

Information Flow

Execution of α causes information flow from object X to object Y if information about the value of X can be determined from the value of Y after executing α .

Denoted: $X \xrightarrow{\alpha} Y$

Explicit and Implicit Flows

- $X \longrightarrow Y$ is explicit whenever the operation generating the flow is independent of the value of X
- $X \longrightarrow Y$ is implicit whenever there is an operation generating a flow from an arbitrary Z to Y and the operation is dependent on the value of X

Notation

X The value stored in object X

\underline{X} The security class of X

$\underline{X} \Rightarrow \underline{Y}$ Information flow is allowed from class \underline{X} to class \underline{Y} by the information flow policy

$X \xrightarrow{\alpha} Y$ is secure iff $\underline{X} \Rightarrow \underline{Y}$

Information Flow Policy

A set of rules governing information flow among a set of objects, each of which has a unique security class that belongs to the set of security classes SC .

Partially Ordered Set (poset)

A relation R that satisfies

- Reflexivity

$$aRa$$

- Transitivity

$$aRb \ \& \ bRc \ \rightarrow \ aRc$$

- Anti-symmetric

$$aRb \ \& \ bRa \ \rightarrow \ a=b$$

Lattice

A lattice is a partially ordered set S such that
 $\forall A, B \in S$

- i) \exists unique least upper bound of A, B
- ii) \exists unique greatest lower bound of A, B

Notation

⊕

LUB

least upper bound

⊗

GLB

greatest lower bound

Linear Lattice

$$SC = \{0,1,2,3\}$$

$$\forall \underline{A}, \underline{B} \in SC$$

$$\underline{A} \Rightarrow \underline{B} \text{ iff } \underline{A} \leq \underline{B}$$

$$\underline{A} \oplus \underline{B} = \max(\underline{A}, \underline{B})$$

$$\underline{A} \otimes \underline{B} = \min(\underline{A}, \underline{B})$$



Subset Lattice

$SC = \{S \mid S \text{ is a subset of } \{cs, ece, math\}\}$

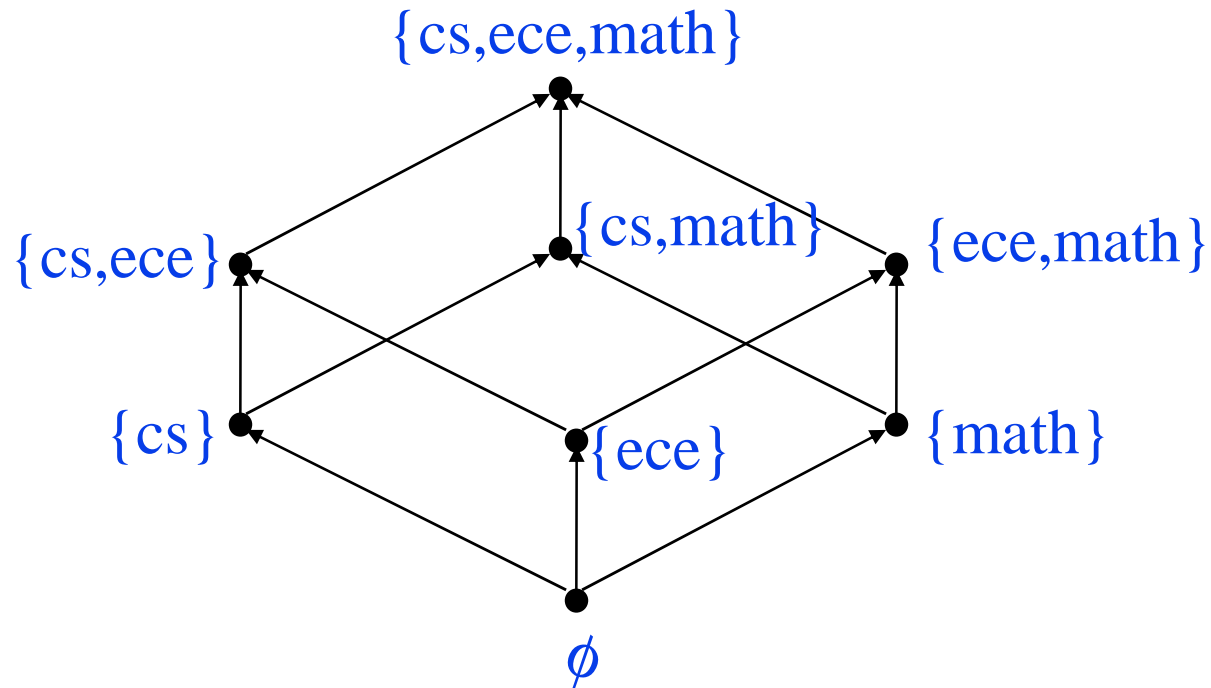
$\forall \underline{A}, \underline{B} \in SC$

$\underline{A} \Rightarrow \underline{B} \text{ iff } \underline{B} \supseteq \underline{A}$

$\underline{A} \oplus \underline{B} = \underline{A} \cup \underline{B}$

$\underline{A} \otimes \underline{B} = \underline{A} \cap \underline{B}$

Subset Lattice



Linear x Subset Lattice

$SC = \{(t,s) \mid t \in \{0,1,2\}, s \text{ is a subset of } \{A,N\}\}$

$\forall (t,s),(k,j) \in SC$

$(t,s) \Rightarrow (k,j) \text{ iff}$

$(t,s) \oplus (k,j) =$

$(t,s) \otimes (k,j) =$

Linear Lattice Revisited

$$SC = \{U, C, S, TS\}$$

$$\forall \underline{A}, \underline{B} \in SC$$

$$\underline{A} \Rightarrow \underline{B} \text{ iff } \underline{A} \leq \underline{B}$$

$$\underline{A} \oplus \underline{B} = \max(\underline{A}, \underline{B})$$

$$\underline{A} \otimes \underline{B} = \min(\underline{A}, \underline{B})$$



Subset Lattice Revisited

$SC = \{S \mid S \text{ is a subset of } \{\text{crypto}, \text{nuclear}, \text{intel}\}\}$

