Access control

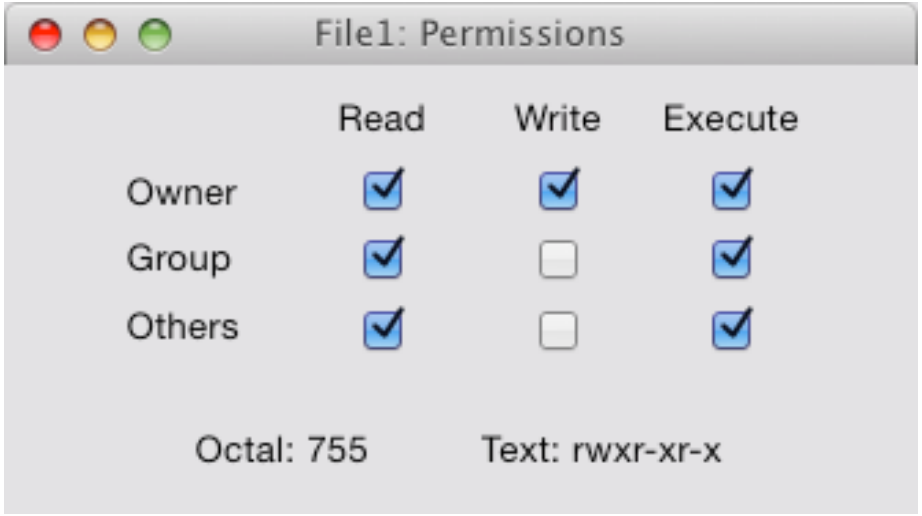
Mariano Ceccato

mariano.ceccato@univr.it

What is Access Control?

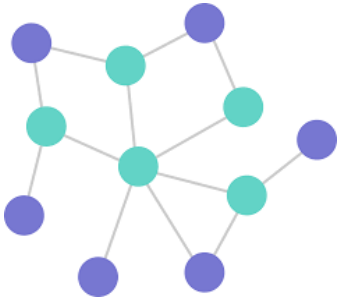
- Central element of cyber security
- Objective: prevention of access/use of a resource by unauthorized users, or by authorized users but in unauthorized manner
  - Involves users and groups
  - Authenticate to system
  - Assigned access rights to certain resources on system

Access Control in Use

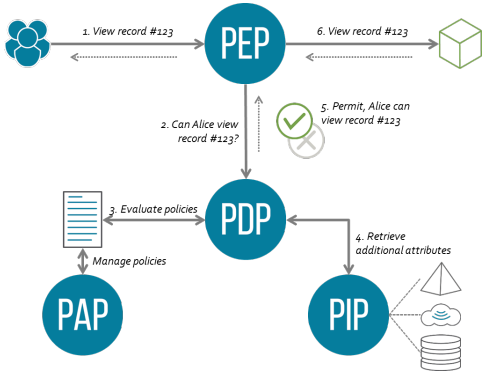


Access Control System

Access Control Policies



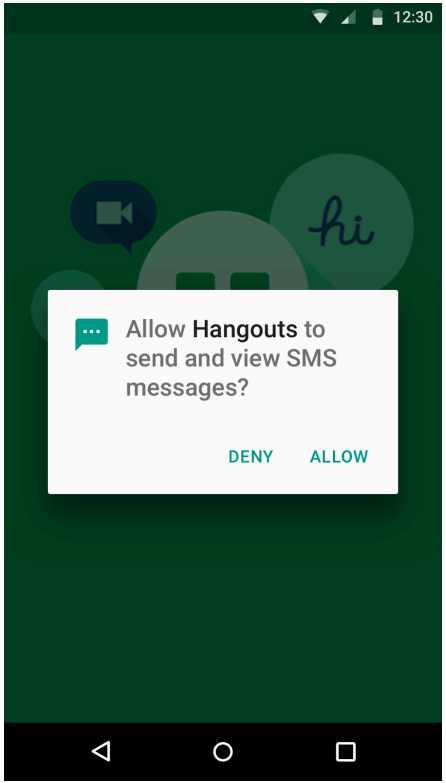
Access Control Model



Access Control Mechanism

Access Control Policy Elements

- **Subject** - entity that can access objects
  - a process representing user/application
- **Object** - access controlled resource
  - e.g. files, directories, records, programs etc
- **Access right** (or permission) - way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search



