CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

User Authentication, Access Control, and Operating System

AC UNIX/LINUX Access Control

Video Summary

- How UNIX/LINUX Files are Administered?
- What is inodes?
- UNIX/LINUX File Access Control
- DEMO

UNIX File Access Control

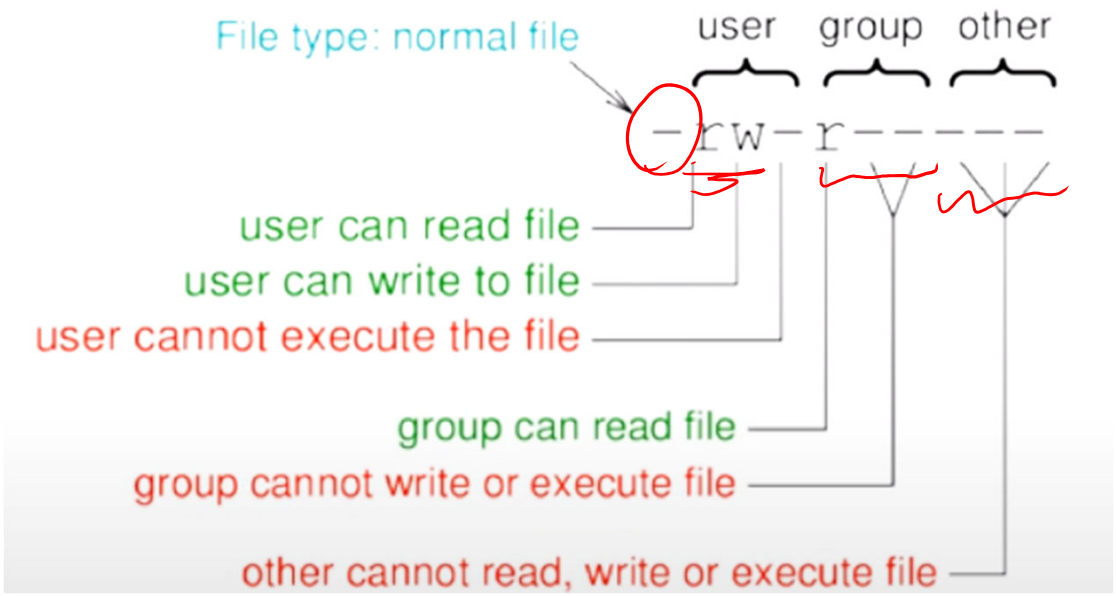
UNIX files are administered using inodes (index nodes)

- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

Protection bits in an inode



inode

- Files and directories administered by operating system using inodes
- inode is data structure that stores important information about a file or directory
  - mode
  - owner information
  - size
  - timestamps
  - pointers to data blocks (data blocks contain the actual file)
- OS maintains list of inodes in inode table

inode Contents

mode 16 bits

- 12 protection bits: permissions
- 4 bit file type: regular file, directory, ...

owner id 16 bit user ID

group id 16 bit group ID

size size of file in bytes

timestamps last time, in seconds since epoch:

- atime: inode accessed
- ctime: inode changed
- mtime: file data modified

and other fields ...

Permissions and Users

Permissions

- read the file; list the contents of the directory
- write to the file; create and remove files in the directory
- execute the file; access files in the directory

Categories of Users

- user that owns the file
- users in the file's group
- other users
- (all users, i.e. the above three)

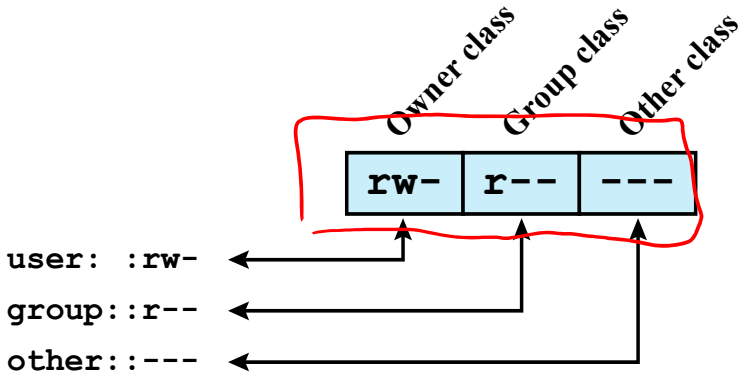
Permissions and Users

Special Permissions

- setuid bit: Set the process's effective user ID to that of the file
  - Directory: files created in that directory are given same user owner as the directory
- setgid bit: Set the process's effective group ID to that of the file
  - Directory: files created in that directory are given same group owner as the directory
- sticky bit: prevent users from removing or renaming a file unless they are user owner

UNIX File Access Control (DEMO)

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



(a) Traditional UNIX approach (minimal access control list)