isec

INFORMATION SECURITY

lectures by Ferucio Laurentiu Tiplea

Introduction to Access Control

Prof.dr. Ferucio Laurențiu Țiplea

Fall 2021

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Introduction

Preparing the scene

Policies, models, and mechanisms

Introduction

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 (please see Samarati and de Capitani di Vimercati (2001); Bishop (2005); Stallings (2020)).

Access control: who can do what

- Access control is critical to preserving:
  - confidentiality;
  - integrity;
  - availability;
- Two key ingredients necessary to access control:
  - authentication: process of determining who you are;
  - authorization: process of determining what you are allowed to do.

Preparing the scene

Users, subjects, objects, operations, 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, permissions

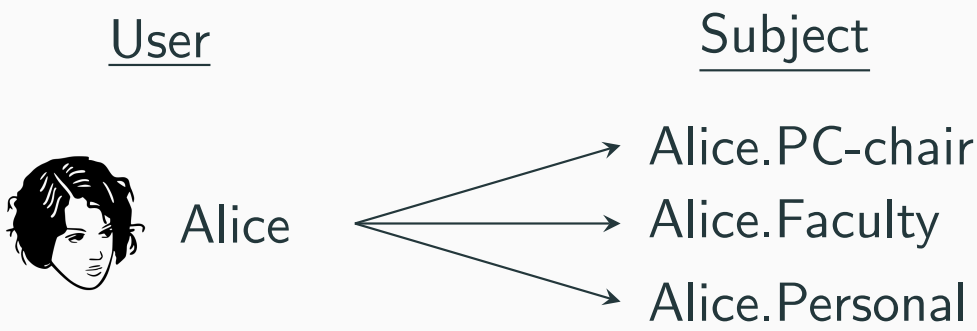
Remark 1

- *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, such as files or folders or memory segments, and should be protected of subjects);*
- *However, subjects may be themselves objects (with operations like kill, suspend, resume).*

User-subject distinction

Remark 2

- *A user can impersonate multiple users using different accounts, for example;*
- *A user may not be active at some time in the system, and when it is, there may be several subjects executing on its behalf;*
- *The user-subject distinction is vital if the subject's rights are different from the user's rights;*
- *In many systems, a subject that acts on behalf of a user has all the rights of the user.*



Principle of least privilege

Principle of least privilege (Saltzer (1974)): "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job".

Benefits:

- Better stability;
- Better security;
- Easy of deployment.

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

Policies, models, and mechanisms

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).

The fourth class of policies comes into force: attribute-based access control (ABAC).

Models

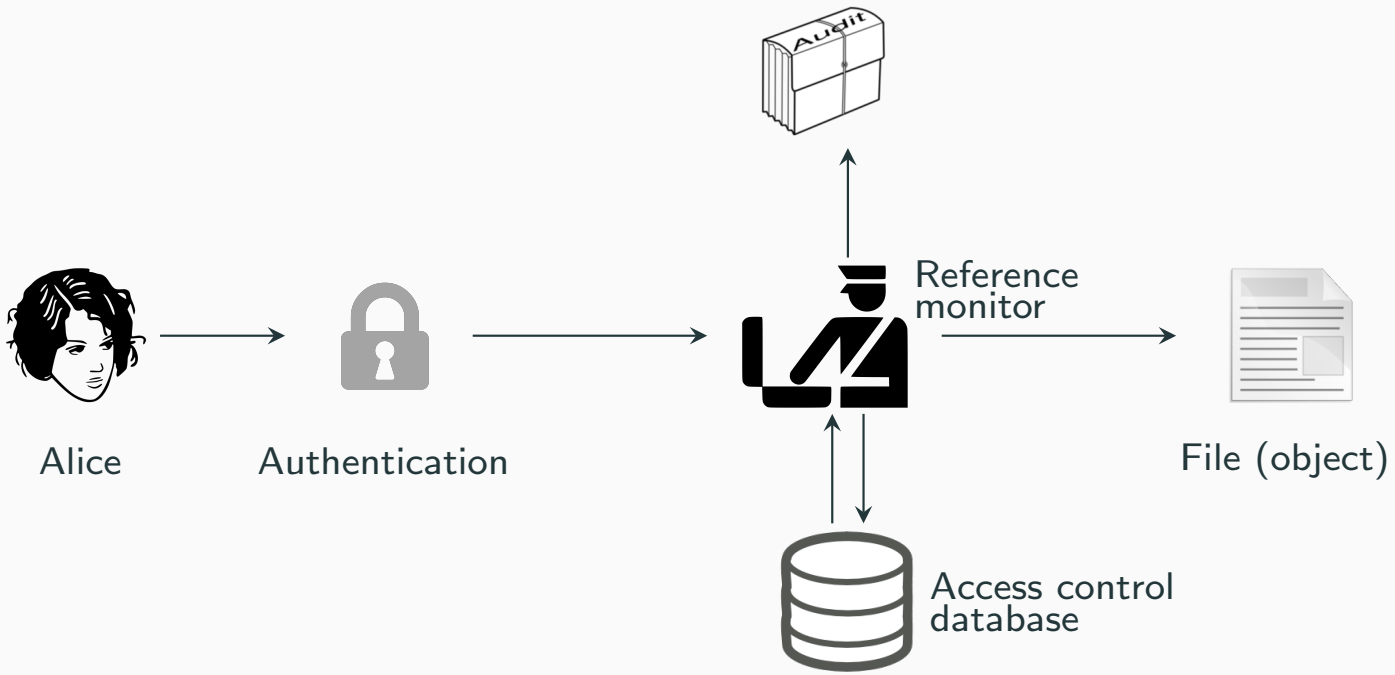
Security models based on:

- Matrices;
- Graphs;
- Partial orders;
- Logics.

Mechanisms

Modern access control mechanisms are based on the reference monitor concept introduced by Anderson (1972).

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

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.

Auditing

- System auditing is a method of obtaining information on the effectiveness of implementing specific policies or procedures for the operation or security of the system;
- Auditing can help correct operating errors, security breaches, or improper granting of access rights to system resources;
- For example, many events can be audited in the Windows operating system (Microsoft (2021)), such as account logon events, account management, directory service access, object access, privilege use, etc.

References

Anderson, J. P. (1972). Computer Security Technology Planning Study. Technical Report ESD-TR-73-51, U.S. Air Force Electronic Systems Division.

Bishop, M. A. (2005). *Introduction to Computer Security*. Addison-Wesley.

Microsoft (2021). Windows security. Technical report, Microsoft.

Saltzer, J. H. (1974). Protection and the control of information sharing in multics. *Commun. ACM*, 17(7):388–402.

Samarati, P. and de Capitani di Vimercati, S. (2001). Access control: Policies, models, and mechanisms. In Focardi, R. and Gorrieri, R., editors, *Foundations of Security Analysis and Design*, pages 137–196, Berlin, Heidelberg. Springer Berlin Heidelberg.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson, 8th edition.