File Permissions & Security

Module 17

Overview

- In this module:
  - How Permissions Work
  - Permission Evaluation
  - Permissions on Files & Directories
  - Changing Permissions – Symbolic
  - Changing Permissions – Numeric
  - Changing Ownership
  - Changing File Ownership
  - SUID & SGID

Ownership

- Every file & directory has:
- an owner or user
- a group owner
- It also has 3 sets of permissions, for:
- user
- group
- other – everyone else

Process Ownership

- Every process also has:
- an owner or user
- a group owner

Permissions on Files

- read
- process can read data in the file
- write
- process can write to file
- execute
- process can load the data into memory and attempt to execute it

Permissions on Directories

- read
- process can read content of the directory

–ie list its contents

- write
- process can write to directory

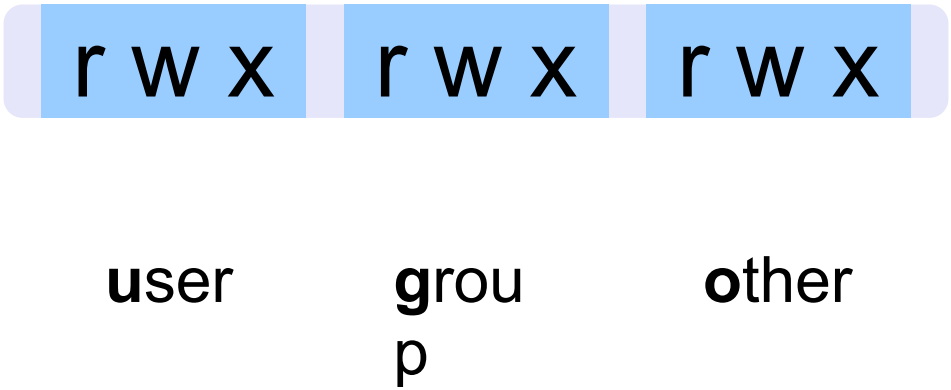
–ie add or remove files

- execute
- process can ‘search’ directory for a named file

Permission Types

- Files and directories have 9 permission bits:

```
[peter@server1 ~]$ ls -l
-rw-rw-r--. 1 peter peter  23726 May 18  2011 file1
[peter@server1 ~]$
```

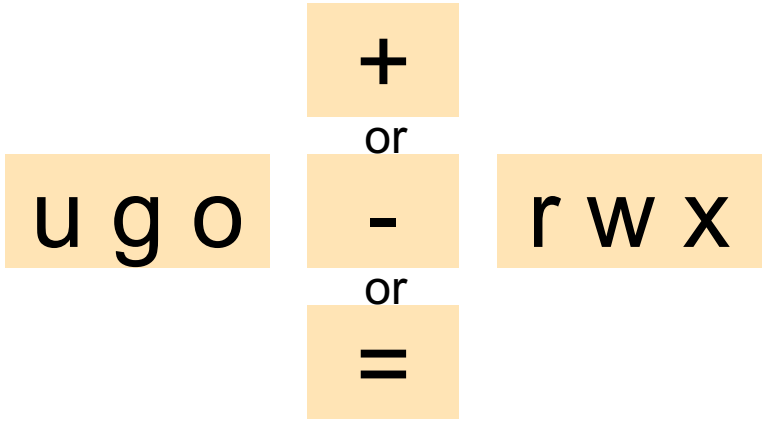


Permission Evaluation

- Permissions are evaluated left-to-right:
- if process owner matches file owner
  - user permissions are used
- if process group matches file group
  - group permissions are used
- otherwise
  - other permissions are used

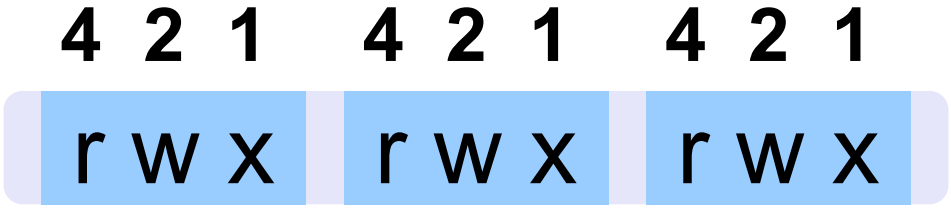
Changing Permissions – Symbolic

- Examples:
- To add permissions:
  - chmod u+w file1
- To remove permissions:
  - chmod g-wx file1
- To set permissions:
  - chmod o=rx,g=r file1



Changing Permissions – Numeric

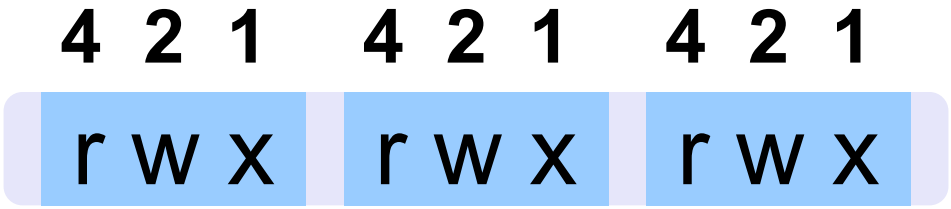
- Alternatively, specify all permissions in octal:



- Examples
  - chmod 644 file1
  - chmod 755 prog1
  - chmod 511 dir1

Default Permissions

- Typically, files created with



- umask
- specifies bits to switch **off**
  - eg umask 022

Changing File Ownership

- chown
- Change file owner
  - $ chown dave file1
- chgrp
- Change file group owner
  - $ chgrp users file1

SUID & SGID

- Additional permissions bits
- SUID – set user ID
  - assume user identity of executed file
- SGID – set group ID
  - assume group identity of executed file