Access Control: Basic Concepts

Prof.Dr. Ferucio Laurenţiu Ţiplea

Department of Computer Science
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania
E-mail: fltiplea@info.uaic.ro

Outline

1. Introduction
2. Users, Subjects, Objects, Operations, and Permissions
3. Policies, Models, and Mechanisms

Access Control: Who Can Do What

- Access control – guards, gates, locks
- Access control in computing – the way in which users can access resources in a computer system
- Access control – the most fundamental and most pervasive security mechanism in use today
- Access control shows up in virtually all systems, can take many form, and acts at different levels:
    - Hardware
    - Operating system
    - Middleware
    - Application
- Formal study of access control: early 1970s

Access Control: Who Can Do What

- Access control is critical to preserving the confidentiality and integrity of information
- Access control is also important to preserving availability
- Authorization and authentication are fundamental to access control:
  - authentication: process of determining who you are
  - authorization: process of determining what you are allowed to do

Users, Subjects, Objects, Operations, and Permissions

- User – people who interface with the computer system
- Subject – computer process acting on behalf of a user
- Object – resource accessible on a computer system
- Operation – active process invoked by a subject
- Permission (privilege, right) – authorization to perform some action on the system

Users, Subjects, Objects, Operations, and Permissions

Remark 1

- *Subjects/Objects/Operations/Permissions may be different in different systems or application contexts*
  - *in operating systems, objects are typically files, directories or programms*
  - *in database systems, objects can be relations, views etc.*
- *Traditionally, subjects are viewed as active entities (they request access to objects)*
- *Traditionally, objects are viewed as passive entities (they contain or receive information and should be protected of subjects)*
- *However, subjects may be themselves objects*

Principle of Least Privilege

Principle of least privilege: "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job"

> J. H. Saltzer. *Protection and the control of information sharing in multics*, Communications of the ACM, vol.17, no. 7, 1974, 388–402.

Benefits:

- Better stability
- Better security
- Easy of deployment

In practice, the principle is neither definable nor possible to enforce

Policies, Models, and Mechanisms

Development process of an Access Control System (ACS) based on:

- (Security) Policy – defines the high-level requirements that specify how access is managed and who, under what circumstances, may access what information
- (Security) Model – provides a formal representation of the access control policy and its working. A model allows proof of properties
- (Security) Mechanism – defines the low level (software and hardware) functions that implement a policy

Policies

Three main classes of security policies:

- Discretionary (DAC) – enforce access control on the basis of the identity of the requester and explicit access rules that establish who can or cannot execute which actions on which resources
- Mandatory (MAC) – enforce access control on the basis of regulations mandated by a central authority
- Role-based (RBAC)– enforce access control decisions on the functions a user is allowed to perform within an organization (the users cannot pass access permissions on to other users at their discretion)

Models

Security models based on:

- Matrices
- Graphs
- Partial orders
- Logics

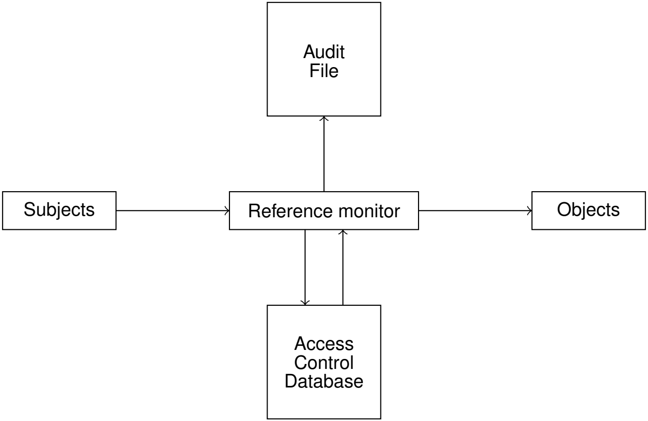
Mechanisms

Modern access control mechanisms are based on the reference monitor concept introduced in 1972 by Anderson:

> J. Anderson. *Computer Security Technology Planning Study*, ESD-TR-73-51, US Air Force Electronic Systems Division, Oct 1972, 142 pages.

Reference monitor: hardware and software portion of an operating system that is responsible for the enforcement of the security policy of the system

Reference Monitor



Reference Monitor

Fundamental implementation principles of a reference monitor:

- Completeness – it must be always invoked and impossible to bypass
- Isolation – it must be tamper-proof
- Verifiability – it must be shown to be properly implemented

Additional design principles of an access control system:

- Flexibility – the system should be able to enforce the access control policies of the host enterprise
- Manageability – the system should be intuitive and easy to manage
- Scalability – with respect to the number of users and resources

Reference Monitor

The reference monitor can be implemented using various topologies:

- System-wide enforcement of the reference monitor
- Enforcement of the reference monitor at the resource manager level
- Application-based reference monitor