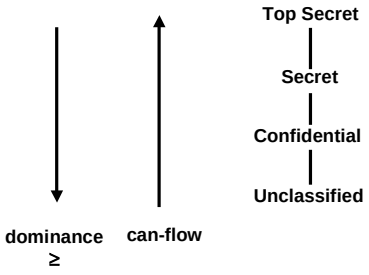
- Lattice of confidentiality labels

  $\Lambda = \{\lambda 1, \lambda 2, ..., \lambda p\}$
- Static assignment of confidentiality labels

  λ: SUB ∪ OBJ → Λ
- M, an m × n current access matrix with
  - $r \in M[i,j] \Rightarrow r \in D[i,j] \wedge \lambda(Si) \geq \lambda(Oj)$ simple security
  - $w \in M[i,j] \Rightarrow w \in D[i,j] \wedge \lambda(Si) \leq \lambda(Oj)$ star-property

18

BLP MODEL



19

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

20

BIBA MODEL

- Lattice of integrity labels

  $\Omega = \{\omega 1, \omega 2, ..., \omega q\}$
- Assignment of integrity labels

  ω: SUB $\cup$ OBJ $\rightarrow \Omega$
- M, an m $\times$ n current access matrix with
  - $r \in M[i,j] \Rightarrow r \in D[i,j] \wedge \omega(Si) \leq \omega(Oj)$ simple integrity
  - $w \in M[i,j] \Rightarrow w \in D[i,j] \wedge \omega(Si) \geq \omega(Oj)$ integrity confinement

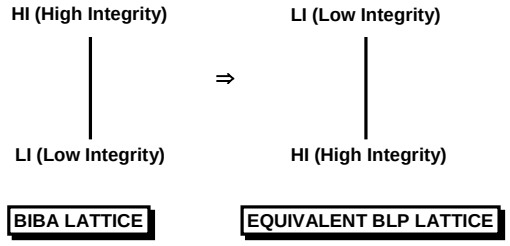
21

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

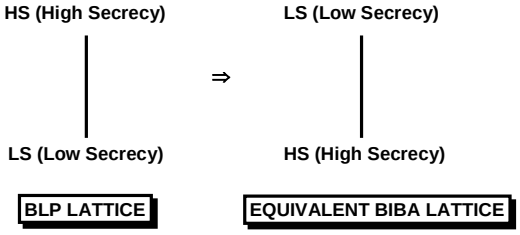
22

EQUIVALENCE OF BLP AND BIBA



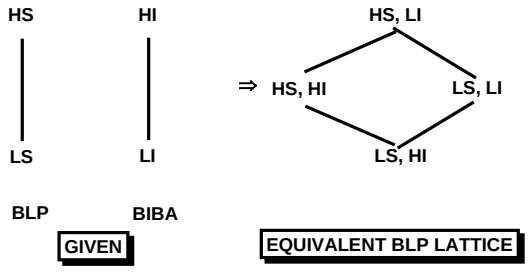
23

EQUIVALENCE OF BLP AND BIBA



24

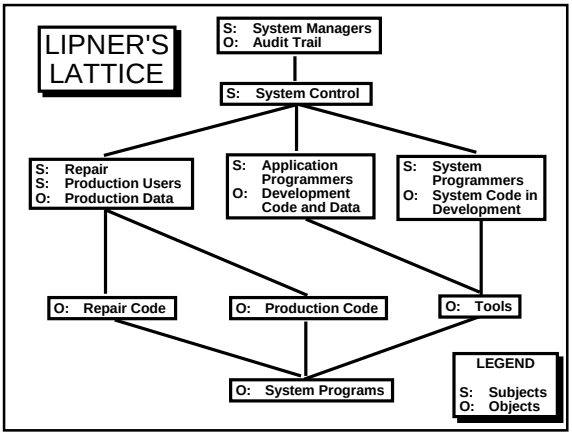
COMBINATION OF DISTINCT LATTICES



25

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**



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)**

29

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**

30

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

31

REFERENCES

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

© 1993 Ravi Sandhu