# Foundations of Computer Security

## Lecture 12: Lattice-Based Security and the BLP Metapolicy

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

## Lattice Based Security

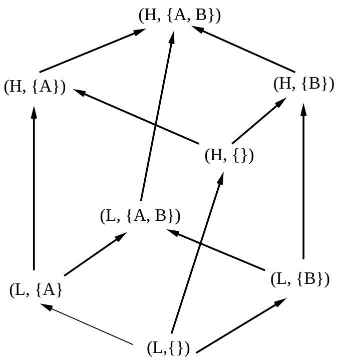
Recall that the set of labels within our MLS system form a partial order under the dominates relation. The following is also true:

1. any two elements have a least upper bound (supremum or join), and
2. any two elements have a greatest lower bound (infimum or meet).

Thus, the set of labels form an algebraic structure called a *lattice*.

## A Lattice

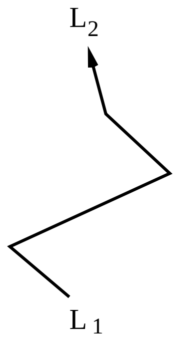
Assume a BLP system with hierarchical levels $\{H, L\}$ (with $H > L$) and categories $\{A, B\}$. On the right is a directed graph representation of the resulting lattice of labels.



The arrows represent (some of) the dominates relationships among the labels. If there is an path from $L_1$ to $L_2$ in the graph, then $L_1 \leq L_2$.

To simplify the picture, it does not include the reflexive or transitive arrows.

## The BLP Metapolicy



A path in the graph from $L_1$ to $L_2$ means that "information is allowed to flow" from level $L_1$ to level $L_2$. That can happen in either of two ways:

1. a subject at level $L_2$ can read a level $L_1$ object, or
2. a subject at level $L_1$ can write a level $L_2$ object.

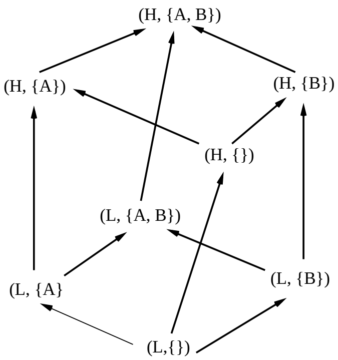
If no such path exists from $L_1$ to $L_2$, then Simple Security should prevent 1 and the *-Property should prevent 2.

## So What is the Metapolicy?

Recall that a metapolicy is the collection of *overall security goals of the system*.

So for any Bell and LaPadula system, we only want information to flow "upward" in the lattice of security levels. Equivalently, information may flow from $L_1$ to $L_2$ only if $L_2 \geq L_1$.

Any other flow indicates a violation of the security goals.



## The Bottom Line

The metapolicy of any BLP system is to constrain the flow of information among the different security levels.

Recall that the metapolicy is *what we really care about* from the security standpoint.

So, if we can build a system that satisfies the BLP rules yet still violates the metapolicy, the BLP rules must not be enough!

## Lessons

- BLP is a collection of access control rules: Simple Security, *-Property, some version of Tranquility.
- The set of BLP labels under dominates forms a *lattice*; such a policy is an instance of *lattice-based security*.
- The overall goal of BLP (the metapolicy) is to constrain the flow of information among the different security levels within the lattice.
- The metapolicy gives us a means of evaluating whether the BLP rules are up to the job.

**Next lecture:** Covert Channels