Bell-LaPadula Model

Lattice Models

- **Lattice Model**
  - subjects
  - objects
  - security classes (SC)
  - (object x is in security class y)

- **Flow Policy**:
  - (SC, \rightarrow)
  - \rightarrow is a reflexive, antisymmetric, transitive relation over SC
  - information is allowed to flow from object x to object y iff x \rightarrow y

**Lattice Flow Policy**
- A flow policy is a lattice if there exists least upper bound and greatest lower bounds on SC

An Example Lattice

Certification of Information Flow

For:

- \( b = f(a_1, \ldots, a_n) \)
- verify that:
  - \( a_1 + \ldots + a_n \rightarrow b \)

For:

- if \( e \) then \( S_1 \) else \( S_2 \)
- verify that:
  - \( e \rightarrow S_1 \times S_2 \)
  - where:
    - \( S_1 = \{ b \mid b \text{ is a target of an assignment in } S_1 \} \)
    - \( S_2 = \{ b \mid b \text{ is a target of an assignment in } S_2 \} \)