



# CSC 474/574 Information Systems Security

## Topic 4.2: Lattice Based Access Control Models

## LATTICE-BASED MODELS

- Information flow policies
  - Denning's axioms
- Bell-LaPadula model (BLP)
- Biba model and its duality (or equivalence) to BLP

## Information Flow Policies

- Concerned with the flow of information from one *security class* to another.
  - Not between objects
  - Does such a policy care about
    - Information from *top secret class* to *secret class*?
    - Information from *file A* to *file B*?
- Approach
  - Assign each object a security class (also called a security label).
  - Control information flow between objects based on their labels.
- Information flows from security class A to security class B
  - Information flows from an object labeled A to an object labeled B.

## Denning'S Definition of Information Flow Policy

$\langle SC, \rightarrow, \oplus \rangle$

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

### Intuitions:

$A \rightarrow B$ : Information can flow from security class A to security class B.

$A \oplus B \rightarrow C$ : Information combined from A and B can flow to C.

## Example 1

- High-low policy
  - Information can only flow between each class and from low class to high class, but not from high class to low class
- In Denning's formalism:
  - $SC = \{H, L\}$
  - $\rightarrow = \{ \_, \_, \_ \}$
  - $\oplus = \{H \oplus \_ = \_, \_ \oplus L = \_, L \oplus H = \_, L \oplus L = \_ \}$

## Example 2

- Policy
  - Two departments A and B.
  - Four security classes
    - $\{\}$ : Public information
    - $\{A\}$ : Only people working in A can access
    - $\{B\}$ : Only people working in B can access.
    - $\{A, B\}$ : Only people working in both A and B can access.
  - Never disclose any secret information.
- In Denning's formalism:
  - $SC = \{ \_, \_, \_, \_ \}$
  - $\rightarrow = \{ \_, \_, \_, \_, \_, \_, \_, \_ \}$
  - $\oplus = \{ \_, \_, \_, \_, \_, \_ \}$

## DENNING'S AXIOMS

$\langle SC, \sqsubseteq, \oplus \rangle$

1. SC is finite
2.  $\sqsubseteq$  is a partial order on SC
3. SC has a lower bound L such that  $L \sqsubseteq A$  for all  $A \in SC$
4.  $\oplus$  is a totally defined least upper bound operator on SC

## DENNING'S AXIOMS (Cont'd)

- Axiom 2:  $\sqsubseteq$  is a partial order on SC
  - $\rightarrow$  is reflexive:
    - For all A in SC,  $A \rightarrow A$ .
    - Intuition: Information can flow within each class.
  - $\rightarrow$  is transitive:
    - If  $A \rightarrow B$  and  $B \rightarrow C$ , then  $A \rightarrow C$ .
    - Intuition: If indirect flow is possible from A to C via B, then we should allow directly information flow from A to C.
    - Not always desirable.
  - $\rightarrow$  is anti-symmetric:
    - If  $A \rightarrow B$  and  $B \rightarrow A$ , then  $A=B$ .
    - Intuition: We don't need redundant classes.
    - Equivalently, if  $A \rightarrow B$  and  $A \neq B$ , then  $B \not\rightarrow A$ .

### Example 3

- Which of the following are partial orders?
  - $\{A, B, C\}, A \rightarrow B, B \rightarrow C, A \rightarrow C$
  - $\{A, B, C\}, A \rightarrow A, B \rightarrow B, C \rightarrow C$
  - $\{A, B, C\}, A \rightarrow A, B \rightarrow B, C \rightarrow C, A \rightarrow B$

### DENNING'S AXIOMS (Cont'd)

- Axiom 3: SC has a lower bound  $L$  such that  $L \rightarrow A$  for all  $A$  in SC.
  - Existence of public information in the system.

