CS604: Advanced System Security

Access Control Fundamentals II

Deepti Vidyarthi

Safety Problem

RBAC — DAC, MAC

Problem?

- Using protection state operations, untrusted user processes can modify the access matrix by adding new subjects, objects, or operations assigned to cells
- Permits untrusted processes to modify the protection state - discretionary access control (DAC) system
- Protection System is at discretion of users & processes

Role based Access. Dep Head Sec. Critical Fixed. General Purpose

Team Lead / Project Head MAC Fraud No Admin com.. MAC → DAC

Mandatory protection system

- Protection system that can only be modified by trusted administrators via trusted software

<u>mandatory protection state</u>

- operations that subject labels may take upon object labels
- Subjects and obje

<u>labeling state</u>

- maps the processes and system resource objects to label

<u>transition state</u>

- the legal ways that processes and system resource objects may be re-labeled.

Mandatory protection system

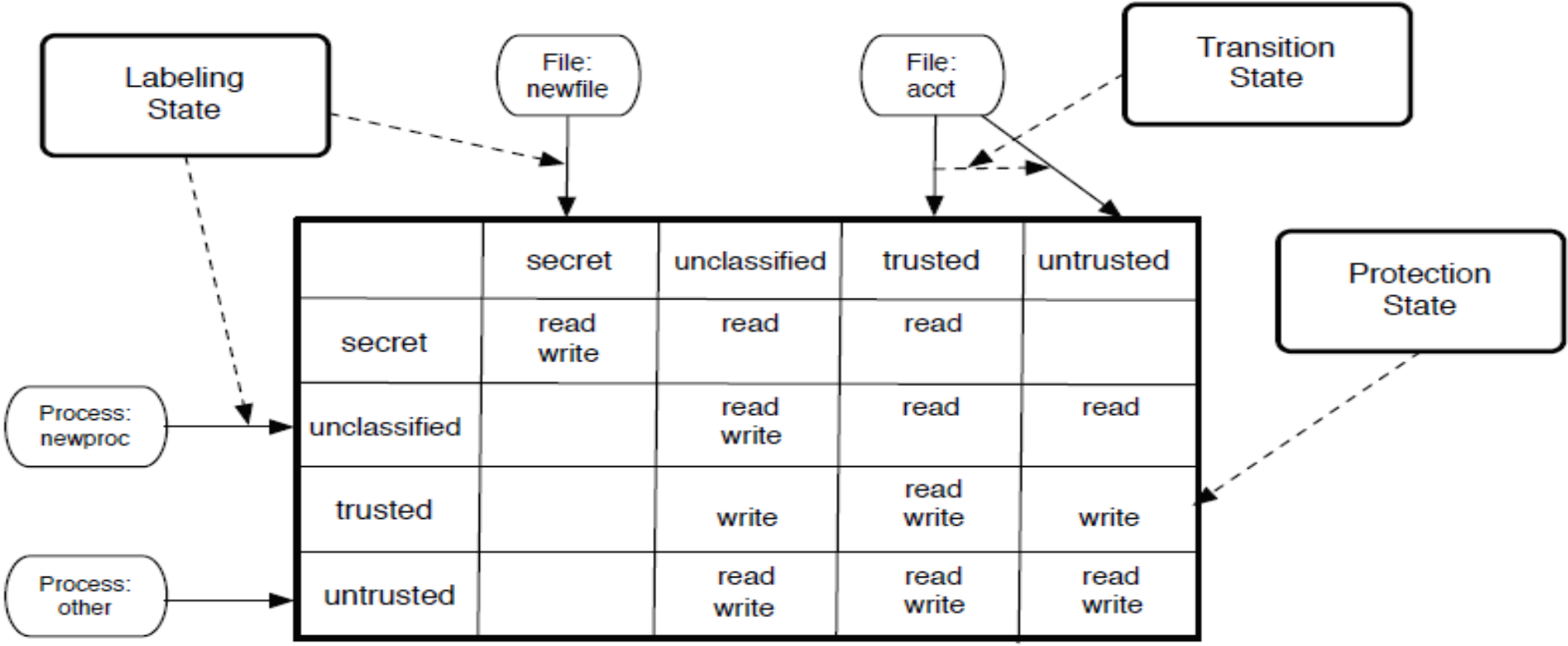
- Subjects & objects represented by system-defined labels - abstract identifier
- Tamperproof:
  - Set of labels is defined by trusted administrators using trusted software
  - Set of labels is immutable
- Mandatory access control (MAC) systems - protection system is immutable to untrusted processes
- Trusted administrators define the access matrix's labels and set the operations that subjects of particular labels can perform on objects of particular labels

