Process Credentials

Real User and Real Group id (r): who executes the process)

inherit from login shell whose real user/group id is from /etc/passwd

Effective user/group id (e): process permission of system calls (file, IPC, signal ...)

when e=0, it is a privileged process.

e=r if not set user/group-id program, otherwise e =owner of file.

Set user/group id program: e = owner of file

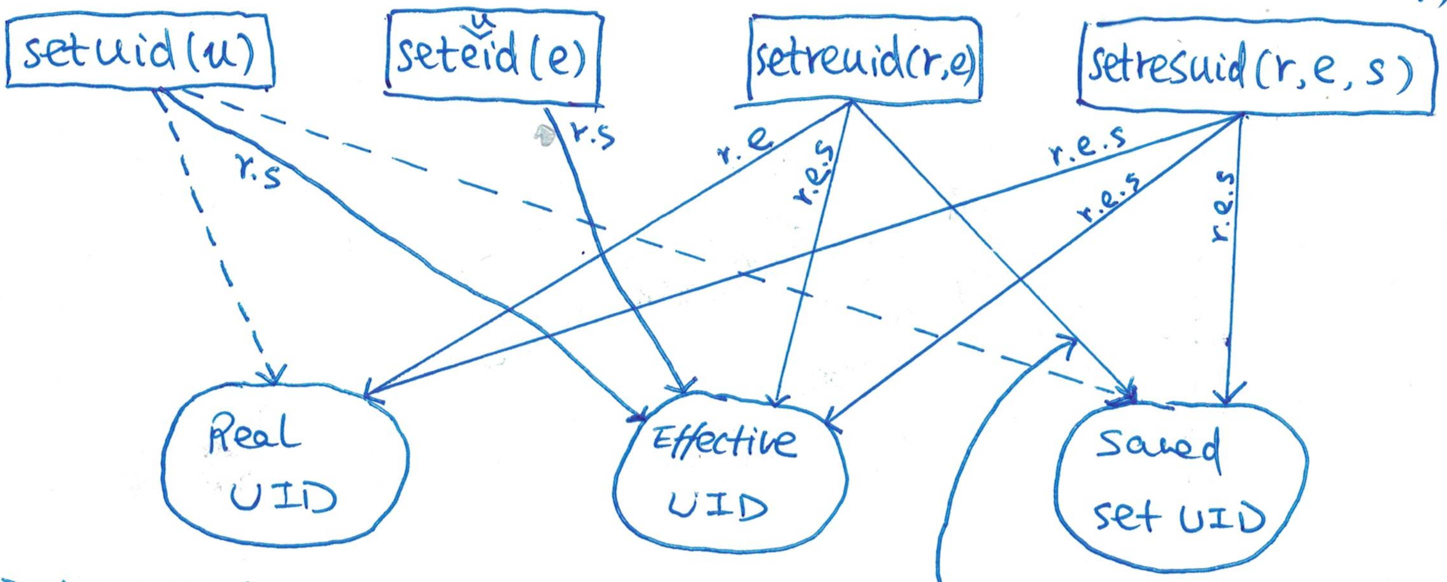
in ls, we use 's' to rep 'x' for set-u/g id program

```
ls -l prog  →  -rwxr-xr-x
chmod u+s prog ; ls -l prog → -rwsr-xr-x
chmod g+s prog ; ls -l prog → -rwsr-sr-x
```

saved user/group id: s = e after e is inited

Supplementary Group IDs. additional groups of the use that executes the process
inherit from login shell and ~~/etc~~ read from /etc/groups.

Change id system calls (CAP_SETUID/CAP_SETGID can change user/group id arbitrarily)



---> only privileged

$\xrightarrow{r.s}$ can only change to current r and s

if r≠-1 or e != previous real then saved set-user-ID is made same as possibly new e.

eg: setuid(u) for privileged will change r. s and e

for un-privileged change only e (can only change to r or s)