Setting: General Eisenhower’s office in 1943 Europe. Assume an environment in which we have:
- information at different “sensitivity” levels;
- individuals permitted access to selected pieces of information.

The goal: Understand what “security” (confidentiality) could mean in this context and define a policy (rules) to implement it.

Folder Sensitivity Labels

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

Examples:

- (Secret: \{Nuclear, Crypto\})
- (Top Secret: \{Crypto\})

Authorization Levels

Let’s assign individuals clearances or authorization levels, of the same form as document sensitivity levels.

That is, each individual has:
- a hierarchical security level indicating the degree of trustworthiness to which he or she has been vetted;
- a set of “need-to-know categories” indicating domains of interest in which he or she is authorized to operate.

Notice that labels on documents indicate the sensitivity of the contained information; “labels” on humans indicate classes of information that person is authorized to access.

A question we suggested for confidentiality policies is: How do I characterize who is authorized to see what?
Least Privilege: An Aside

The need-to-know categories are a reflection that even within a given security level (such as Top Secret) not everyone needs to know everything. This is an instance of:

**Principle of Least Privilege:** Any subject should have access to the *minimum* amount of information needed to do its job.

This is as close to an axiom as anything in security. *Why does it make sense?*

---

Now What?

**Question:** Given that we have labels for documents and clearances for individuals, how do we decide which humans are permitted access to which documents?

**Answer:** Surely it’s some relationship between the subject level and the object level. But what?

Should a human with the given clearance be able to read a document at the given sensitivity?

<table>
<thead>
<tr>
<th>Clearance</th>
<th>Sensitivity</th>
<th>Access?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Secret: {Crypto})</td>
<td>(Confidential: {Crypto})</td>
<td>Yes?</td>
</tr>
<tr>
<td>(Secret: {Crypto, Nuclear})</td>
<td>(Top Secret: {Crypto})</td>
<td>No?</td>
</tr>
<tr>
<td>(Secret: {Nuclear})</td>
<td>(Unclassified: {})</td>
<td>Yes?</td>
</tr>
</tbody>
</table>

---

Lessons

- To control access by individuals to documents/folders, we need “labels” for both.
- For documents the labels indicate the sensitivity of the information contained.
- For individuals, the labels indicate the authorization (clearance) to view certain classes of information.
- An individual should be given the minimal authorization to perform the job assigned. (Least Privilege)
- Whether an individual should be able to view a specific document depends on a relationship between the label of the document and the clearance of the individual.

**Next lecture:** MLS Example: Part III