Foundations of Computer Security

Lecture 8: MLS Example: Part III

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

MLS Thought Experiment

Recall that we've assigned sensitivity labels to documents and clearances to individuals within our MLS environment. Now we're attempting to answer the following confidentiality question:

How are the permissions administered and checked? According to what rules?

Clearance	Sensitivity
(Secret: {Crypto})	**(Confidential: {Crypto})**
(Secret: {Crypto, Nuclear})	**(Top Secret: {Crypto})**

A Little Vocabulary

In the type of security policy we're constructing, the following terms are often used:

Objects: the information containers protected by the system (documents, folders, files, directories, databases, etc.)

Subjects: entities (users, processes, etc.) that execute activities and request access to objects.

Actions: operations, primitive or complex, executed on behalf of subjects that may affect objects.

The *subjects* in our MLS example are the humans; the *objects* are the folders containing information.

The Dominates Relation

Given a set of security labels (L, S), comprising hierarchical levels and categories, we can define an ordering relation among labels.

Definition: (L_1, S_1) *dominates* (L_2, S_2) iff

1. $L_1 \geq L_2$ in the ordering on levels, and
2. $S_2 \subseteq S_1$.

We usually write $(L_1, S_1) \geq (L_2, S_2)$.

Note that this is a *partial order*, not a total order. I.e., there are security labels A and B, such that neither $A \geq B$ nor $B \geq A$.

Dominates Example

In the following table, for which pairs does **Label 1** dominate **Label 2**?

Label 1	Label 2	Dominates?
(Secret: {Crypto})	**(Confidential: {Crypto})**	Yes
(Secret: {Crypto, Nuclear})	**(Top Secret: {Crypto})**	No
(Secret: {Nuclear})	**(Unclassified: {})**	Yes

Does this suggest how you might decide whether to allow a subject to read an object?

Simple Security Property

The following rule appears to capture our intuition about when a subject can read an object.

The Simple Security Property: Subject S with clearance (L_S, C_S) may be granted *read* access to object O with classification (L_O, C_O) only if $(L_S, C_S) \geq (L_O, C_O)$.

Can you guess why it's "only if" instead of "if and only if"?

Operationally, an individual asking to see a document must show that his clearance level *dominates* the sensitivity level of the document.

Lessons

- The dominates relation formalizes a relationship between any two labels.
- The Simple Security Property shows how to use dominates to decide whether a read access should be allowed.

Next lecture: MLS Example: Part IV