Types of Access Control Models

- **Discretionary Access Control (DAC)**
  - Access based on the identity of the subjects
- **Mandatory Access Control (MAC)**
  - Access based on objects security labels and subjects security clearances
- **Role based Access Control (RBAC)**
  - Access based on the role played by a subject
- **Attribute-based Access Control (ABAC)**
  - Access is based on attributes of the subject, the object, and the context

Discretionary Access Control (DAC)

- Access to data objects (files, directories, etc.) is permitted based on the identity of users.
- Explicit access rules that establish who can, or cannot, execute which actions on which resources.
- Often provided using an access matrix

- Discretionary: users can be given the ability of passing on their privileges to other users, where granting and revocation of privileges is regulated by an administrative policy

Access Control Matrix

objects

subjects	news.doc	photo.png	fun.com
alice	read	view edit	view
bob	read write	view edit	view modify
charlie			
dave		view	

Access Control List

news.doc

bob	read write
alice	read

photo.png

alice	view, edit
bob dave	view, edit
	view

fun.com

alice	view
bob	view modify

Capability List

Alice's capability

news.doc	photo.png	fun.com
read	view, edit	view

Bob's capability

news.doc	photo.png	fun.com
read write	view, edit	view edit

Charlie's capability

Dave's capability

photo.png
`view`

DAC Limitations

- Managing a policy is a complex task in a large system
  - Set of subjects or objects is large
  - Set of subjects or objects change frequently
- Capability Lists
  - Difficult to get an overview of permissions granted on a given object
- Access Control Lists
  - Difficult to get an overview of permissions granted to a given user

Role-based Access Control (RBAC)

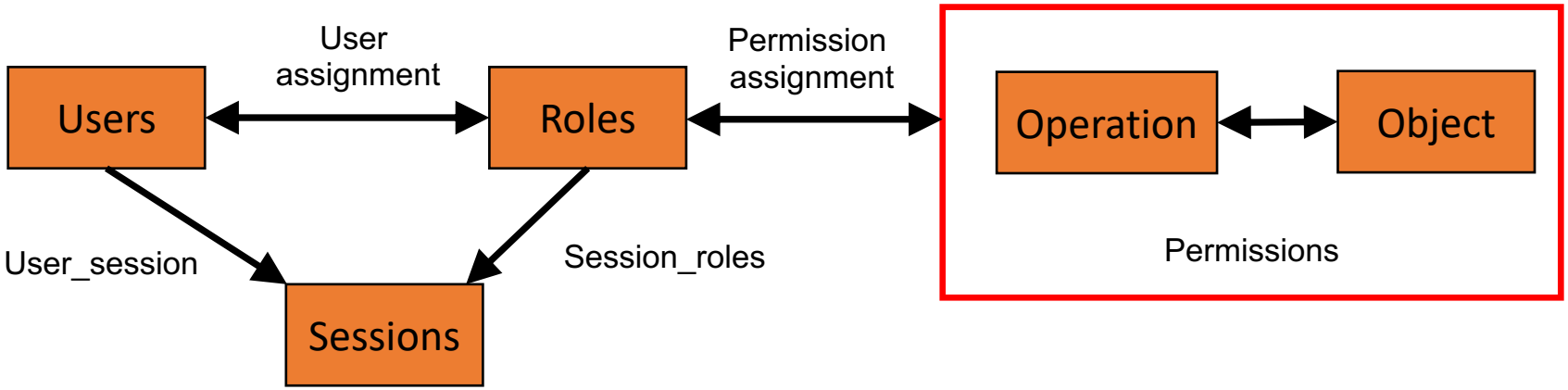
- Widely adopted access control model
- Based on the role played by a user within an organization
- Roles are assigned access rights to resources
- Users are assigned to roles
  - Inherit access rights of the role they play