Mandatory protection system

- Labeling state assigns labels to new subjects and objects
- E.g. When newfile is created, it must be assigned one of the object labels in the protection state

- Transition state enables a secure operating system to change the label of a process or a system resource
- Must be defined by trusted administrators and immutable during system execution

Mandatory protection system



	secret	unclassified	trusted	untrusted
secret	read write	read	read	
unclassified		read write	read	read
trusted		write	read write	write
untrusted		read write	read write	read write

Access Control Models

- Access Control Models:
- Three Main Types
  - Discretionary
  - Mandatory
  - Non-Discretionary (Role Based)

Access Control Models

- Discretionary Access Control (DAC)
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.

Access Control Models

- Mandatory Access Control (MAC)
  - Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
  - This model is used in environments where information classification and confidentiality is very important (e.g., the military).

Access Control Models

- Non-Discretionary (Role Based) Access Control Models
  - Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
  - Is the best system for an organization that has high turnover.

Access Control Techniques

- There are a number of different access controls and technologies available to support the different models.
  - Rule Based Access Control
  - Access Control Matrix
  - Content Dependent Access Control
  - Context Dependent Access Control

Access Control Techniques

- Rule Based Access Control
  - Uses specific rules that indicate what can and cannot happen between a subject and an object.
  - Not necessarily identity based.
  - Traditionally, rule based access control has been used in MAC systems as an enforcement mechanism.

Access Control Techniques

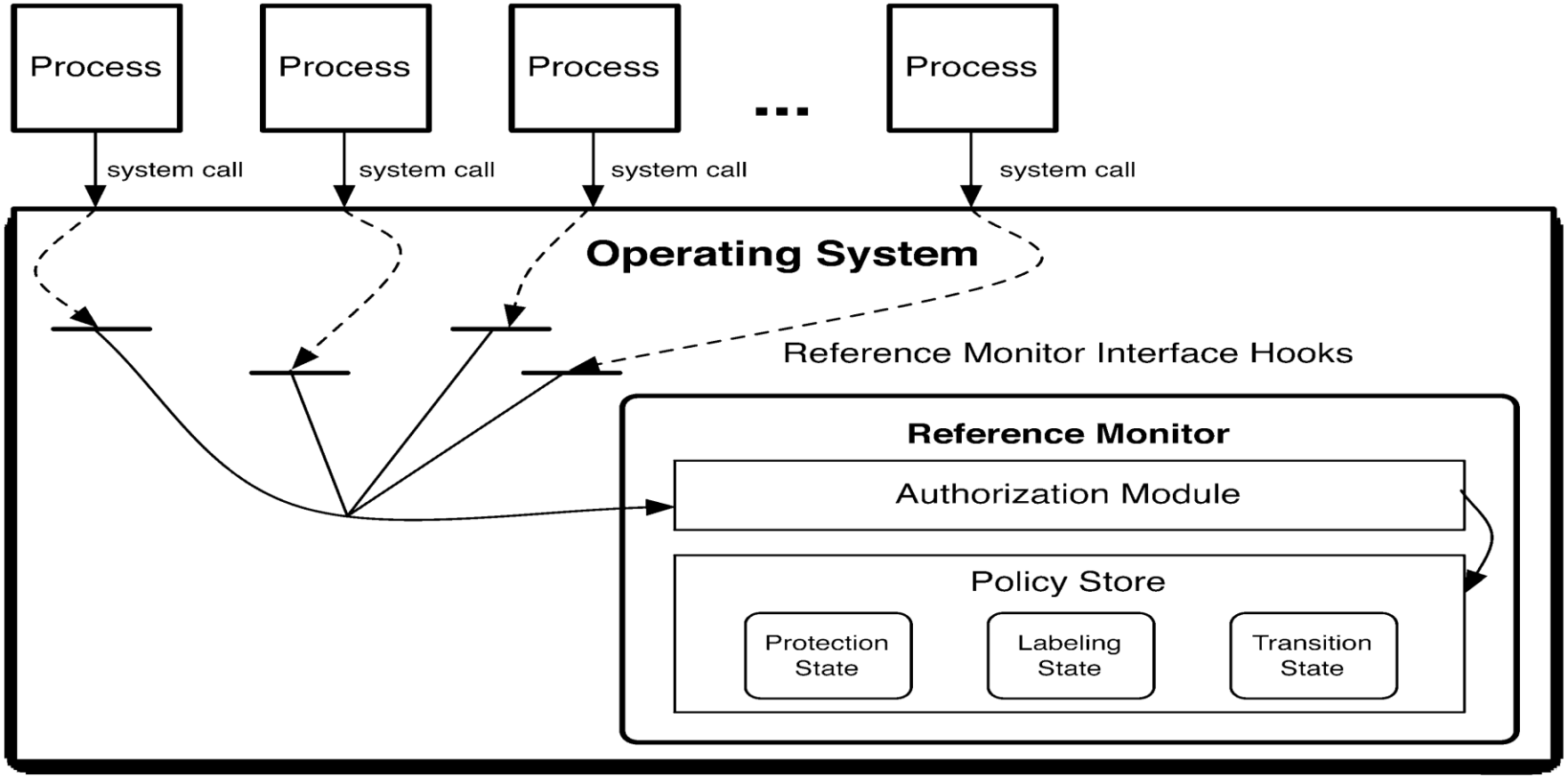
- Content Dependent Access Control: Access to an object is determined by the content within the object.
- Context Based Access Control: Makes access decision based on the context of a collection of information rather than content within an object.

