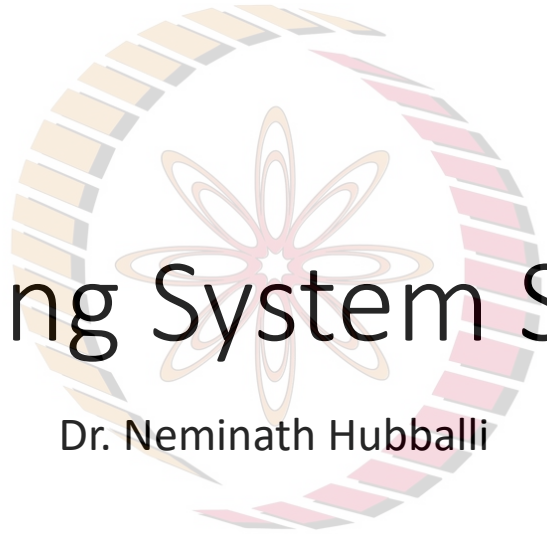


The NPTEL logo is a circular emblem. It features a central stylized flower or star shape with eight petals, rendered in a light pink and orange color. This central motif is surrounded by a ring of alternating orange and pink segments, creating a circular border. The entire logo is semi-transparent and serves as a background for the title text.

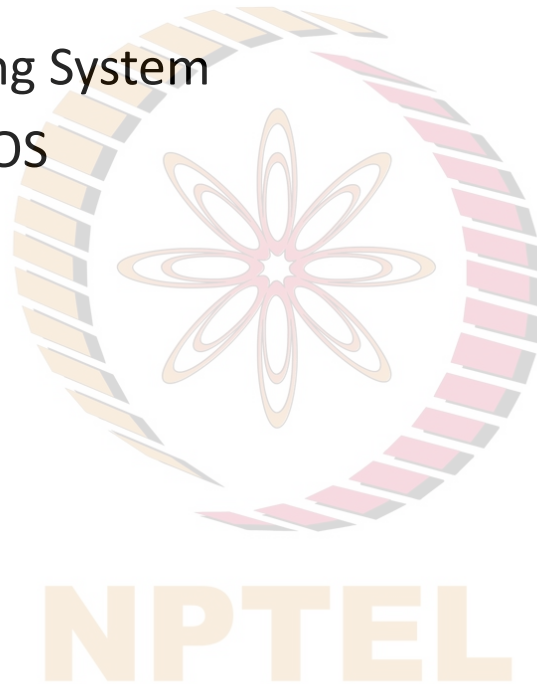
Operating System Security

Dr. Neminath Hubballi

NPTEL

Outline

- ❑ Functions of Operating System
- ❑ Security concerns in OS
- ❑ Process security
- ❑ File Security



Functions of Operating System

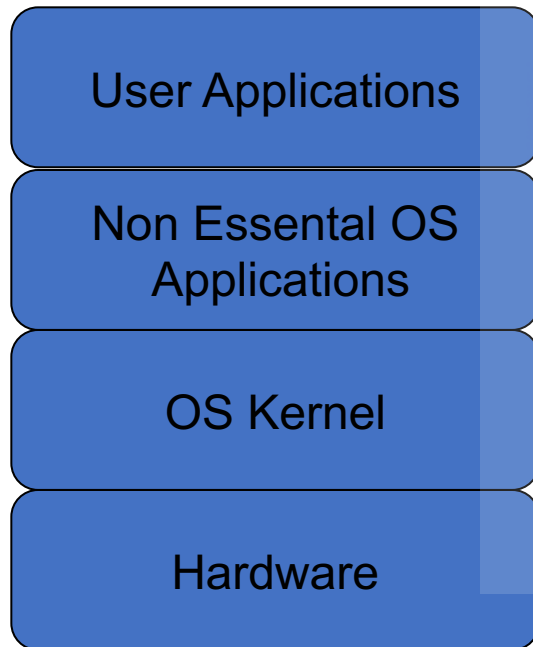
- ☐ Provides abstraction from hardware
- ☐ Handle many complex tasks
 - ☐ Memory management
 - ☐ Process management
 - ☐ Handling deadlocks
 - ☐ File system support
 - ☐ Multitasking
 - ☐ Multi user support



What Can Go Wrong ?

