Foundations of Computer Security

Lecture 6: A Policy Example: MLS

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

Multi-Level Security

An early security problem was protection of *confidentiality* within a military setting.

> *Given information at various sensitivity levels and individuals having various degrees of trustworthiness, how do you control access to information within the system to protect confidentiality?*

This problem is called *multi-level security* (MLS) and predates computers.

MLS Thought Experiment

Setting: General Eisenhower's office in 1943 Europe. Assume an environment in which there are

- *information* at different "sensitivity" levels: the war plan, the defense budget, the base softball schedule, the cafeteria menu, etc.;
- *individuals* permitted access to selected pieces of information: Gen. Eisenhower, privates, colonels, secretaries, janitors, spies, etc.

The goal: Understand what "security" might mean in this context and define a policy (some rules) to implement it.

Risk Assessment

Question: What are we protecting? Against what threats?

Answer: The confidentiality of information—no person not authorized to view a piece of information may have access to it.

Very important proviso: For this thought experiment we are only concerned with *confidentiality*, not integrity or availability.

Confidentiality Questions

Recall the questions appropriate for considering a confidentiality policy:

- Is all of my data equally sensitive? If not, how do I group and categorize data?
- How do I characterize who is authorized to see what?
- How are the permissions administered and checked? According to what rules?
- Can authorizations change over time?

Categorizing Data

Back to Gen. Eisenhower's office. The relevant "space" of information contains lots of individual atoms or factoids:

1. The base softball team has a game tomorrow at 3pm.
2. The Normandy invasion is scheduled for June 6.
3. The cafeteria is serving chopped beef on toast today.
4. Col. Jones just got a raise.
5. Col. Smith didn't get a raise.
6. The British have broken the German Enigma codes.
7. and so on.

Not all information is equally sensitive. *How do we group and categorize information rationally?*

Object Sensitivity Labels

Information is parcelled out into separate containers (documents/folders/objects/files) *labeled* according to their sensitivity level.

One part of the label is taken from a linearly ordered set: **Unclassified**, **Confidential**, **Secret**, **Top Secret**.

There are also "need-to-know" *categories*, from an unordered set, expressing membership within some interest group, e.g., **Crypto**, **Nuclear**, **Janitorial**, **Personnel**, etc.

Sensitivity Labels

Ideally, the label on any folder reflects the sensitivity of the information contained within that folder. The label contains both a hierarchical component *and* a set of categories.

For example, two documents might have levels:

(Secret: {Nuclear, Crypto}),
(Top Secret: {Crypto}).

One can infer that the first contains somewhat sensitive information related to the categories Nuclear and Crypto. This second contains very sensitive information in category Crypto.

Some security officer makes these labeling decisions. How they are made is outside the scope of our concern.

Mixed Information

Question: How do you label a document that contains "mixed information"?

- Suppose the document contains both sensitive and non-sensitive information? *Use the highest appropriate level.*
- Suppose it contains information relating to both the Crypto and Nuclear domains? *Use both categories.*

Aside: Sometimes a decision is made that a document classification should be changed. This is called *downgrading* (or *upgrading*).

Lessons

- For our MLS example, we partition information into containers and provide labels that reflect the sensitivity of the information.
- The labels are structured, with a hierarchical component and a set of need-to-know categories.
- A folder with "mixed" information must be labeled to protect the information at the highest hierarchical level and protect all categories of information.

Next lecture: MLS Example: Part II