

# Access Control

## ITS335: IT Security

Sirindhorn International Institute of Technology  
Thammasat University

Prepared by Steven Gordon on 20 December 2015  
its335y15s2l04, Steve/Courses/2015/s2/its335/lectures/access.tex, r4287

## Contents

### **Access Control Concepts**

### Discretionary Access Control

### Role-Based Access Control

### Mandatory Access Control

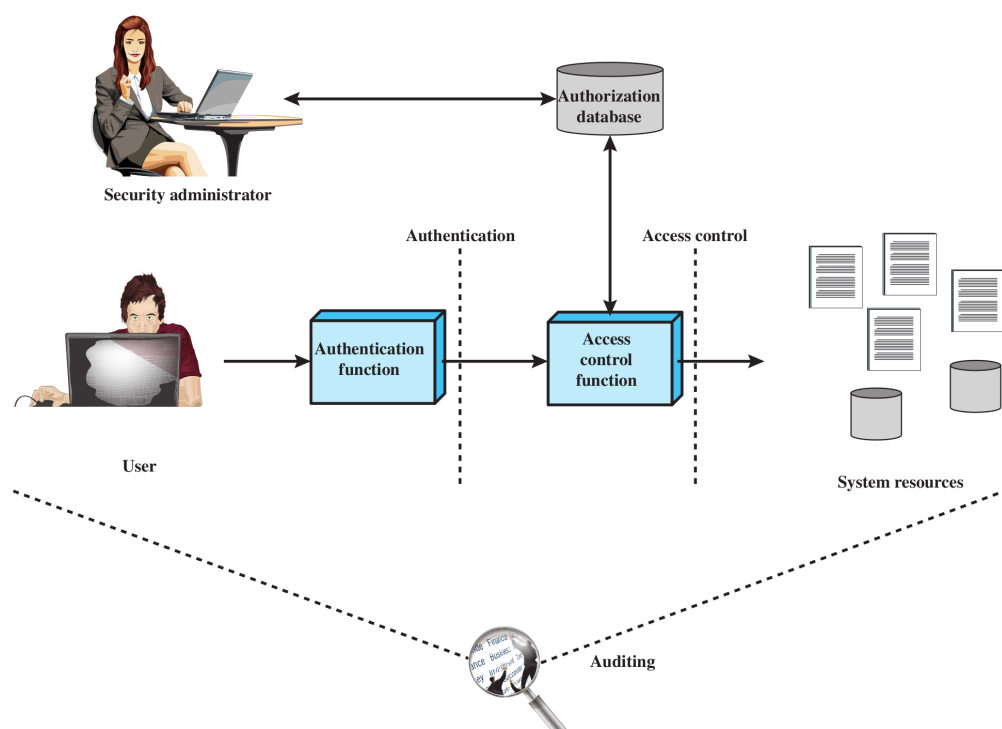
### Summary

*The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.*

— ITU-T Recommendation X.800 “Security architecture for Open Systems Interconnection”

3

## Relationship Among Access Control and Other Security Functions



# Access Control and Other Security Functions

**Authentication** verification that the credentials of a user or other entity are valid

**Authorization** granting of a right or permission to a system entity to access a resource

**Audit** independent review of system records and activities in order to test for adequacy of system control, ensure compliance to policy, detect breaches and recommend changes

5

## Access Control Policies

**Discretionary Access Control** use identity of requestor and access rules (that determine what requestor is allowed to do) to control access; entities may allow other entities to access resources

**Mandatory Access Control** compare security labels with security clearances to determine access; entities cannot grant access to resources to other entities

**Role-based Access Control** roles of users in system and rules for roles are used to control access

DAC, MAC and RBAC are not mutually exclusive

6

# General Requirements of Access Control

- ▶ Reliable input
- ▶ Fine and coarse specifications
- ▶ Least privilege
- ▶ Separation of duty
- ▶ Open and closed policies
- ▶ Policy combinations and conflict resolution
- ▶ Administrative policies
- ▶ Dual control

7

# Basic Elements of Access Control System

**Subject** entity capable of access resources

- ▶ Often subject is a software process
- ▶ Classes of subject, e.g. Owner, Group, World

**Object** resource to which access is controlled

- ▶ E.g. records, blocks, pages, files, portions of files, directories, email boxes, programs, communication ports

**Access right** describes way in which a subject may access an object

- ▶ E.g. read, write, execute, delete, create, search

8

# Contents

## Access Control Concepts

### Discretionary Access Control

### Role-Based Access Control

### Mandatory Access Control

### Summary

9

## Discretionary Access Control

- ▶ DAC: an entity may be granted access rights that permit the entity, if they choose so, to enable another entity to access a resource
- ▶ Common access control scheme in operating systems and database management systems
- ▶ Access Matrix specifies access rights of subjects on objects
- ▶ In practice, access matrix is sparse, so implement as either:
  - ▶ **Access Control Lists (ACL)** For each object, list subjects and their access rights
  - ▶ **Capability Lists** For each subject, list objects and the rights the subject have on that object
- ▶ Alternative implementation: authorization table listing subject, access mode and object; easily implemented in database