## DENNING'S AXIOMS (Cont'd)

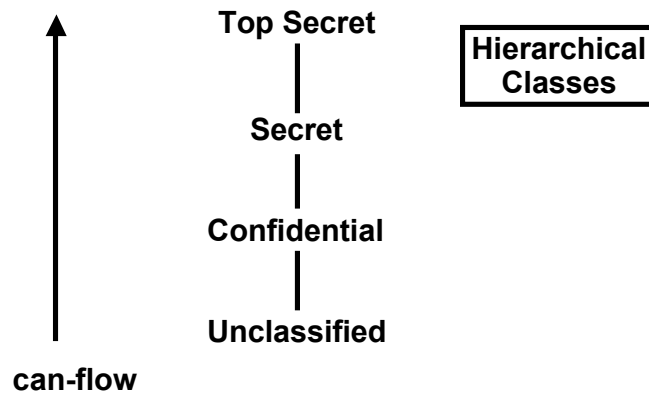
- Axiom 4:  $\oplus$  is a totally defined least upper bound (lub) operator on SC
  - $A \oplus B$  is defined for each pair of A and B in SC.
    - Intuition: It is possible to combine information from any two classes.
  - The  $\oplus$  operator is a least upper bound
    - $A \rightarrow A \oplus B$  and  $B \rightarrow A \oplus B$  for all A, B in SC
    - If  $A \rightarrow C$  and  $B \rightarrow C$ , then  $A \oplus B \rightarrow C$ .
      - $A \oplus B$  is the least one among all the upper bounds of A and B.
  - The  $\oplus$  operator can be applied to any number of security classes.

## DENNING'S AXIOMS IMPLY

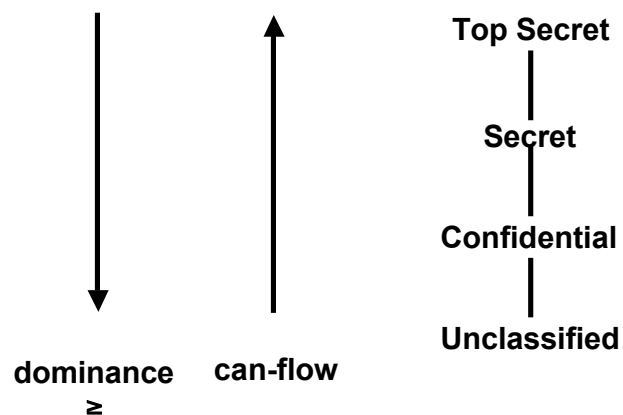
- SC is a universally bounded lattice
- there exists a Greatest Lower Bound (glb) operator (also called meet)
- there exists a highest security class H

## LATTICE STRUCTURES

- reflexive and transitive edges are implied but not shown



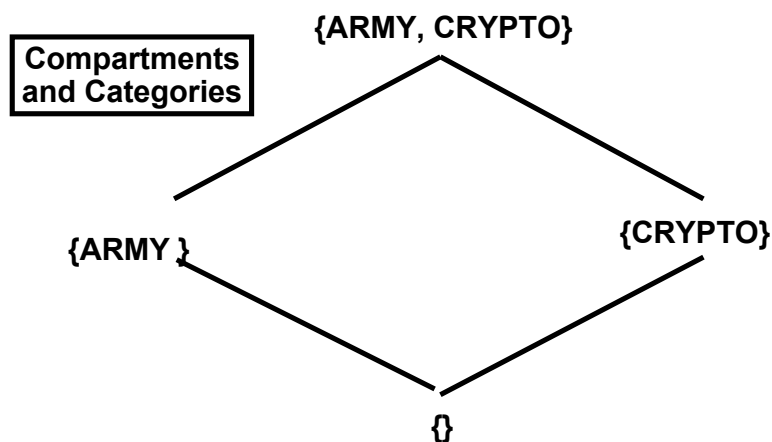
## LATTICE STRUCTURES



## Categories and Compartments

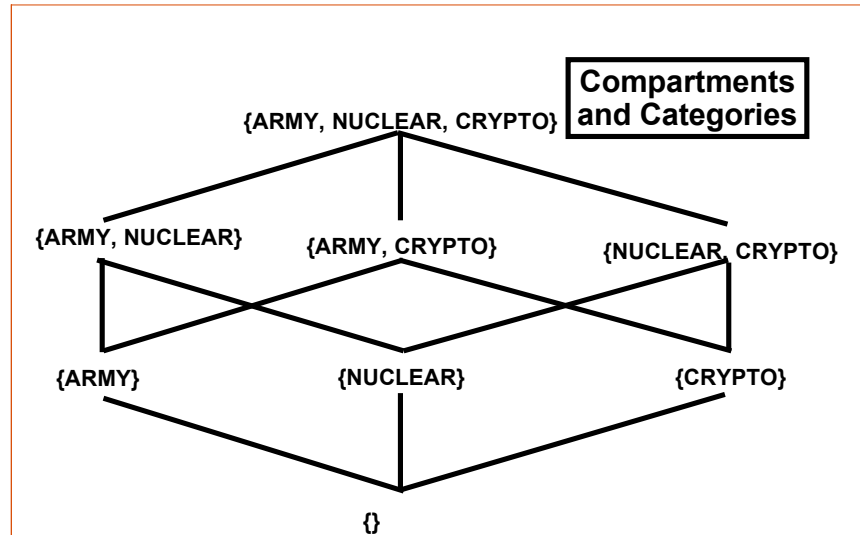
- Categories: individual elements
- Compartments: set of categories.
  - The set of compartments is the power set of the set of categories.
  - Compartments form a subset lattice over the set of categories.
- Example:
  - The set of categories: {A, B}
  - The set of Compartments:
    - { \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_ }

