- 1. Last time
- 2. Protection and security in Unix
  - Intro
  - Setuid
  - TOCTTOU
  - Other thoughts

---

2. Protection and security in Unix

A. Intro

UIDs, GIDs (user id, group id)

A process has one user id and one or more group ids

Files and directories are access-controlled

- Saw this in lab 2 (ls)
- System stores w/ each file who owns it
- Where is the info stored?

Special user: uid 0, called root, treated by kernel as the administrator.

(rwx) permissions: can

UID 0 (root) has all permissions

read any file, do anything.

certain things only root can do:

- set clock
- halt machine
- mount filesystems
- change process's user or group id

B. setuid

ex: how do users change their password?

/etc/passwd

/etc/shadow

$ passwd

A prog. can be "setuid"

$ ls

real uid: mwalfish

effective uid: mwalfish

$ passwd

real uid: mwalfish

effective uid: root

"substitute user"

"su": stands for substitute user

binary ↗

change to new userid if correct passwd is typed.

Example attacks

(a) attacker in an attacker binary

eff uid: <eviluser>
real uid: <eviluser>

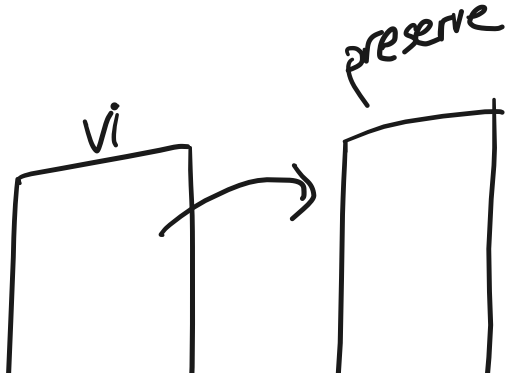
```
close(2);
exec("/usr/bin/passwd");
```

real uid: <eviluser>
eff uid: 0 <root>

```
passwd:
    main()
    {
        fd = open("/etc/passwd", ...)   // WR
        2
        .
        .
        .
        fprintf(stderr, "Err msg\n");
                ?
```

(b) old days: "preserve"

setuid root



attacker:
create "bin", which does:

```
cp /bin/sh ./attack
chown root attack
chmod 4755 attack
```

define IFS back

attacker redefines IFS='/',
and runs vi in that environment.

preserve:

```
system("/bin/mail");
```

parsed as "bin mail"

---

ptrace() attacks

TOCTTOU

setuid program: P <logfile>

/etc/shadow

user input

```
fd = open(logfile,
          O_CREAT | O_WRONLY |
                    OTRUNC,
          0666)
```

access(): check whether the real id, not effective id, is allowed to access the file.

```
if (access (logfile, W_OK) < 0)
    return ERROR;
fd = open (logfile, ... )  /* as above */
```

attacker runs "P /tmp/X"

P

attacker

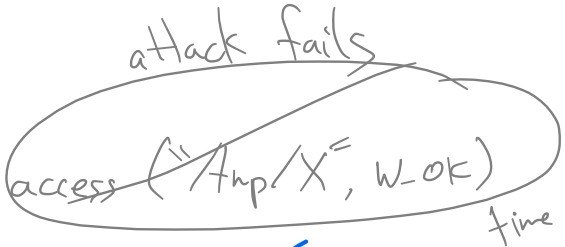
creat("/tmp/X");

time of check

checks access("/tmp/X") → OK

unlink("/tmp/X");

symlink("/etc/passwd", "/tmp/X");



time of use

fd = open("/tmp/X", O_TRUNC | O_WRONLY);

fd represents /etc/passwd