

System Security

Access Control Fundamentals

Giovanni Russello

`g.russello@auckland.ac.nz`

`http://www.cs.auckland.ac.nz/compsci725s2c/`

Access Control

- ◆ “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner“
- ◆ central element of computer security
- ◆ assume have users
 - authenticate to system
 - assigned access rights to certain resources on system

Access Control Requirements

- ◆ reliable input
- ◆ least privilege
- ◆ separation of duty
- ◆ fine and coarse specifications
- ◆ open and closed policies
- ◆ policy combinations, conflict resolution
- ◆ administrative policies

Access Control 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 - way in which subject accesses an object
 - e.g. read, write, execute, delete, create, search

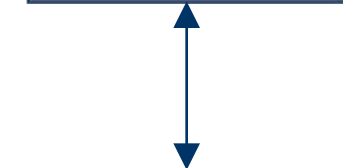
Access Control Features



Auditor



User



Security Administrator

Access Control Models

- ◆ Discretionary AC (DAC)
- ◆ Mandatory AC (MAC)
- ◆ Role-based AC (RBAC)
- ◆ Usage Control (UCON)
- ◆ Policy-based Access Control

Discretionary Access Control

- ◆ Subjects are able to assign on the objects they control access rights to other subjects
- ◆ Model used in operating systems and DB management systems
- ◆ often provided using an access matrix