## LATTICE STRUCTURES





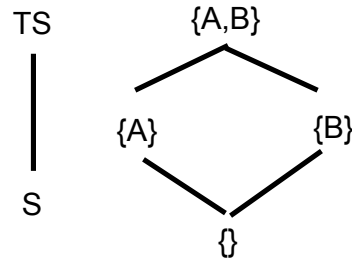
## LATTICE STRUCTURES



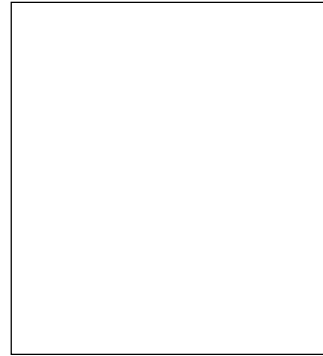
## Combining Different Lattices

- Two lattices  $L1 = (SC1, \rightarrow, \sqsubseteq)$  and  $L2 = (SC2, \rightarrow, \sqsubseteq)$  can be combined into  $L = (SC, \rightarrow, \sqsubseteq)$  as follows:
  - $SC = SC1 \sqcup SC2$ 
    - Intuition: The result security classes are all combinations of those in  $L1$  and  $L2$ .
  - For  $(c1, c2)$  and  $(c1', c2')$  in  $SC$ ,  $(c1, c2) \rightarrow (c1', c2')$  if and only if  $c1 \rightarrow c1'$  and  $c2 \rightarrow c2'$ .
    - Intuition: Information can flow from  $(c1, c2)$  to  $(c1', c2')$  if and only if  $L1$  permits information flow from  $c1$  to  $c1'$  and  $L2$  permits information flow from  $c2$  to  $c2'$ .
  - $(c1, c2) \sqsubseteq (c1', c2') = (c1 \sqsubseteq c1', c2 \sqsubseteq c2')$ .
    - Intuition: Combining security classes in  $L$  is equivalent to combining security classes in  $L1$  and  $L2$  separately.

## LATTICE STRUCTURES



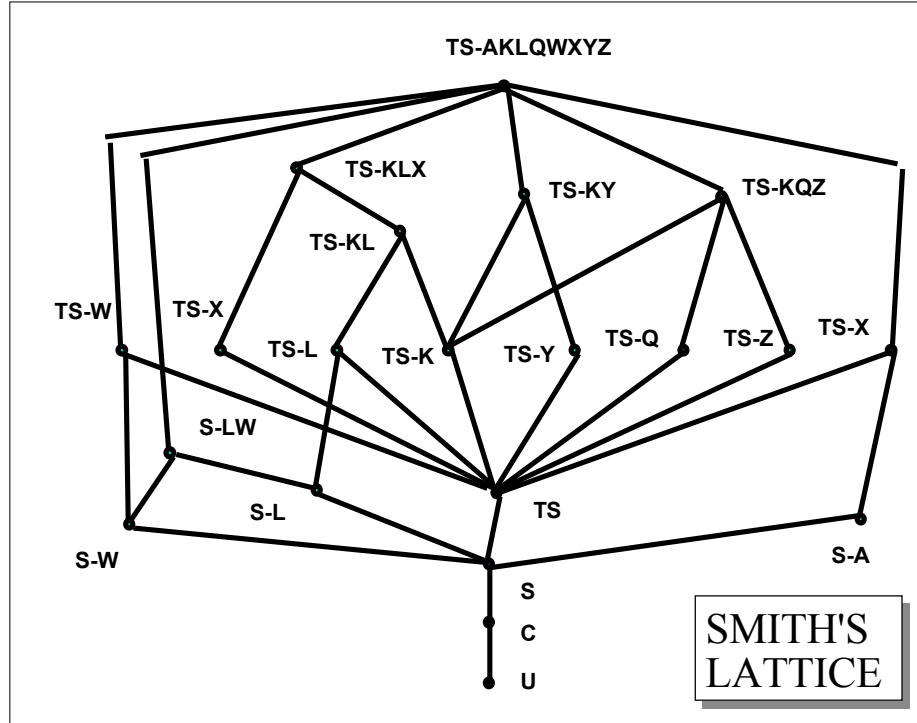
Combined Lattice:



The product of the two lattices.

