Permissions

Matt Warner

1 Overview

Unix is a multi user system, meaning more than one user has access to the system. Therefore, access to directories and files needs to be controlled, so that one user does not interfere with what other users have in mind

Unix uses discretionary access control (DAC) model. So,

- Each directory/file has an owner
- The owner has discretion over access control details

Access control includes

- read, write: to protect information
- execute: to protect state of system

Note:-

There is an exception for the super user. The super user does not need permission to access directories/files. They have access to everything

2 User Terminology

- user
  - any one who has account on the system, listed in /etc/passwd
  - protected via password, listen in /etc/shadow
  - internally recognized via a number called "user id"
- group
  - users are organized into groups, listed in /etc/group
  - user can belong to multiple groups
- super user, root
  - has user id "0"
  - responsible for system administration

3 File/Directory access

- file or directory has an owner, that is, the user who created it.
- owner sets access permissions
  - access mode: read, write, execute
  - accessor category: self, group, others
- ownership change via: **chown**

	Meaning on File	**Meaning on Directory**
r (read)	View file contents (open, read)	List directory contents
w (write)	Change file contents	Change directory contents
x (execute)	Run executable file	Make it current directory, search for files in it

Table 1: Permissions and their meanings on files and directories

4 Accessor Categories

3 categories of users want access