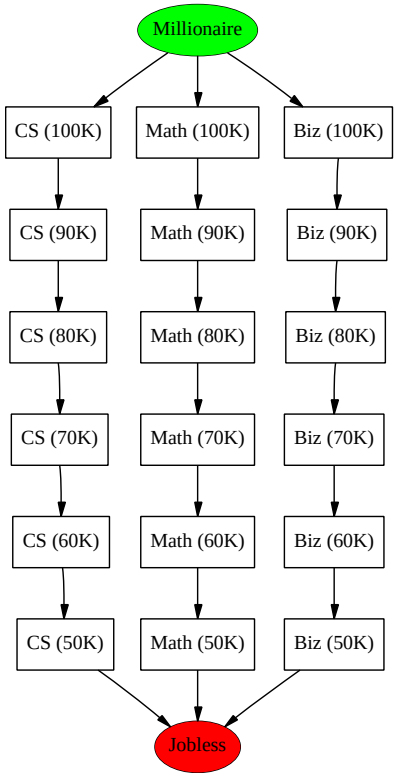
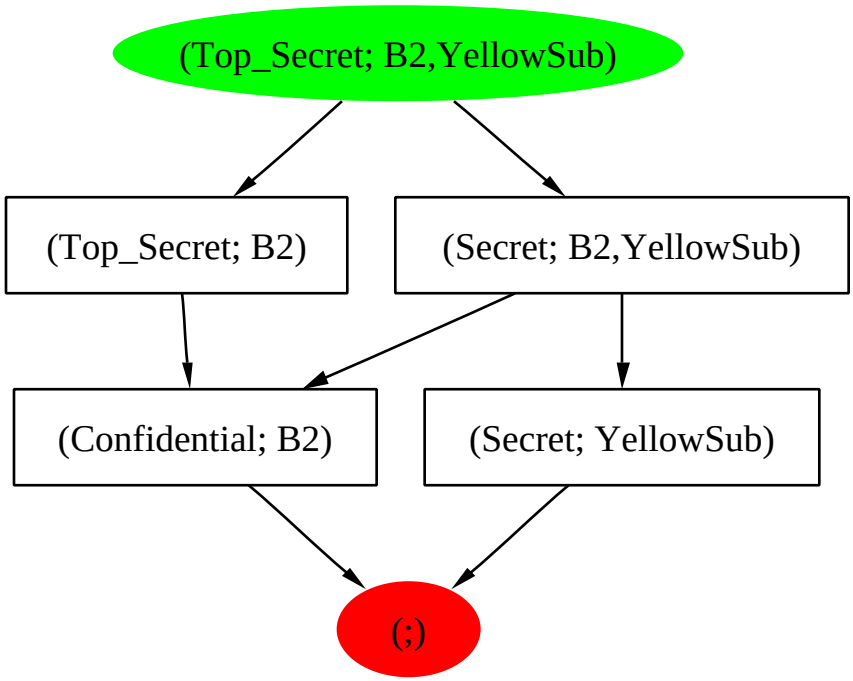
What is a Lattice?

Consider the relation "smarter than" in the following diagram.



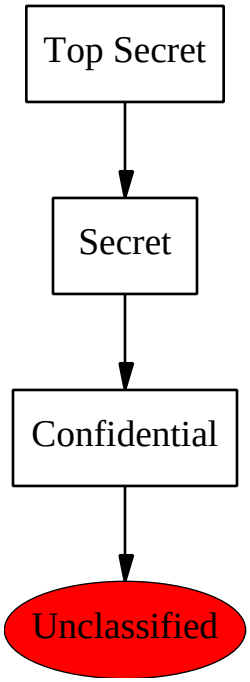
- $\longrightarrow$ is reflexive and transitive.
- $\longrightarrow$ is antisymmetric.
- Not every pair of elements is comparable.
- $\forall a, b \; \exists$ unique least upper bound $x \mid x \geq a$ **and** $x \geq b$.
- $\forall a, b \; \exists$ unique greatest lower bound $y \mid y \leq a$ **and** $y \leq b$.

A Military Security Lattice?