## SMITH'S LATTICE

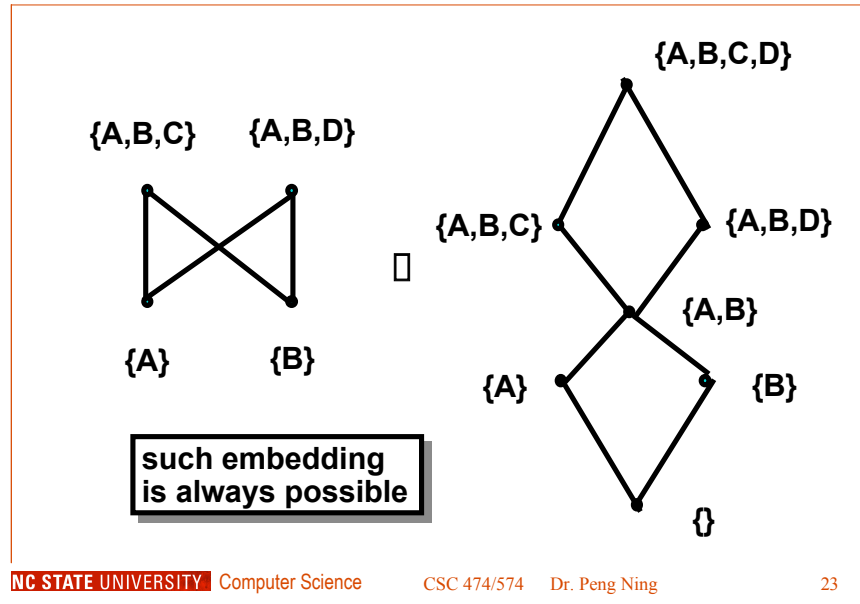
- With large lattices a vanishingly small fraction of the labels will actually be used
- Smith's lattice: 4 hierarchical levels, 8 compartments, therefore
  - number of possible labels =  $4 \cdot 2^8 = 1024$
  - Only 21 labels are actually used (2%)
  - Consider 16 hierarchical levels, 64 compartments 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

## EMBEDDING A POSET IN A LATTICE



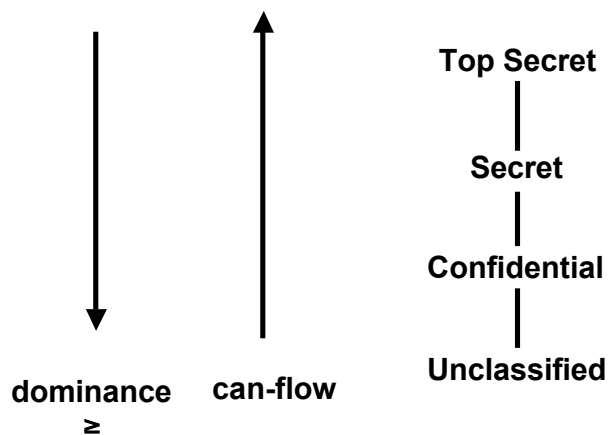
## BELL LAPADULA (BLP) MODEL

- SIMPLE-SECURITY — Subject  $S$  can read object  $O$  only if
  - $\text{label}(S)$  dominates  $\text{label}(O)$
  - information can flow from  $\text{label}(O)$  to  $\text{label}(S)$
- STAR-PROPERTY — Subject  $S$  can write object  $O$  only if
  - $\text{label}(O)$  dominates  $\text{label}(S)$
  - information can flow from  $\text{label}(S)$  to  $\text{label}(O)$