Reference monitor

- Access enforcement mechanism
- A request as input, and returns a binary response (request is authorized or not)
- Three components:

1) interface
2) authorization module
3) policy store

Reference monitor



Reference monitor

1) interface
2) authorization module
3) policy store

Access Control

- Study aspects of access control in OS:

- User management
- Login
- Privileges
- Access Permissions

Access Control in Windows

- Users
  - Administrator
  - User
  - Guest User

Access Control in Windows

Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

Family & other users

Your family

Add your family so everybody gets their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.

Add a family member

Learn more

Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

Set up a kiosk

Access Control in Windows

This PC > Docs (G:) > COURSES > OS_Security > 2020 >

Name

- 2020
- COURSE_HANDOUT-OSS2020.docx
- OSS20-1intro.pdf
- OSS20-1intro.pptx
- OSS20-2intro.pdf
- OSS20-2intro.pptx
- OSS20-3access-control.pdf
- OSS20-3access-control.pptx
- OSS20-5access-control-examples.pptx
- OSS2020-Syllabus-course-handout.pdf
- updated-OSS20-4mac.pdf
- updated-OSS20-4mac.pptx
- video.mp4

OSS20-1intro.pdf Properties

General | Security | Details | Previous Versions

Object name: G:\COURSES\OS_Security\2020\OSS20-1intro.pc

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (LAPTOP-J69NJLPQ\Administrators)
- Users (LAPTOP-J69NJLPQ\Users)

To change permissions, click Edit. Edit...

Permissions for Authenticated Users

	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced. Advanced

OK | Cancel | Apply

Access Control in Linux

- Users -
  - Root
  - normal users
  - Guest users

- File properties
  - command “ls –l”
  - rwx

- Who can change

Access Control in Android/iOS

- Users -
  - Root / normal users?
  - Different privileges?
- File properties
  - Permission model
- Who can change

Practice

- Explore
  - Users – login mechanisms
  - Privileges
  - Accesses w.r.t files
  - Who can modify

- Lab setup –
  - Oracle Virtual box
  - Ubuntu/Fedora/Kali Linux – stable version

- Submit
  - Screenshots
  - Observation
  - Friday 5 pm

References

- Operating System Security (Trent Jaeger)
- All in One Book (Shon Harris, 2005)