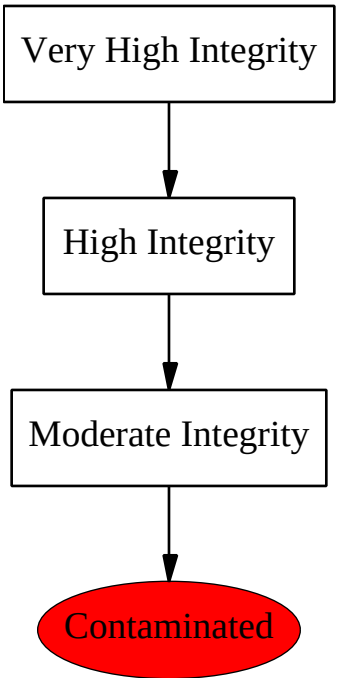
- Top Secret $\geq$ Secret $\geq$ Confidential $\geq$ Unclassified.
- Someone authorized for the B2 bomber need not know about the Yellow submarine.

Bell-La Padula



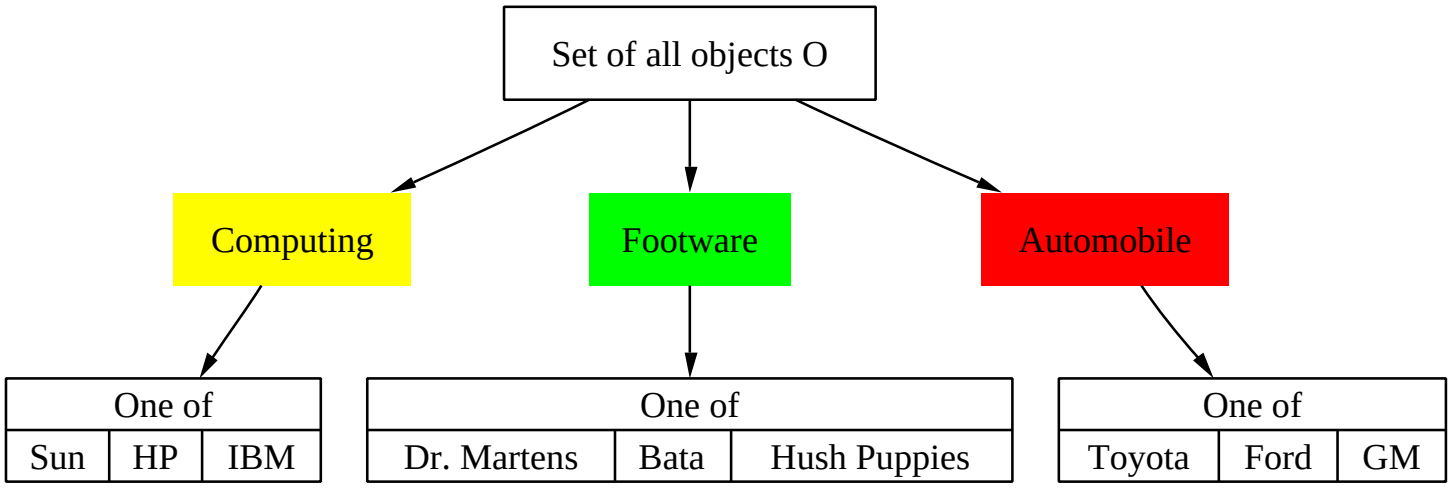
- Intended for confidentiality.
- Information only flows "up".
  - ss: can only read down.
  - $\star$: can only write up.
- Level$(x, y, z, \ldots)$ = max(Level(x), Level(y),...).

Biba



- Intended for integrity. For e.g., contamination in a wafer fab plant.
- Information only flows "down".
  - ss: can only write down.
  - $\star$: can only read up.
- Level$(x, y, z, \ldots) = \min($Level$(x)$, Level$(y), \ldots)$.

Chinese Wall



- Intended for "conflict of interest" type policies.
- Access not constrained by attributes of data, but by what subject already holds access rights to.
- Information doesn't flows within a conflict class.
  - ss: can only access one data set within a conflict class.
  - $\star$: cannot read from a different company dataset than the one to which write access is requested.

    If you can change information about "Sun", then you can't read from "Bata" or "Ford".

Clark Wilson

- Intended primarily for commercial integrity settings.

  > For that core of commercial data processing that relates to management and accounting for assets, preventing fraud and error is the primary goal [CW87].

- Well-formed transaction and Separation of durty.
  - Users should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data.
  - Separate all operations into subparts and require each subpart to be executed by a different person.
  - A data item is not necessarily associated with a particular security level, but rather with a set of programs permitted to manipulate it.

    Implemented as (user, program) determine which objects can be written to.

References

[CW87] David D. Clarke and David R. Wilson. A comparison of commercial and military computer security policies. *IEEE Symposium on Research in Security and Privacy*, pages 184–194, 1987.