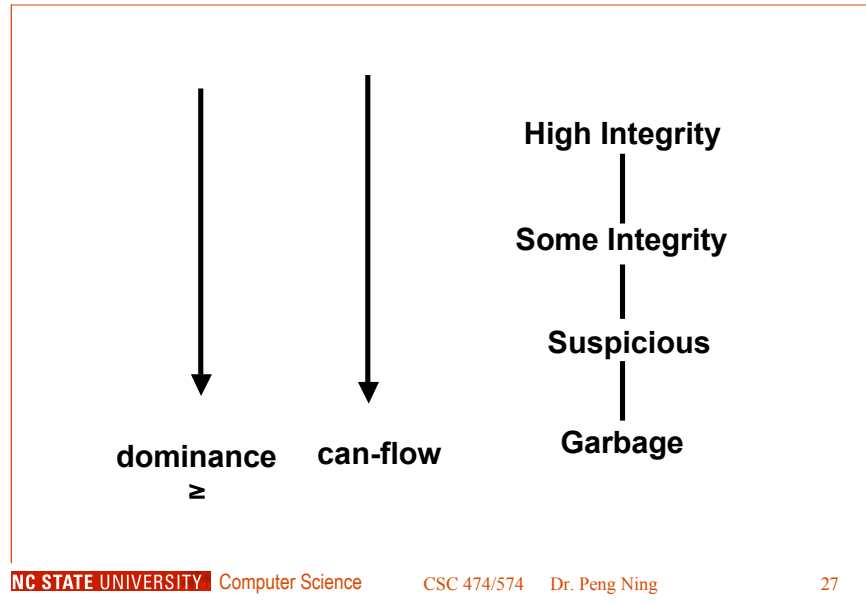
## STAR-PROPERTY

- applies to subjects (principals) 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

## BLP MODEL



## BIBA MODEL



## BIBA MODEL

- **SIMPLE-INTEGRITY** — Subject S can read object O only if
  - label(O) dominates label(S)
  - information can flow from label(O) to label(S)
- **STAR-PROPERTY** — Subject S can write object O only if
  - label(S) dominates label(O)
  - information can flow from label(S) to label(O)

## 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

HI (High Integrity)



LI (Low Integrity)

**BIBA LATTICE**

LI (Low Integrity)



HI (High Integrity)

**EQUIVALENT BLP LATTICE**



## EQUIVALENCE OF BLP AND BIBA

HS (High Secrecy)

LS (Low Secrecy)



LS (Low Secrecy)

HS (High Secrecy)

**BLP LATTICE**

**EQUIVALENT BIBA LATTICE**

## COMBINATION OF DISTINCT LATTICES

HS

HI

HS, LI



HS, HI

LS, LI

LS, HI

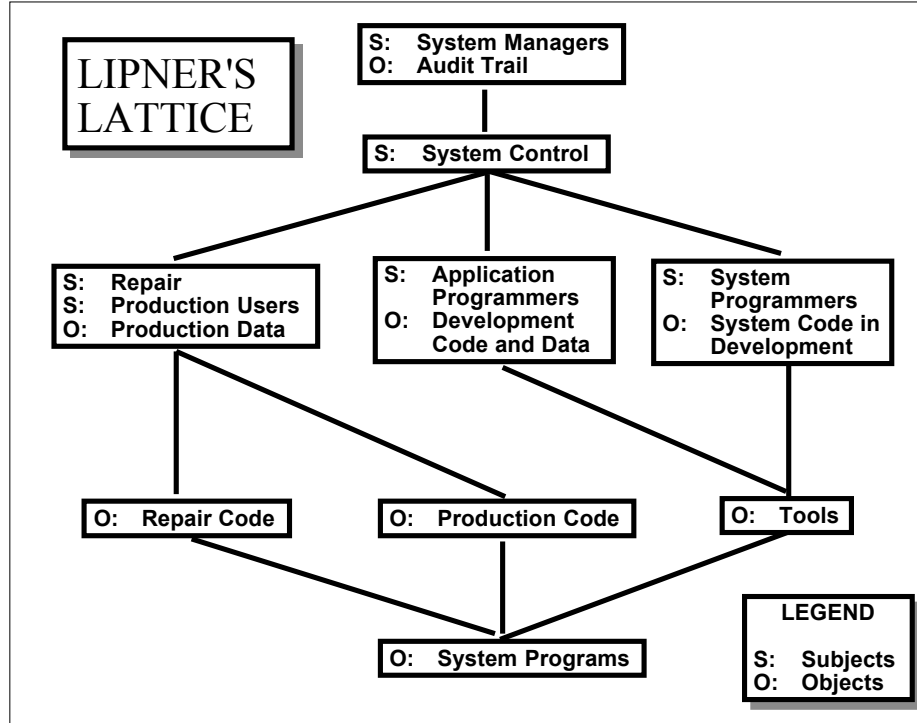
BLP

BIBA

**GIVEN**

**EQUIVALENT BLP LATTICE**





## 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

## 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)