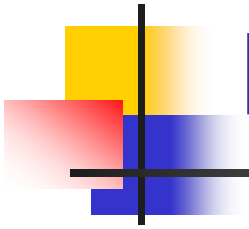
CS590U

Access Control: Theory and Practice

Lecture 4 (Jan 20)

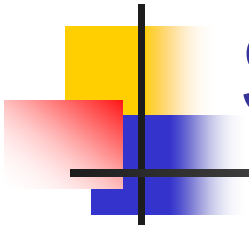
Partial Order, Lattices, and Security Labels



Review: Kripke Structures

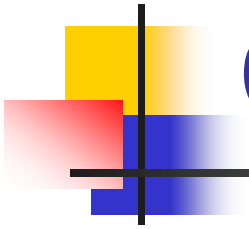
- Let AP be a set of atomic propositions. A Kripke structure M over AP is a four-tuple
  - S is finite set of states
  - $S_0 \subseteq S$ is the set of initial states
  - $R \subseteq S \times S$ is a transition relation
  - $L: S \rightarrow 2^{AP}$ is a function that labels each state with the set of atomic propositions true in that state
- Often times, R is required to be total
  - $\forall s \; \exists s' \; (s,s') \in R$

New Definition: A Family of State Transition Systems

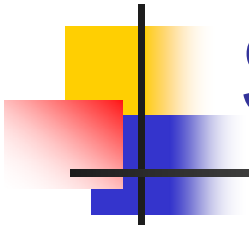


- Given by $(\Gamma, \Psi, Q, \Rightarrow)$
  - Γ a set of states
  - Ψ a set of state-transition rules
    - each $\psi \in \Psi$ is a binary relation over Γ
  - Q a set of queries
  - $\Rightarrow$ $\Gamma \times Q \rightarrow \{true, false\}$
    - whether a query is true or false in a particular state
- Each pair (γ, ψ) is a state-transition system

Bell-LaPadula: Secure Computer System

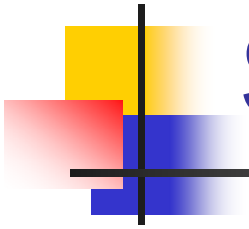


- Model computer systems
  - use state-transitional systems
  - GO TO THE LAST FEW SLIDES OF LECTURE 3
- Define a notion of a secure state
  - no-read-up, no-write-down, every access is allowed by the access matrix
- Define that a computer system is secure if every reachable state is secure
- Prove a Basic Security Theorem



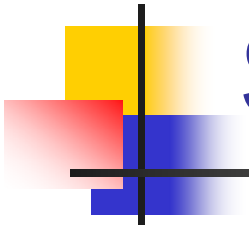
Security Levels

- Used as attributes of both subjects & objects
  - clearance & classification
- Typical military security levels:
  - top secret $\geq$ secret $\geq$ confidential $\geq$ unclassified
- Typical commercial security levels
  - restricted $\geq$ proprietary $\geq$ sensitive $\geq$ public



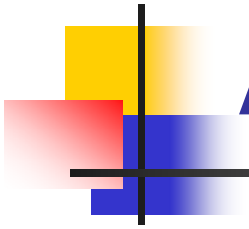
Security Categories

- Also known as compartments
- Typical military security categories
  - army, navy, air force
  - nato, nasa, noforn
- Typical commercial security categories
  - Sales, R&D, HR
  - Dept A, Dept B, Dept C



Security Labels

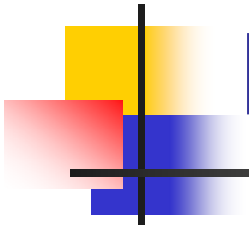
- Labels = Levels $\times$ P (Categories)
- Define an ordering relationship among Labels
  - (e1, C1) $\leq$ (e2, C2) iff. e1 $\leq$e2 and C1 $\subseteq$ C2



An Example

- levels={confidential,secret}
- categories={army,navy}

Go through the Partial Order & Lattices Handout



End of Lecture 4

- Next lecture:
  - Bell-LaPadula