Thesis Journal
Week 1

Aytar Akdemir

September 5, 2021

1 Types of Access Control

First step is to determine the types of AC systems to be simulated. These could be merged, removed. Other AC systems might be added. In this section, a simple description of the AC systems are specified. The goal of this part is to determine which of the specified AC systems are suitable to model and simulate.

1.1 Mandatory Access Control

Subjects and objects have security attributes. When a subject tries to access an object, the operation is tested if it complies with the policy. Operationg system enforces the policy rules.

Security Policy Administrator controls the policies, users cannot change policy.

1.2 Discretionary Access Control

Access control is determined by the group which the subjects belong to.

Subjects can transfer permissions to other subjects.

1.3 Role-based Access Control

Roles are created for different job functions and assigned to users. Permissions come with the role and there is no need for the micromanagement of the permissions.

1.4 Identity-based Access Control

A user can only access to certain resources if their identity can be matched. A mechanism to authenticate the identity of the user is required. (e.g. Biometric readings)

1.5 Attribute-based Access Control

Uses policy that use attributes. Attributes may be:

- User attributes (Includes role)
- Resource attributes
- Object attributes
- Environment attributes

1.6 Organization-based Access Control

Focuses on Subject - action - object

- Roles: Subjects are abstracted into roles
- Activity: Actions are grouped to comply to the same rules
- View: Set of objects with the same security rule

Every security model is defined by an organization and is parametrized by it. The model includes permissions, obligations and prohibitions.

1.7 Lattice-based Access Control

A lattice is used to define the security levels of objects and clearance levels of the subjects. A subject can only access an object if the clearance level is higher than the security level of the object.

1.8 Graph-based Access Control

The access rights are granted to objects but also accounts. Difference from the role-based access control is GBAC uses a organizational query language for defining access rights while RBAC uses enumeration.

Two building blocks

- A semantic graph modeling an organization
- A query language

1.9 History-based Access Control

Run-time rights of a code is determined by examining the attributes of the code and the requests that were made by that code.

2 Modelling

After determining which ones will be used, all AC systems should be modelled using flowcharts. All flowcharts should be standardized for comparison. These flowcharts will be used as guides when programming the simulation.