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`

Unix permissions on non-files

Many devices show up in file system
e.g. `/dev/tty1` permissions just like for files

Other access controls not represented in file system
e.g. must usually be root to do the following

- Bind any TCP or UDP port number less than 1024
- Change the current process's user or group ID
- Mount or unmount most file systems
- Create device nodes (such as `/dev/tty1`) in the file system
- Change the owner of a file
- Set the time-of-day clock; halt or reboot machine