Access Control and File Permission

Discretionary Access Control (DAC)

- Users can protect what they own
  - The owner may grant access to others
  - The owner may define the type of access (read/write/execute) given to others
- DAC is the standard model used in operating systems
- Mandatory Access Control (MAC)
  - Alternative model not covered in this lecture
  - Multiple levels of security for users and documents
  - Read down and write up principles

Access Control Entries and Lists

- An Access Control List (ACL) for a resource (e.g., a file or folder) is a sorted list of zero or more Access Control Entries (ACEs)
- An ACE specifies that a certain set of accesses (e.g., read, execute and write) to the resources is allowed or denied for a user or group
- Examples of ACEs for folder "Bob's CS167 Grades"
  - Bob; Read; Allow
  - TAs; Read; Allow
  - TWD; Read, Write; Allow
  - Bob; Write; Deny
  - TAs; Write; Allow

Unix Permissions

- Standard for all UNIXes.
- Every file is owned by a user and has an associated group.
- Permissions often displayed in compact 10-character notation.
- To see permissions, use **ls –l**.
- For the first character a **-** (hyphen) indicates a plain file, **d** a directory and **l** a soft link.
- The remaining 9 characters are split into 3 components of 3 characters each, to describe the user's, group's and others' privileges respectively.
- Within each 3 character triplet, the first indicates read permission, the second is for write permission and the third is for execute permission.
- If the **r, w** or **x** character is present, the permission is allowed, if the position is occupied by a **-** (hyphen) the permission is denied.

File Permission Examples

-rwxr-xr--	indicates user read, write and execute rights, group read and execute rights, and read rights only for others.
drwxr-xr--	indicates a directory which can be displayed and searched by user and group. User can also delete, create and rename files in the directory. Others may list the directory but not search through it or access files in it.

```
rodan:~/java % ls -l
total 24
-rwxrwxrwx   1 goodrich faculty     2496 Jul 27 08:43 Floats.class
-rw-r--r--   1 goodrich faculty     2723 Jul 12  2006 Floats.java
-rw-------   1 goodrich faculty      460 Feb 25  2007 Test.java
rodan:~/java %
```