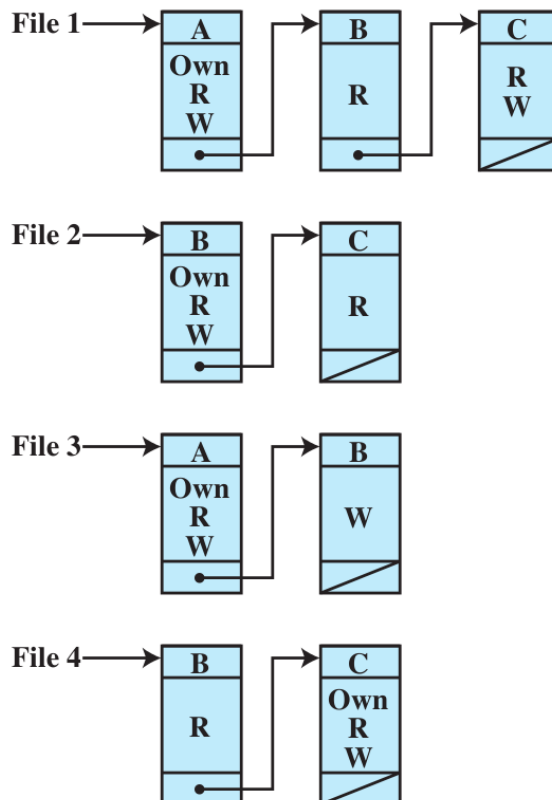
10

# Example of DAC Access Matrix

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

Credit: Figure 4.3(a) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

# Example of Access Control Lists



Credit: Figure 4.3(b) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

# Example of Capability Lists

Access Control

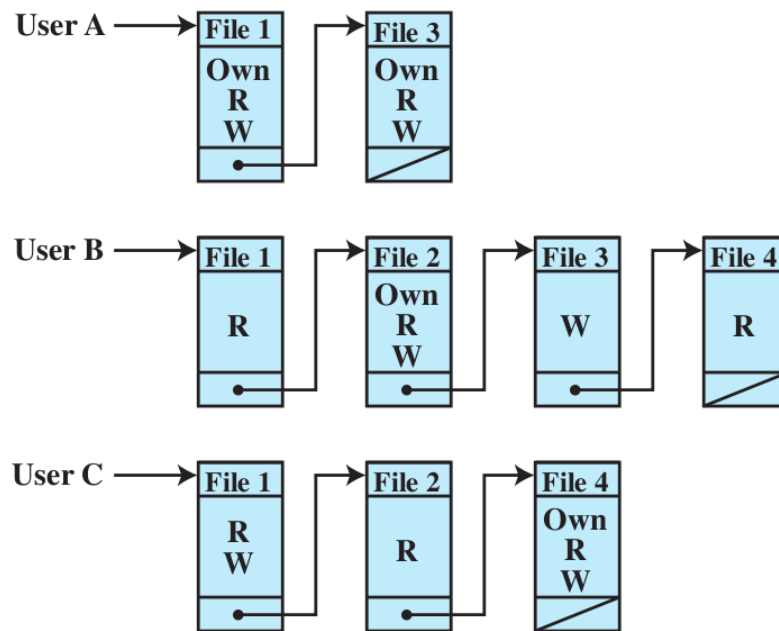
Concepts

DAC

RBAC

MAC

Summary



Credit: Figure 4.3(c) in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

13

# Example of Authorization Table

Access Control

Concepts

DAC

RBAC

MAC

Summary

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Credit: Table 4.1 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

14

# Contents

## Access Control Concepts

## Discretionary Access Control

## Role-Based Access Control

## Mandatory Access Control

## Summary

15

# Role-Based Access Control

- ▶ RBAC: users are assigned to roles; access rights are assigned to roles
- ▶ Roles typically job functions and positions within organisation, e.g. senior financial analyst in a bank, doctor in a hospital
- ▶ Users may be assigned multiple roles; static or dynamic
- ▶ Sessions are temporary assignments of user to role(s)
- ▶ Access control matrix can map users to roles and roles to objects

16



# Example of RBAC Access Control Matrix

Access Control

Concepts

DAC

RBAC

MAC

Summary

	R <sub>1</sub>	R <sub>2</sub>	...	R <sub>n</sub>
U <sub>1</sub>	✗			
U <sub>2</sub>	✗			
U <sub>3</sub>		✗		✗
U <sub>4</sub>				✗
U <sub>5</sub>				✗
U <sub>6</sub>				✗
⋮				
⋮				
U <sub>m</sub>	✗			

	OBJECTS								
	R <sub>1</sub>	R <sub>2</sub>	R <sub>n</sub>	F <sub>1</sub>	F <sub>1</sub>	P <sub>1</sub>	P <sub>2</sub>	D <sub>1</sub>	D <sub>2</sub>
R <sub>1</sub>	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R <sub>2</sub>		control		write *	execute			owner	seek *
⋮									
⋮									
R <sub>n</sub>			control		write	stop			