Access Control Matrix

	File1	File2	File3	File4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

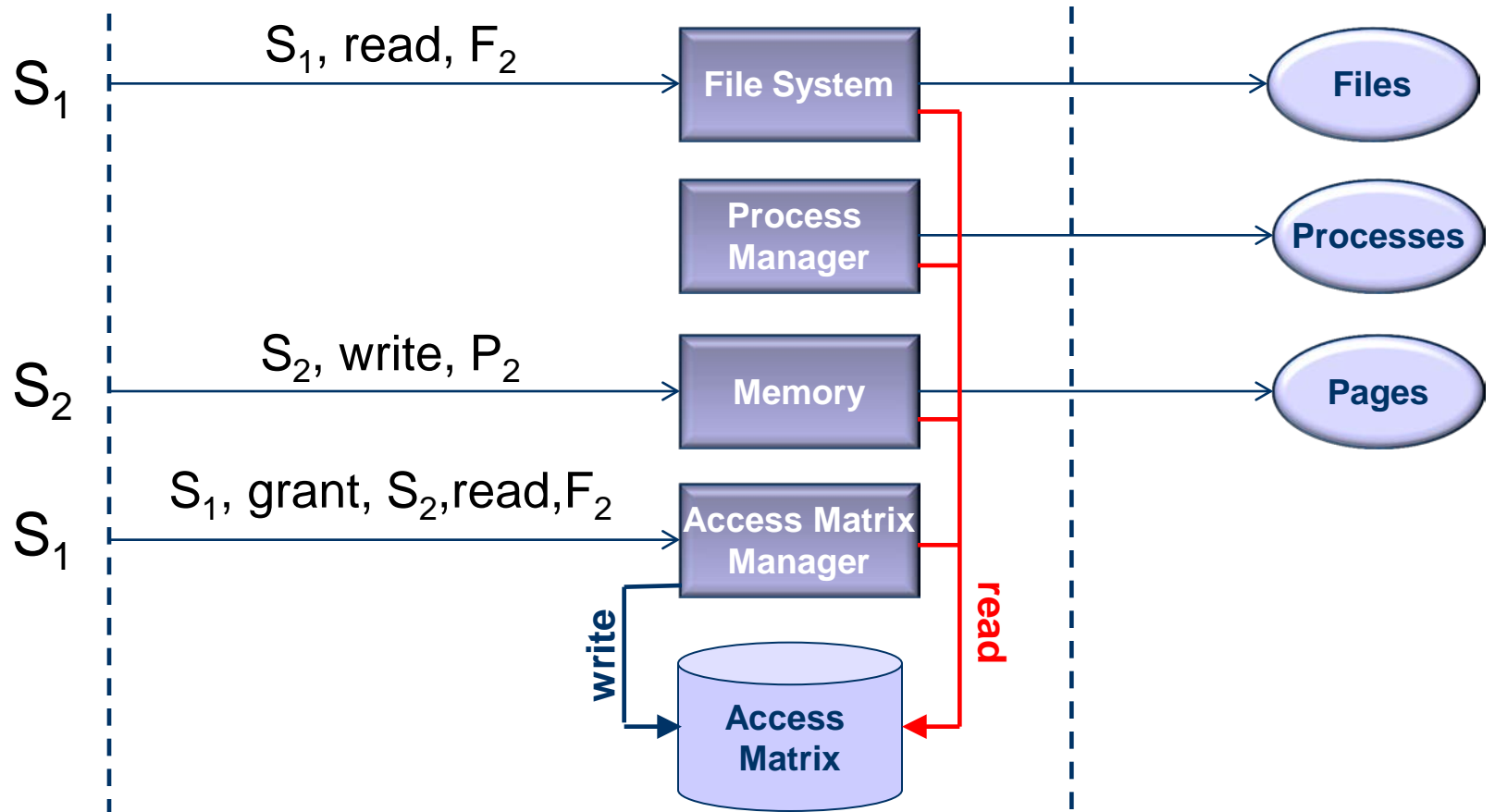
Access Control List

	File1	File2	File3	File4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

Capability List

	File1	File2	File3	File4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

Access Matrix Details



Mandatory AC

Entities cannot enable other entities to access their resources

It enforces a lattice between labels assigned to subjects and object

- ◆ security labels: how sensitive or critical a system resource is
- ◆ security clearances: which entities are eligible to access certain resources

MAC: The Bell-LaPadula Model ('76)