- ☐ Consider a situation where there is shortage of systems in school of CSE
- ☐ If you are asked to share same PC with your peers
 - ☐ What do you want to do
- ☐ Users have different level of access
 - ☐ Based on role
- ☐ Multiple users and multi tasking requires a level of protection
 - ☐ One user from interfering other users
 - ☐ One program from interfering other users
- ☐ Sharing of resources
 - ☐ Optimization

Organization of Computer Hardware and Software



☐ Hardware

- ☐ Many devices

- ☐ Each device has a driver

- ☐ Provides APIs to access

☐ Kernel

- ☐ Heart of OS

- ☐ Manages the low level h/w resources

☐ Non essential component of OS

- ☐ Printing program

☐ User application

- ☐ Access the service provided by OS

- ☐ System calls

Process

- ☐ Kernel defines the notion of a process
- ☐ Programs are stored in persistent storage
- ☐ Can multiple copies of same program run simultaneously ?
- ☐ Time slicing
- ☐ Process tree
- ☐ Fork system call
 - ☐ Parent and child
 - ☐ Peers
- ☐ In Linux system init is the root of process tree
 - ☐ Meaning all other processes are created by it
 - ☐ Its PID is 0

NPTTEL

Process Privileges

- ❑ To grant appropriate access restrictions on the process operating system associates privilege information to a process
- ❑ This privilege is same as privilege of user who is running the process
- ❑ Each process has a user id called *uid*, group id *gid*
- ❑ The *uid* is a number between 0 to 32767 which uniquely identifies each user
- ❑ Typically *uid* 0 is assigned to the root user
- ❑ Similarly *gid* is also a number in the same range
- ❑ Effective user id *eid* is the user id whose privileges are used to access a resource

Inter-Process Communication

- ☐ File
- ☐ Pipes
- ☐ Sockets



File System

- ☐ File System: An abstraction of how the external, nonvolatile memory of the computer organized.
- ☐ File hierarchy
 - ☐ Folders and directories
- ☐ Concerns
 - ☐ Who should access what ?
 - ☐ Who should execute what ?
 - ☐ Prevent one file content going to another

NPTTEL

File Ownership and Permissions

- ☐ Permissions:
 - ☐ Assigned to each file/directory
 - ☐ Provides security
 - ☐ Ability to manage users and their files.
 - ☐ Needed to access file/directory
 - ☐ Usually granted to groups
- ☐ In multi-user operating systems like Linux, access is given only to authorized users
- ☐ Super (root) user:
 - ☐ Has special privileges –
 - ☐ In a sense owns everything
 - ☐ Can change file ownerships
 - ☐ Bypass permissions that owner of file may have set
 - ☐ Uses root account to provide administrative functions

File Ownership and Permissions

- ☐ Unix systems treat everything as a file
- ☐ Special files
 - ☐ Devices- a piece of hardware either part of system or an external unit
 - ☐ Sockets- a means of communicating with other processes
- ☐ Permissions can be of
 - ☐ Read
 - ☐ Write and
 - ☐ Execute

NPTTEL

Sticky Bit in Unix

- ❑ Sticky Bit: Mainly used to avoid some other user deleting a file though she has a write permission on the folder
- ❑ If Sticky bit is enabled on a folder, the folder contents are deleted by only owner who created them and the root user.
- ❑ This is a security measure to avoid deletion of critical folders and their content(sub-folders and files), though other users have full permissions.
- ❑ Setting sticky bit
 - ❑ `chmod +t /opt/dump/`
 - ❑ `+t` indicates sticky bit setting\
- ❑ Check sticky bit
 - ❑ `ls -l` : a `t` will appear in the listing
- ❑ Revoking sticky bit
 - ❑ `Chmod -t /opt/dump/`

NPTTEL