RBAC Family

- Defined by Ravi Sandhu in 1996
- ANSI standard since 2004

- **RBAC0**
  - Core model: users, roles, permissions, sessions
- **RBAC1**
  - RBAC0 + Role Hierarchies
- **RBAC2**
  - RBAC1 + Constraints

RBAC-0: Core


User
assignment
Permission
assignment
Users
Roles
Operation
Object
User_session
Session_roles
Permissions
Sessions

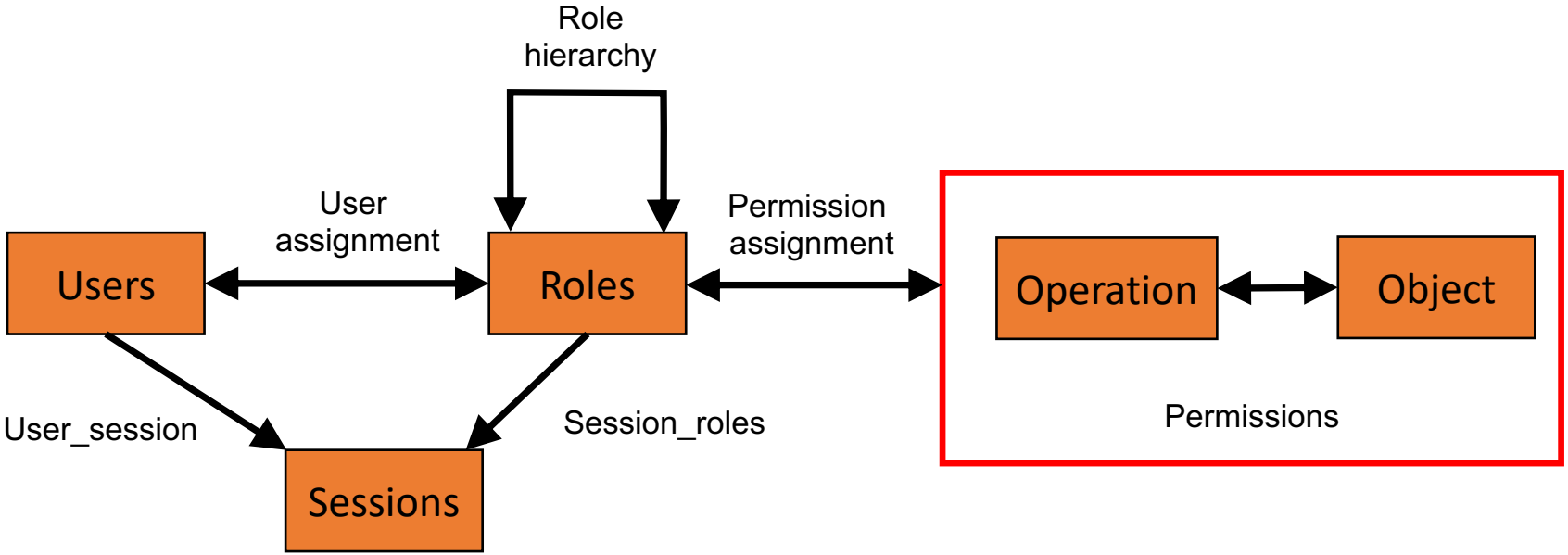
Example: Roles

- Roles
  - Lecturer
  - PhD Student
  - Associate Professor
  - Full Professor
  - Head of Department
- Objects
  - Exam-assignment
  - Lab-assignment