The main goal is to control the **confidentiality of information**

User Labels

Colonel

Major

Sergeant

Private

Data Labels

Top Secret

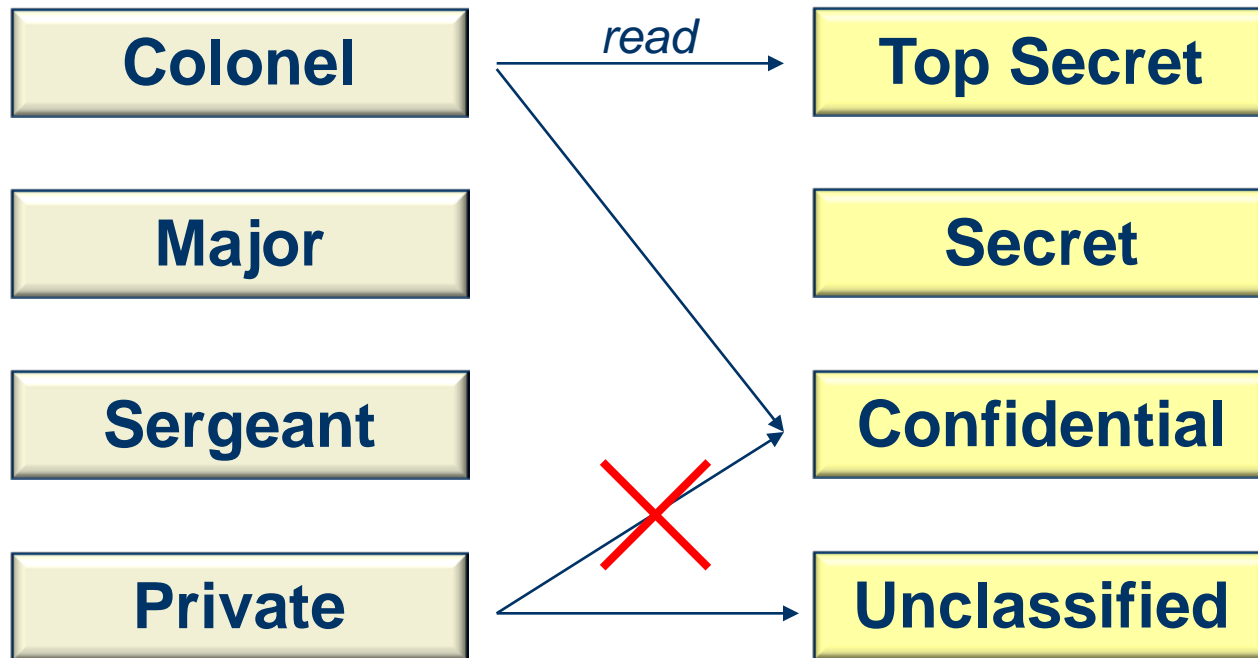
Secret

Confidential

Unclassified

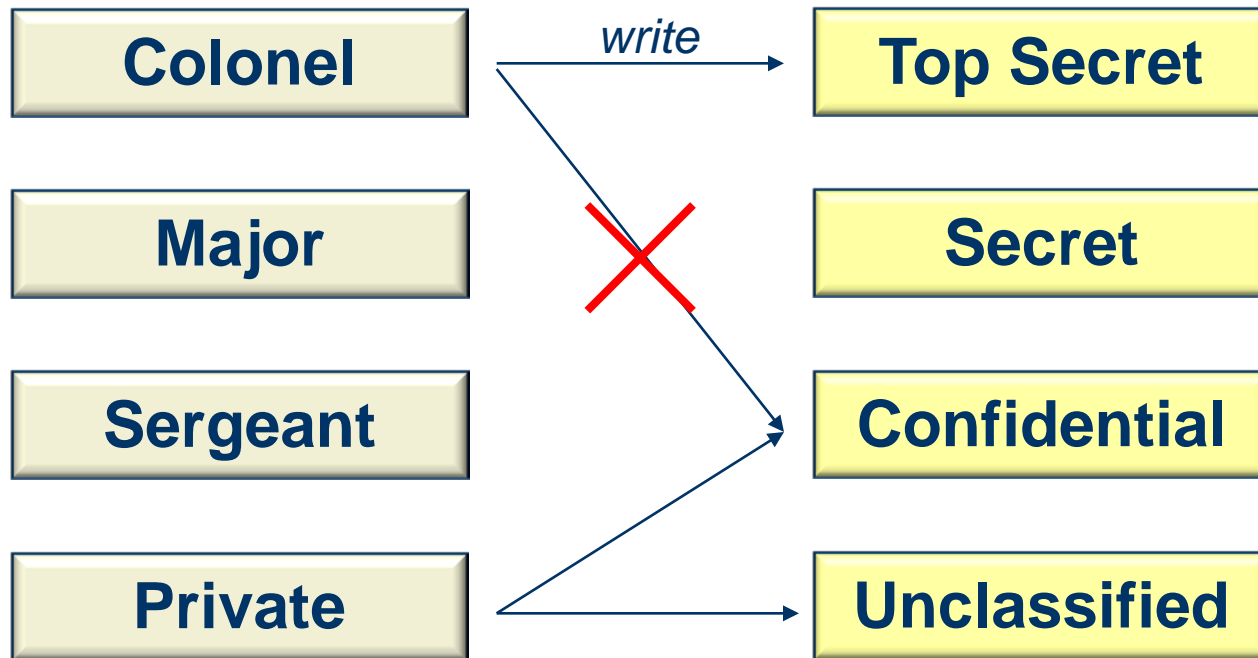
MAC Confidentiality Rules

