

File Protection Mechanisms

Adapted from [Pfl96, Section 6.4].

- All or Nothing Protection: Trust and ignorance.
 - May work in systems with few users who trust each other.
 - No convenient way of limiting file access to subset of users.
- Group Protection: Need to share in a controlled way.
 - (*user, group, world*).
 - Define access rights on file creation. For e.g., the `open(path, mode)` syscall will use (`defaults & umask`).
 - A user is identified by two identifiers (numbers), the user-id and the group-id.
 - On Linux, `/etc/passwd` contains a record for every user (non NIS).
user_name:pwd:uid:gid:comment:home_dir:login_shell
root and lroot
 - `/etc/group` defines groups. (`newgrp`)
group_name:pwd:gid:uid_list
- File and Directory permissions (there are ACLs in other OSes).
 - Sticky bit on directories. Allows removal/renaming of files that you own. `/tmp` is `drwxrwxrwt` on my machine.
 - Extra attributes on the ext2 FS. `lsattr`, `chattr`.
1 word (`include/linux/ext2_fs.h`) = {
 - A (don't update atime)
 - a (open append only)
 - c (compress)
 - d (mark for dump)

```
i (immutable)
s (zero blocks on delete)
S (write synchronously)
u (save contents on delete)
}
```

Linux immutable files: cannot change or delete files.

▷ `chattr +i foo`, only root can set/unset.

▷ `lsattr foo`, (`---i----- foo`)

▷ `ls -l foo`, (`-rw-r--r-- 1 s-kumar emp`)

- Quota (# of blocks/inodes), `ulimit` (core file size, max data segment size, max cpu time, max open files)
`struct rlimit rlim[RLIM_NLIMITS];` (`linux/include/sched.h`).

References

[Pfl96] Charles P. Pfleeger. *Security in Computing*. Prentice Hall, iind edition, 1996.