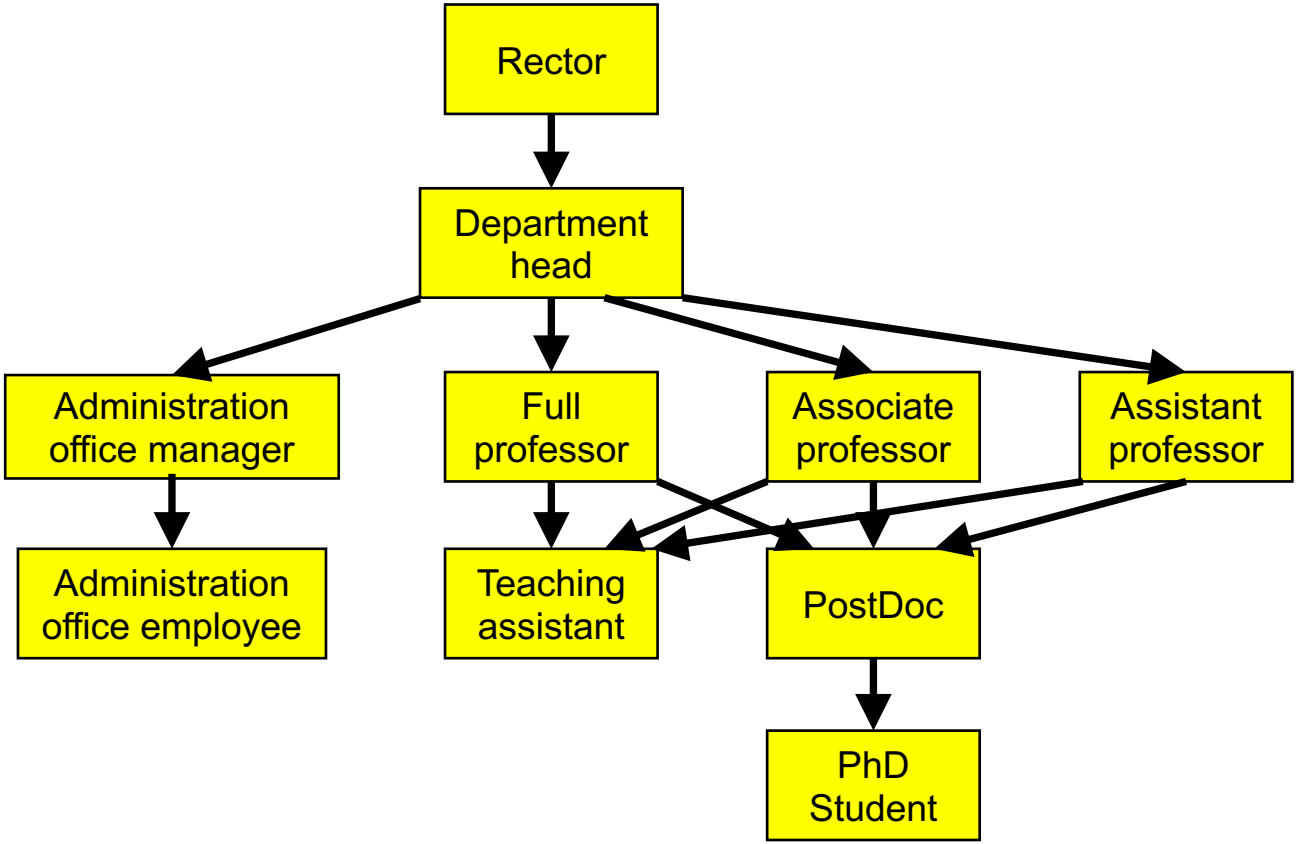
Permissions to Roles

- Lecturer:
  - create exam-assignment, mark exam-assignment
  - create lab-assignment, mark lab-assignment,
- PhD student:
  - view lab-assignment, mark lab-assignment
- Associate Professor
- Full Professor
- Head of Department