Simple Security Property: No Read-Up



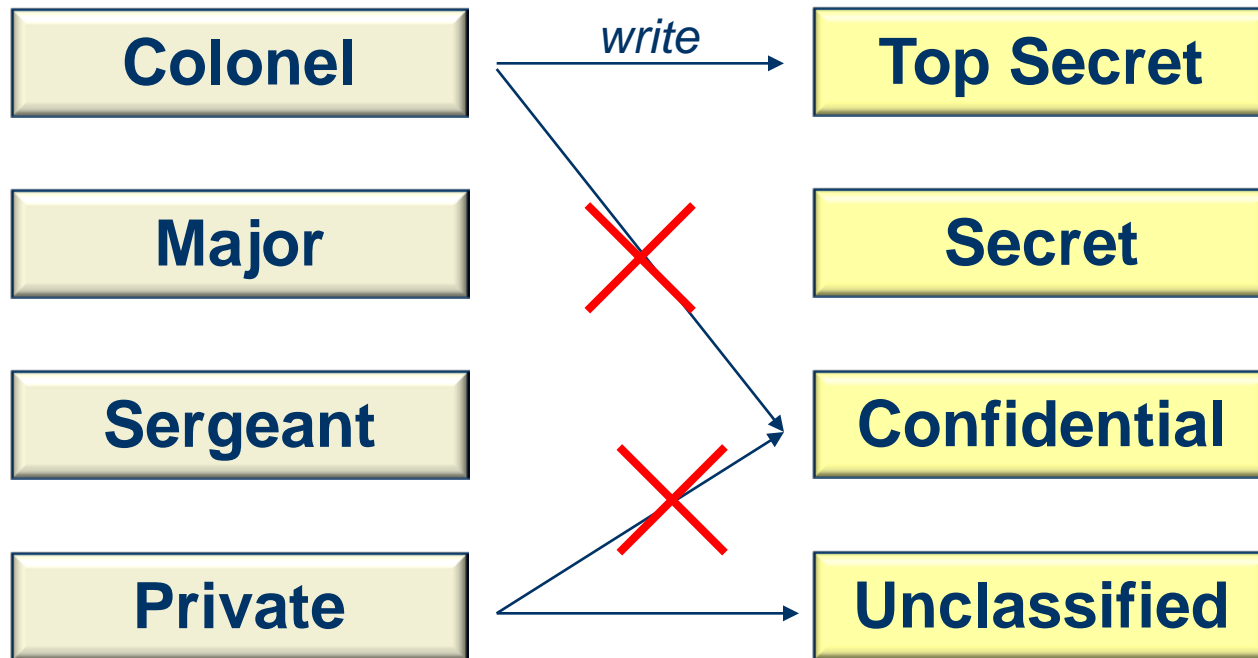
MAC Confidentiality Rules

**(Star)property: No Write-Down*



MAC Confidentiality Rules

*Strong *(Star)-property: No Write-Down & No Write-up*



MAC: Biba Integrity Model ('77)

