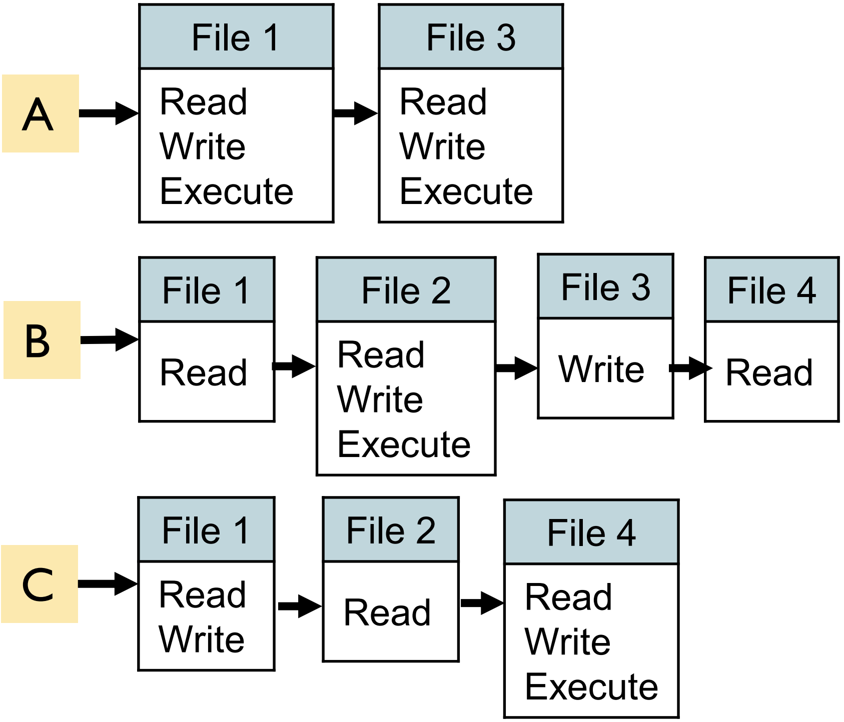
Capability List (C-List)

In practice, an access control matrix is usually sparse and can be implemented by decomposition in one of two ways

Decomposition by rows

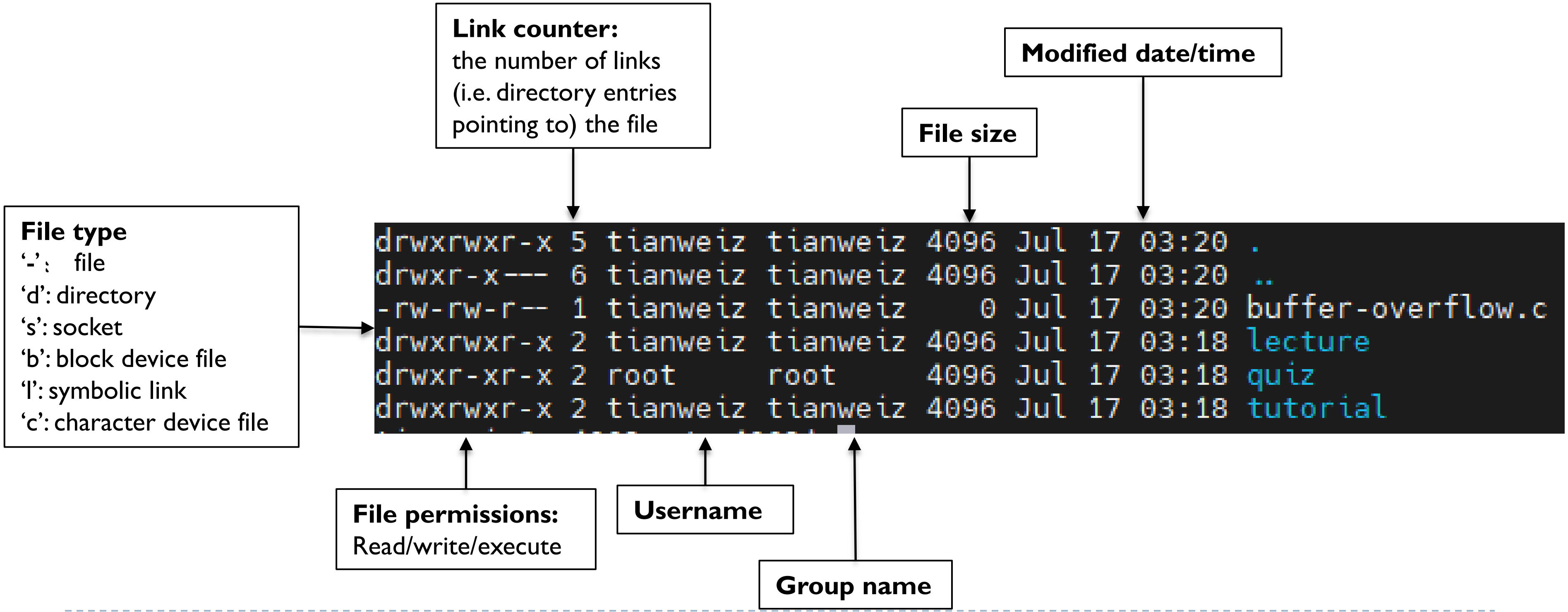
- C-list specifies authorized objects and operations for a particular user.
- C-List is convenient when determining the access rights available to a specific user.