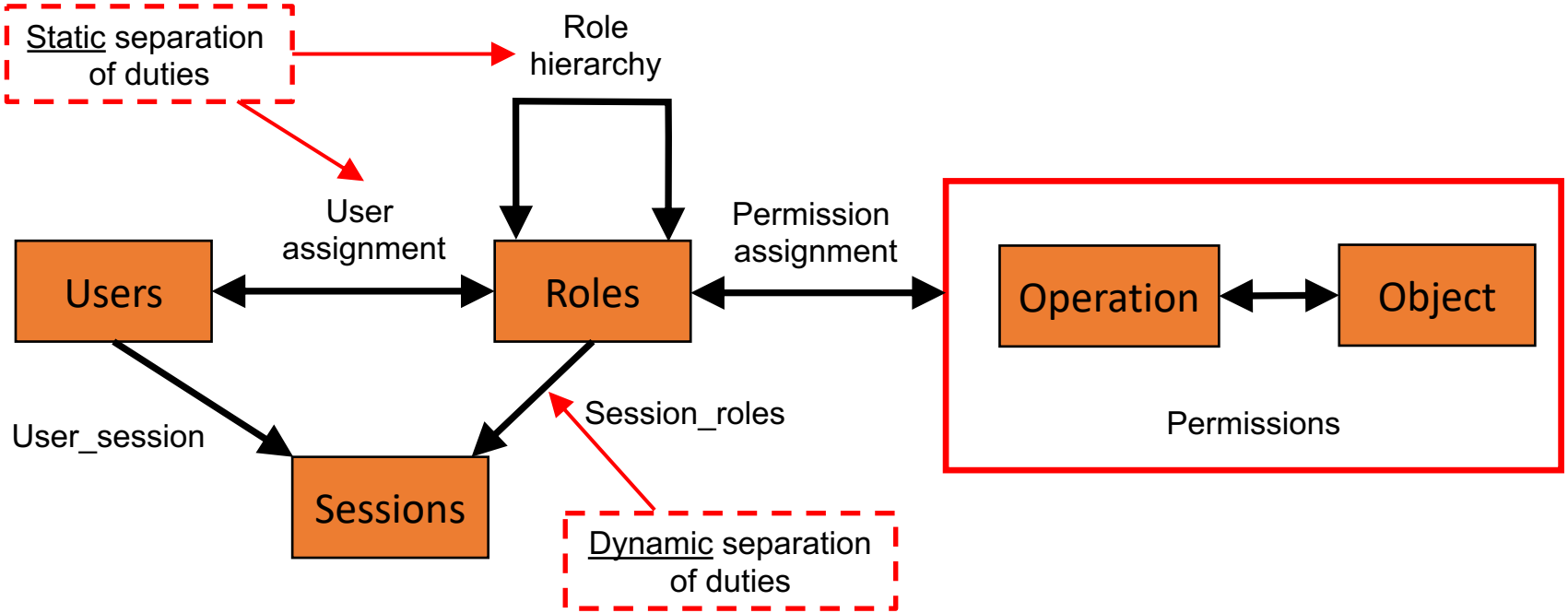
RBAC-1: Core + Hierarchy



Role hierarchy



RBAC-2:
RBAC-1 + separation of duty constraints



Separation of duty constraints

- Static Separation of Duty
  - pair (role set, n)
  - a user cannot be assigned to more than n roles in the role set

A user cannot be assigned to both the role of `student` and `lecturer`

- Dynamic Separation of Duty
  - pair (role set, n)
  - a user cannot activate more than n roles in the role set within the same session

The user `Mariano` cannot activate at the same time the role of `lecturer` and `student` for the course `Cyber Security of IoT`

RBAC Advantages

- Efficient administering and monitoring of permissions
  - No need to manually assign users to permissions
  - Automatically done by assigning users to roles
- Reduce Employee Downtime
- Enhanced System Security and Integrity

RBAC in Use

- Healthcare
  - National healthcare system
- Banking and Finance
  - Banks, Insurance companies
- Commercial products
  - DBMS
- Cloud platforms
  - Microsoft Azure

Threats in RBAC

- Access control is very hard to implement correctly
  - A European bank with over 50,000 employees, 1400 branches and more than 6 million customers
    - 1300 roles
    - 1000 role changes in 3 months
- Organizations over-entitled employees
  - 50% to 90% of employees are over-entitled in large organizations

Summary

- Access control specifies who or what may have access to a system resource and the type of access that is permitted
- Three types of access control policies
  - Discretionary
  - Mandatory
  - Role-based
- Access control is very hard to implement correctly
  - Employees are often over-entitled