The main goal is to control the **integrity of information**

User Labels

Manager

Project Leader

Engineer

Jr. Engineer

Data Labels

Strategic

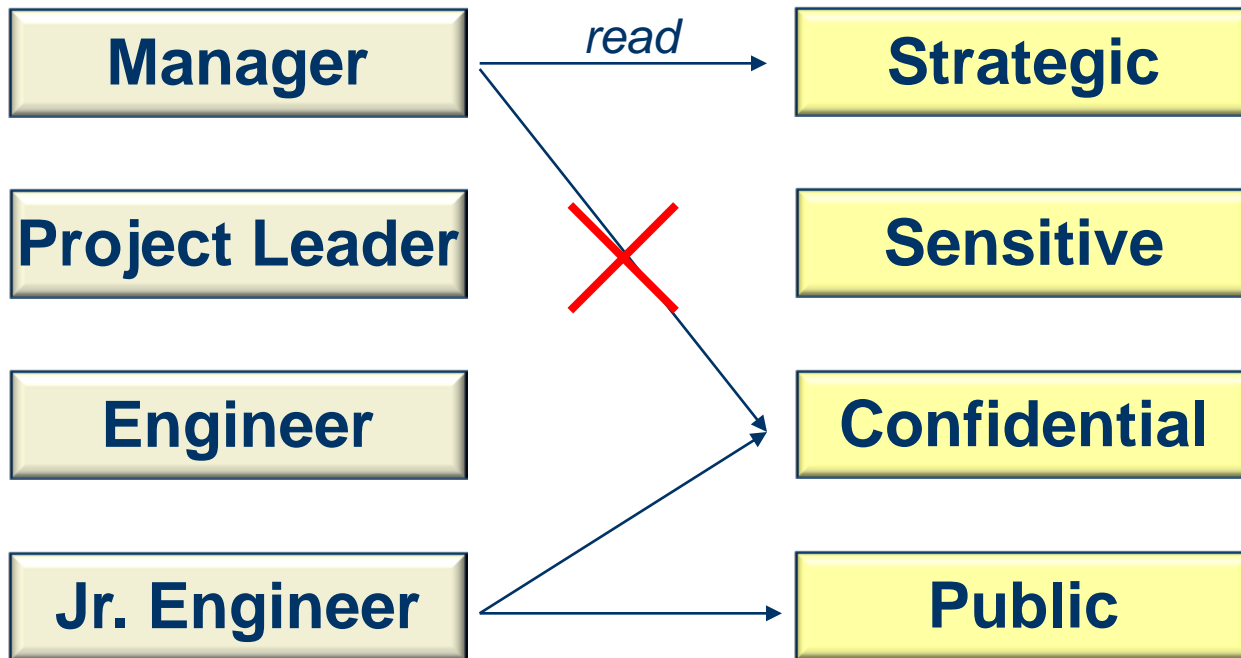
Sensitive

Confidential

Public

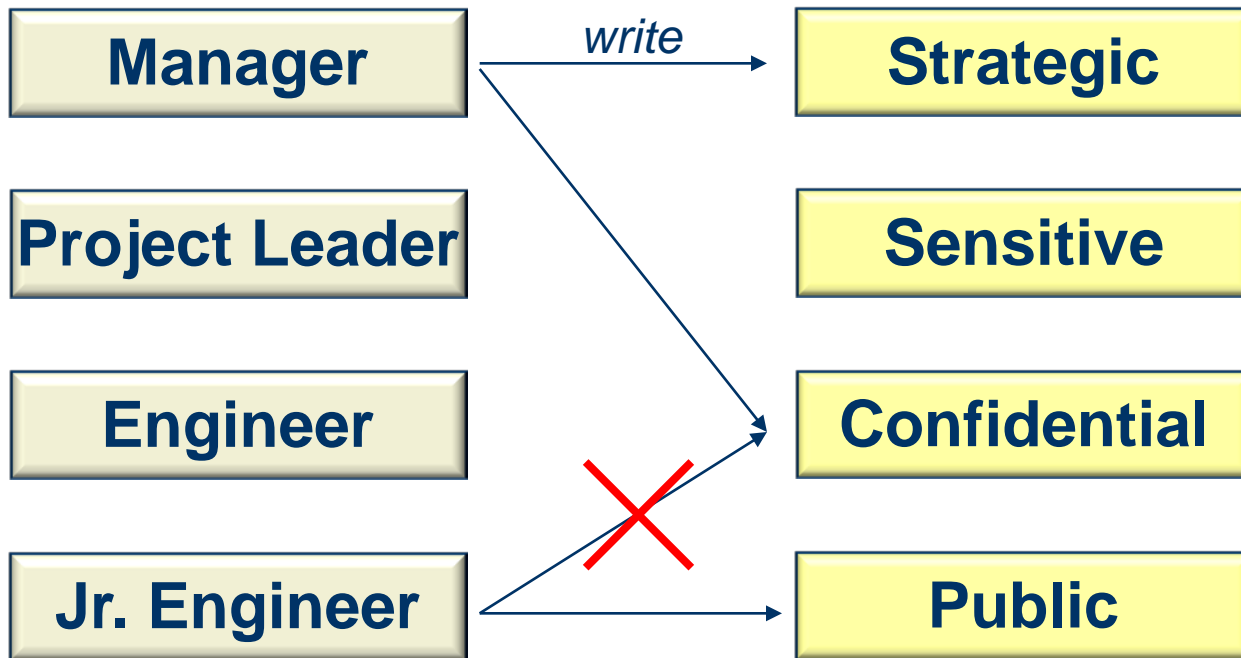
MAC Integrity Rules

Simple Integrity Axiom: No Read Down



MAC Integrity Rules

**(Star)-Integrity Axiom: No Write Up*



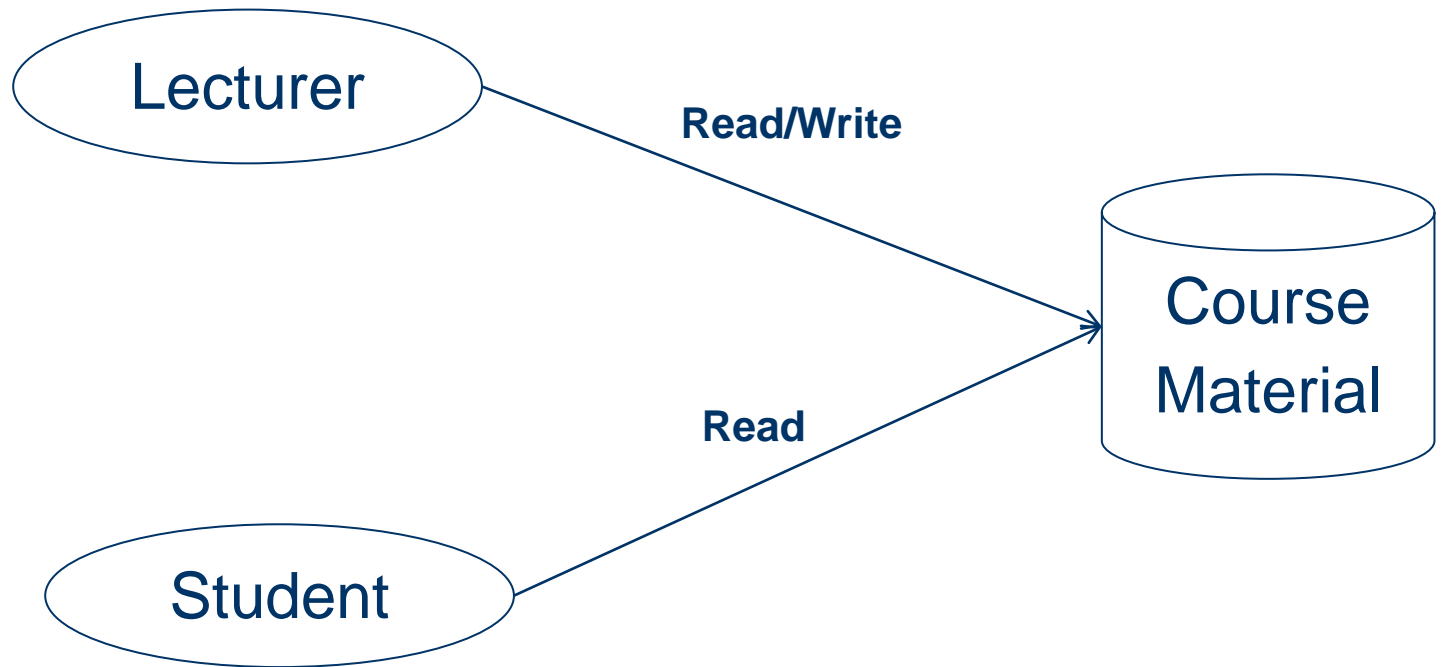
Where is MAC used

- ◆ BLP: Implemented the multi-level security policy for US Department of Defense
- ◆ BIBA: Implemented in the FreeBSD MAC policy
- ◆ A combined versions of BLP and BIBA is used in Android!

Role Based Access Control

- ◆ Enterprises organise employees in different roles
- ◆ RBAC maps roles to access rights
- ◆ Access rights are assigned to roles
- ◆ After Subjects are authenticated they are assigned to roles

A simple example



User to Role

	Lecturer	S Lecturer	Ass Prof	Prof
Giovanni	X			
Ulrich		X		
Clark				X

Role to Access Rights

	File1	File2	File3	File4
Lecturer	Own Read Write		Own Read Write	
S Lectuer	Read	Own Read Write	Write	Read
Professor	Read Write	Read		Own Read Write

Extensions to the Model

- ◆ A user can be in more than one role
 - Gill Dobbie is both Prof. and HoD
- ◆ Roles can be organised in Hierarchies
 - Prof>Ass Prof>Sen Lect>Lect
 - Top Roles inherited access rights of Lower Roles
- ◆ Constraints to enforce enterprise-specific requirements



RBAC Constraints

- ◆ Separation of Duties (SoD)
 - Protecting the organisation from frauds
- ◆ Chinese Wall (CW)
 - Conflict of interests between different domains



SoD Details

SoD are used when an activity involves more than one roles:

Purchase order needs to be **prepared** by a **clerk** and then **authorised** by a **manager**

To avoid a fraud, the user that prepares the order should not be the same that authorises it



Static SoD

- ◆ In Static SoD, the same subject cannot be member of two mutually exclusive roles
 - **clerk** and **manager** are mutually exclusive
- ◆ Too restrictive: the user might get assigned to both roles as long as she is not working on the same order!



Dynamic SoD

- ◆ In Dynamic SoD, the same subject can be member of two mutually exclusive roles
- ◆ **However**, it requires extra checks that need to be done at runtime to avoid undesired behaviour
- ◆ Simple DSoD, Object DSoD, Operational DSoD, History DSoD



Simple DSoD

- ◆ Users cannot be active in mutually exclusive roles at the same time
- ◆ For instance, a user can be assigned to both clerk and manager roles as long as she is not active on both at the same time

Object DSoD

- ◆ Users can be active in mutually exclusive roles at the same time as long as she is not operating on the same object instance for the entire business process
- ◆ For instance, a user can act in either clerk or manager role for a purchase order
- ◆ Let say that there is another operation: sending the order to depot. The user cannot execute this action even if it is not in conflict

Operational DSoD

- ◆ Users can be active in mutually exclusive roles at the same time but cannot perform all the operations of business process
- ◆ For instance, a user can activate both clerk and manager roles but cannot execute both the prepare and authorise operations (even for different objects!!)