Example: Resource Management in Unix OS

Files, directories, memory devices, I/O devices are uniformly treated as resources

- These resources are the objects of access control.
- Each resource has a single user owner and group owner



Link counter: the number of links (i.e. directory entries pointing to) the file

Modified date/time

File size

File type
'-' : file
'd': directory
's': socket
'b': block device file
'l': symbolic link
'c': character device file

```
drwxrwxr-x 5 tianweiz tianweiz 4096 Jul 17 03:20 .
drwxr-x--- 6 tianweiz tianweiz 4096 Jul 17 03:20 ..
-rw-rw-r-- 1 tianweiz tianweiz    0 Jul 17 03:20 buffer-overflow.c
drwxrwxr-x 2 tianweiz tianweiz 4096 Jul 17 03:18 lecture
drwxr-xr-x 2 root     root     4096 Jul 17 03:18 quiz
drwxrwxr-x 2 tianweiz tianweiz 4096 Jul 17 03:18 tutorial
```

File permissions: Read/write/execute

Username

Group name

Permission Representation

Three permissions with three subjects

- Read, Write, Execute
- Owner, Group, Other
- Examples:
  - rw-r--r--: read and write access for owner, read access for group and other.
  - rwx------: read, write, and execute access for owner, no rights to group and other.

Octal Representation

- rw-r--r--: 110 100 100: 644
- rwx------: 111 000 000: 700

Adjust permission:

- Users can change the permissions:
  - chmod 754 filename
  - chmod u+wrx,g+rx,g-w,o+r,o-wx filename
- root can change the ownerships:
  - chown user:group filename

Controlled Invocation

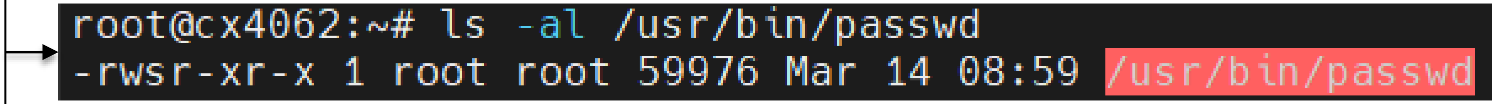
Superuser privilege is required to execute certain OS functions

- Example: password changing
  - User passwords are stored in the file /etc/shadow
  - This file is owned by the root superuser. A normal user has no access to it
  - When a normal user wants to change his password with the program passwd, this program needs to give him additional permissions to write to /etc/shadow

SUID: a special permission flag for a program

- If SUID is enabled, then user who executes this progam will inherit the permissions of the program's owner.
- A normal user executing passwd can get additional root permission to write the new password to /etc/shadow

The execute permission of the owner is given as s instead of x



```
root@cx4062:~# ls -al /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Mar 14 08:59 /usr/bin/passwd
```

Security of Controlled Invocation

Many other SUID programs with the owner of root

- /bin/login: login; /bin/at: batch job submission; /bin/su: change UID

Potential dangers

- As the user has the program owner's privileges when running a SUID program, the program should only do what the owner intended
- By tricking a SUID program owned by root to do unintended things, an attacker can act as the root

Security consideration

- All user input (including command line arguments and environment variables) must be processed with extreme care
- Programs should have SUID status only if it is really necessary.
- The integrity of SUID programs must be monitored.