

# Foundations of Computer Security

## Lecture 20: Modeling Integrity

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

Suppose we associate *integrity labels* with subjects and with objects in our system. The label should reflect the trustworthiness of the subject or reliability of the information in the object.

**Important proviso:** integrity labels are *not also clearance labels*. In a system that enforces both integrity and confidentiality, subjects/objects must have labels for each.

For example, a piece of information may be of dubious validity but very sensitive, or highly reliable and of little sensitivity.

# Structure of Integrity Labels

*What do the labels look like?* According to one popular model, integrity labels look like BLP confidentiality labels.

- A *hierarchical* component gives the level of trustworthiness.
- A set of *categories* provides a list of domains of relevant competence.

For example, a physics professor might have integrity label:

**(Expert: {Physics})**

meaning that she has a very high degree of credibility *in her area of expertise*.

But there's no particular reason to trust her opinion on a matter of politics or animal husbandry.

# Dominates

Since integrity labels have the same structure as BLP labels, the dominates relation applies. It is *defined exactly as with confidentiality*.

Assume an ordered set of hierarchical levels: **Novice**, **Student**, **Expert**. Which of these are such that **Label 1** dominates **Label 2**?

| Label 1                  | Label 2              | Dominates? |
|--------------------------|----------------------|------------|
| (Expert: {Physics})      | (Student: {Physics}) | Yes        |
| (Novice: {Physics, Art}) | (Expert: {Physics})  | No         |
| (Student: {Art})         | (Novice: {})         | Yes        |

# The Integrity Metapolicy

As with MLS, we want to define an access control policy that implements the security (integrity) goals of the system. *But what are the rules?*

Recall with MLS, the BLP rules were really designed to constrain the *flow of information* within the system. We called that the “metapolicy.” *So what is the metapolicy for integrity?*

**Possible answer:** Don't allow bad information to “taint” good information. An alternative formulation is: don't allow information to “flow up” in integrity.

# The Metapolicy: Implications

On analogy with BLP, bad (low integrity) information can flow into a good (high integrity) object if:

- 1 a low integrity subject writes bad information into a high integrity object; or
- 2 a high integrity subject reads bad information from a low integrity object.

This suggests, by analogy with the BLP rules, a subject shouldn't be allowed to "write up" in integrity or to "read down" in integrity.

- We can treat integrity by analogy with confidentiality and construct labels as we did with BLP.
- However, confidentiality and integrity are orthogonal issues; we have to treat them separately.
- A possible integrity metapolicy is this: *information should not flow up in integrity.*

**Next lecture:** Modeling Integrity: Biba