History DSoD

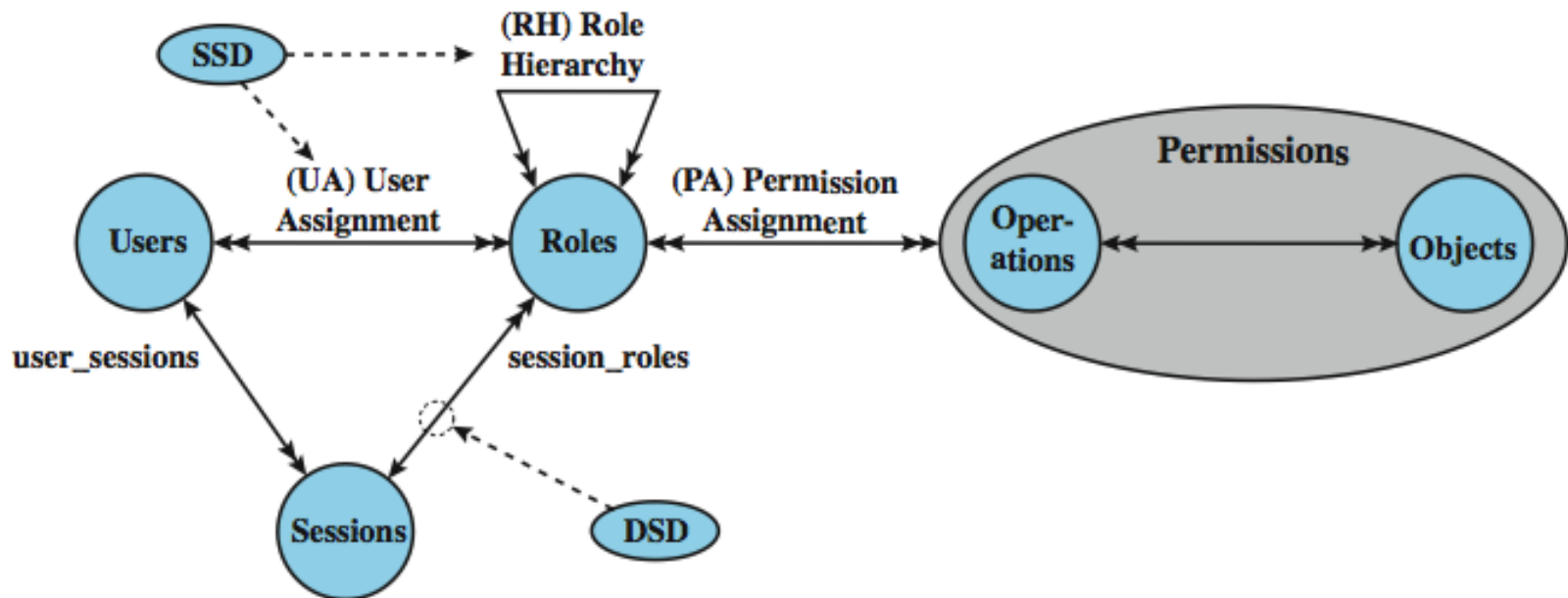
- ◆ Users can be active in mutually exclusive roles at the same time as long as she is not authorised to execute all the operation for the same object instance
- ◆ For instance, a user can be activate in both clerk role for a purchase order and manager role for another order



Chinese Wall

- ◆ It applies to accesses in multiple domains with conflict of interest
- ◆ For instance, a consultant company offering services to both Microsoft and Apple. CW makes sure that an employee of the company will not get access to documents of both companies

NIST RBAC Model



SSD = static separation of duty
DSD = dynamic separation of duty



Resources

- ◆ Chapter 8 in Mark Stamp, *Information Security: Principles and Practice*, Wiley 2011.
- ◆ Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley 2003.