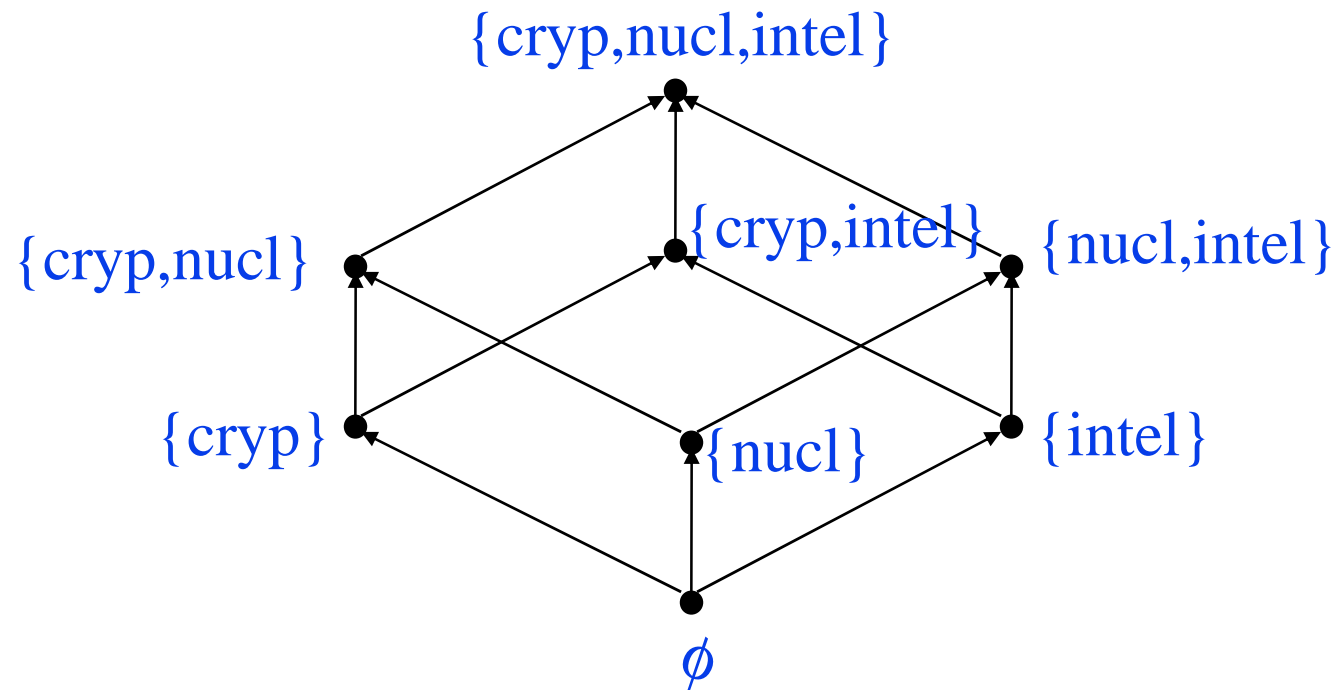
$\forall \underline{A}, \underline{B} \in SC$

$\underline{A} \Rightarrow \underline{B} \text{ iff } \underline{B} \supseteq \underline{A}$

$\underline{A} \oplus \underline{B} = \underline{A} \cup \underline{B}$

$\underline{A} \otimes \underline{B} = \underline{A} \cap \underline{B}$

Subset Lattice Revisited



DoD Secrecy Policy

$SC = \{(i,j) \mid i \in \{U,C,S,TS\},$
 $j \text{ is a subset of } \{\text{crypto,nuclear,intel}\}\}$

$\forall (i,j),(k,l) \in SC$

$(i,j) \Rightarrow (k,l)$ iff $i \leq k$ and $l \supseteq j$

$(i,j) \oplus (k,l) = (\max(i,k), j \cup l)$

$(i,j) \otimes (k,l) = (\min(i,k), j \cap l)$

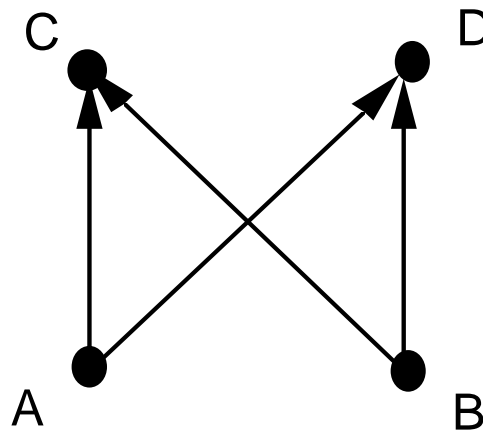
Necessary properties for an information flow policy to be modeled by a lattice are:

1) SC must have a universal upperbound and a universal lower bound

2) $\forall \underline{A}, \underline{B} \in S, \underline{A} \oplus \underline{B}$ and $\underline{A} \otimes \underline{B}$ must be unique

3) \Rightarrow must be anti-symmetric

Consider



Consider

