8.3 Multilevel Security

In some environments data and documents may have critical value and their disclosure could bring serious problems. This pattern describes how to categorize sensitive information and prevent its disclosure. It discusses how to assign classifications (clearances) to users, and classifications (sensitivity levels) to data, and to separate different organizational units into categories. Access of users to data is based on policies, while changes to the classifications are performed by trusted processes that are allowed to violate the policies.

Example

The high command of an army has decided on a plan of attack in a war. It is extremely important that this information is not known outside a small group of people, or the attack may be a failure.

Context

In some environments data and documents may have critical value and their disclosure could bring serious problems.

Problem

How can you control access in an environment with sensitive documents so as to prevent leakage of information?

The solution to this problem must resolve the following forces:

- We need to protect the confidentiality and integrity of data based on its sensitivity.
- Users have to be allowed to read documents based on their rank or position in the organization.
- There should be a way to increase or decrease the ability of users to read documents and the sensitivity of the documents. Otherwise, people promoted to higher positions, for example, could not read sensitive documents, and we would end up with a proliferation of sensitive and obsolete documents.

Solution

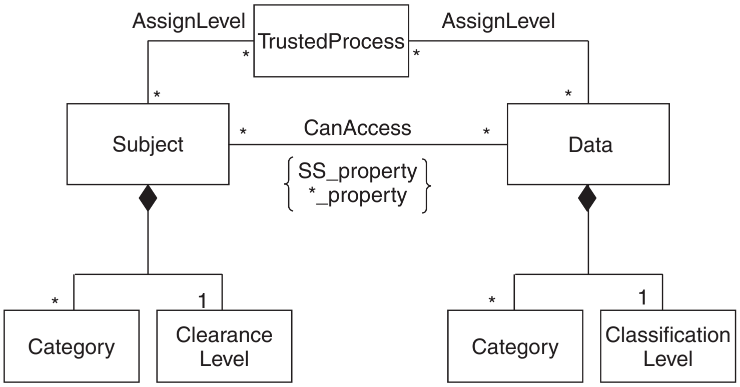
Assign classifications (as clearances) to users and classifications (as sensitivity levels) to data. Separate different organizational units into categories. For example, classifications may include levels such as top secret, secret, and so on, and compartments may include units such as engDept, marketingDept, and so on. For confidentiality purposes, access of users to data is based on policies defined by the Bell-LaPadula model [BL73], while for integrity the policies are defined by Biba's model [Sum97]. Changes to the classifications are performed by trusted processes that are allowed to violate the policies of these models.

Structure

The next figure shows the basic structure of this pattern. The `User Classification` and `Data Classification` classes define the active entities and the objects of access, respectively. Both classifications may include categories and levels. `Trusted Processes` are allowed to assign users and data to classifications, as defined by the `Assignment()` class.

Implementation

Data classification is a tedious task, because every piece of information or document must be examined and assigned a classification tag. New documents may get automatic tags based on their links to other documents. User classifications are based on their rank and unit of work and are only changed when they change jobs. It is hard to classify users in commercial environments in this way: for example, in a medical system it makes no sense to assign a doctor a higher classification than a patient, because a patient has the right to see their record.



Class model for MULTILEVEL SECURITY (253)

Example Resolved

The group involved in planning attacks, as well as all the related documents it produces, are given a classification of Top Secret. This will prevent leakage towards lower-level army staff.

Known Uses

The model has been used by several military-sponsored projects and in a few commercial products, including DBMSs (Informix, Oracle) and operating systems (Pitbull [Arg] and HP's Virtual Vault [HP]).

Consequences

The following benefits may be expected from applying this pattern:

- The classification of users and data is relatively simple and can follow organization policies.
- This model can be proved to be secure under certain assumptions [Sum97].
- The pattern is useful to isolate processes and execution domains.

The following potential liabilities may arise from applying this pattern:

- Implementations should use labels in data to indicate their classification. This assures security: if not done, the general degree of security is reduced.
- We need trusted programs to assign users and data to classifications.
- Data should be able to be structured into hierarchical sensitivity levels and users should be able to be structured into clearances. This is usually hard, or even impossible, in commercial environments.
- Covert channels may break the assumed security.

See Also

The concept of roles can also be applied here, role classifications replacing user classifications.