Unix protection on files

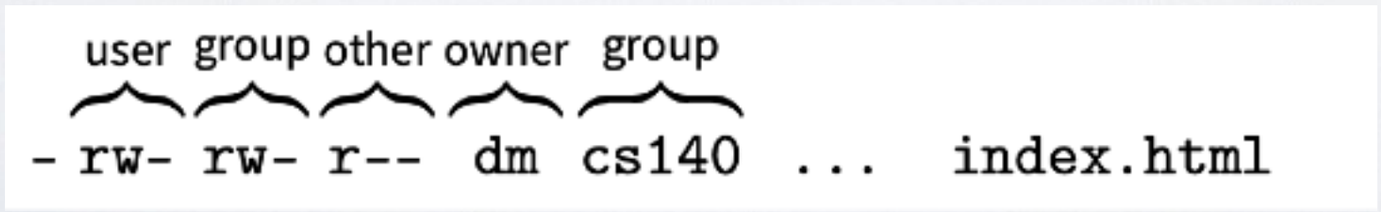
Each process has a User ID & one or more group IDs

System stores with each file

- User who owns the file and group file is in
- Permissions for user, any one in file group, and other

Shown by output of `"ls -l"` command

- Each group of three letters specifies a subset of **r**ead, **w**rite, and **e**xecute permissions
- User permissions apply to processes with same user ID
- Else, group permissions apply to processes in same group
- Else, other permissions apply



Unix protection on directories

Directories have permission bits, too

- Need write permission on a directory to create or delete a file
- Execute permission means ability to use pathnames in the directory, separate from read permission which allows listing

Special user root (UID 0) has all privileges

- e.g. read/write any file, change owners of files
- Required for administration (backup, creating new users, etc.)

For instance `drwxr-xr-x 56 root wheel 4096 Apr 4 10:08 /etc`

- Directory writable only by root, readable by everyone
- Means non-root users cannot directly delete files in `/etc`