Credit: Figure 4.8 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

## Hierarchies in RBAC

Access Control

Concepts

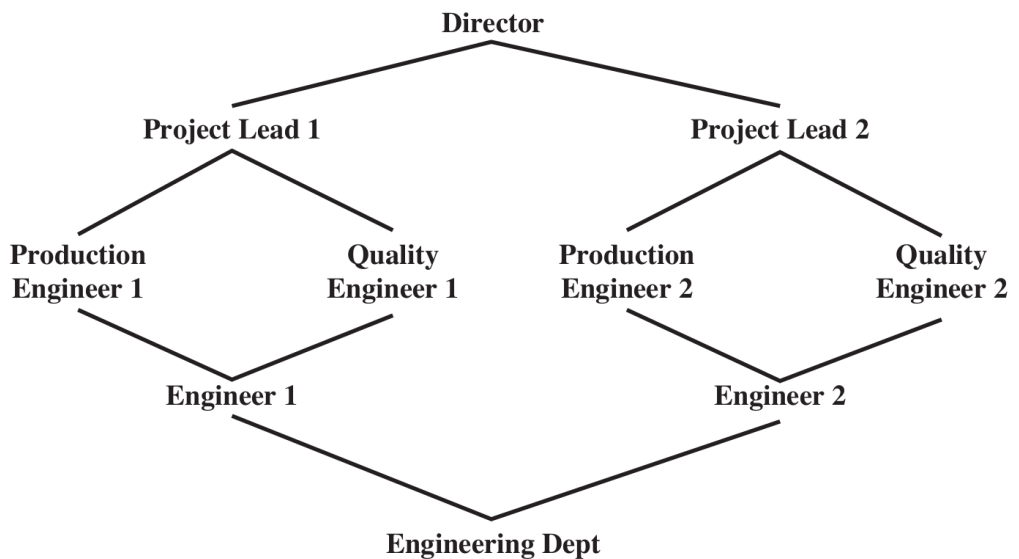
DAC

RBAC

MAC

Summary

- ▶ Hierarchy of an organisation can be reflected in roles
- ▶ A higher role includes all access rights of lower role



Credit: Figure 4.10 in Stallings and Brown, *Computer Security*, 2nd Ed., Pearson 2012

# Constraints in RBAC

- ▶ Constraints define relationships between roles or conditions on roles
- ▶ A higher role includes all access rights of lower role
- ▶ Mutually exclusive roles: user can only be assigned to one role in the set
- ▶ Cardinality: maximum number with respect to roles, e.g.
  - ▶ maximum number of users assigned to a role
  - ▶ maximum number of roles a user can be assigned to
  - ▶ maximum number of roles that can be granted particular access rights
- ▶ Prerequisite: condition upon which user can be assigned a role, e.g.
  - ▶ user can only be assigned a senior role if already assigned a junior role

19

# Contents

Access Control Concepts

Discretionary Access Control

Role-Based Access Control

Mandatory Access Control

Summary

20

# Mandatory Access Control

- ▶ Based on multilevel security (MLS)
  - top secret > secret > confidential > restricted > unclassified
- ▶ Subject has security clearance of a given level
- ▶ Object has security classification of a given level
- ▶ Two required properties for confidentiality:
  - No read up** Subject can only read an object of less or equal security level
  - No write down** Subject can only write into object of greater or equal security level
- ▶ Clearance and classification is determine by administrator; users cannot override security policy
- ▶ Bell-LaPadula model formally defines multilevel security and MAC

21

# Implementations of MAC

- ▶ SELinux: Linux kernel modules available to most Linux distributions (RedHat, Debian, Ubuntu, SuSE, ...)
- ▶ AppArmor: some Linux distributions (Ubuntu, SuSE)
- ▶ TrustedBSD: FreeBSD, OpenBSD, OSX, ...
- ▶ Mandatory Integrity Control: Vista, Windows 7, Windows 8

22

# Contents

## Access Control Concepts

## Discretionary Access Control

## Role-Based Access Control

## Mandatory Access Control

## Summary

23

# Key Points

- ▶ Access control to prevent unauthorized use of resources (objects) by subjects
- ▶ Subjects are processes on behalf of users and applications
- ▶ Classes of subjects: owner, group, world
- ▶ Objects: files, database records, disk blocks, memory segments, processes, . . .
- ▶ Access rights: read, write, execute, delete, create, . . .
- ▶ DAC: access rights may be granted to other subjects (common in operating systems and databases)
- ▶ RBAC: subjects take on role; access rights assigned to roles
- ▶ MAC: subjects/objects assigned to levels; subjects cannot modify assignment (e.g. military classification)

24

# Security Issues

Access Control

Concepts

DAC

RBAC

MAC

Summary

- ▶ Rely on correct assignment of capabilities/levels to subjects and objects by human administrator

25

# Areas To Explore

Access Control

Concepts

DAC

RBAC

MAC

Summary

- ▶ Trusted Computing and Trusted Platform Module (TPM)
- ▶ Secure Boot

26