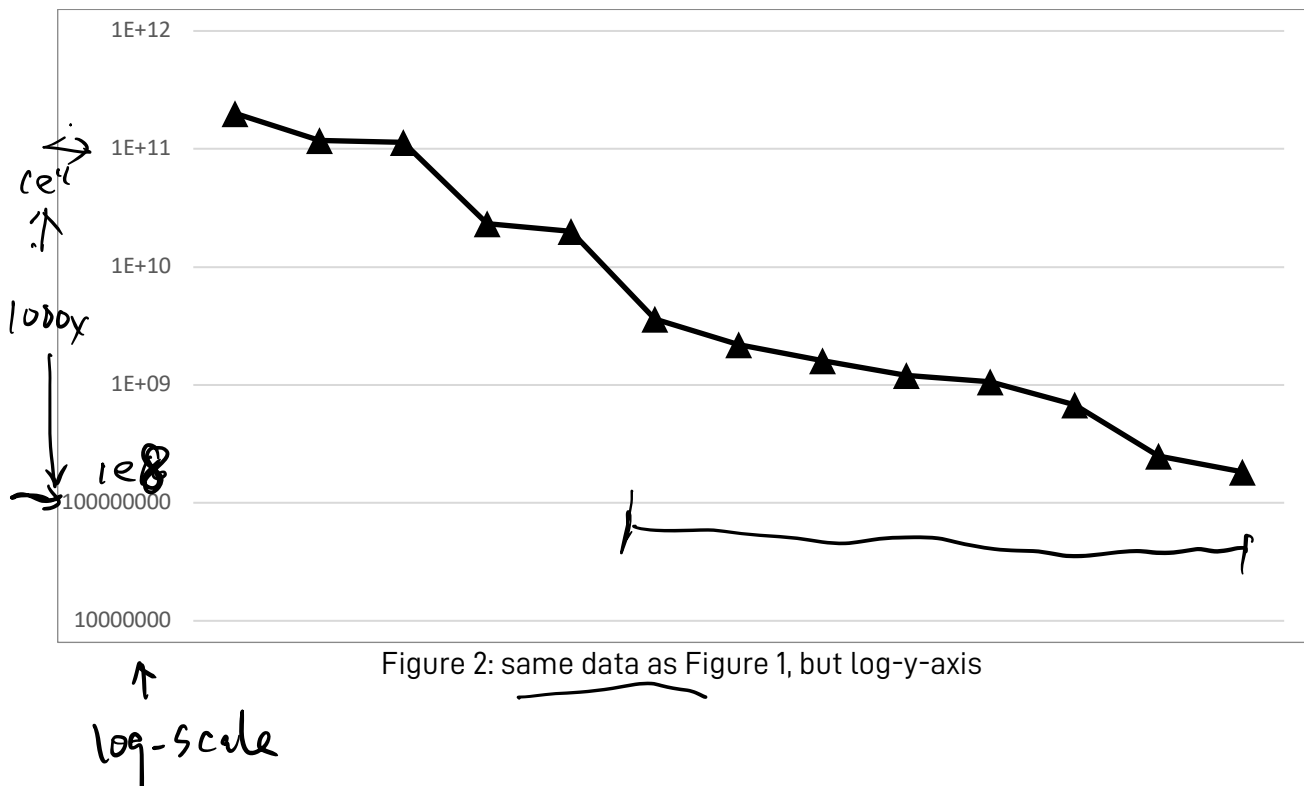
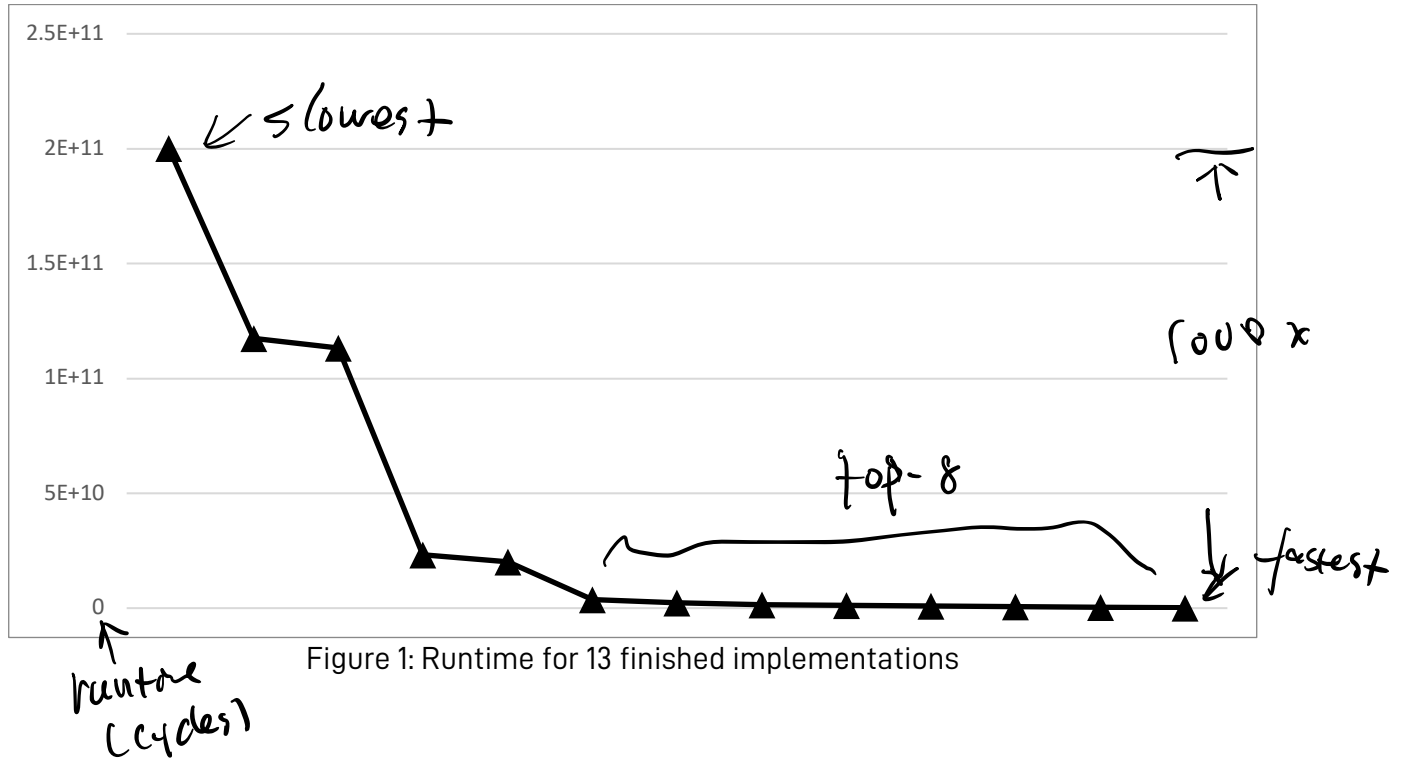
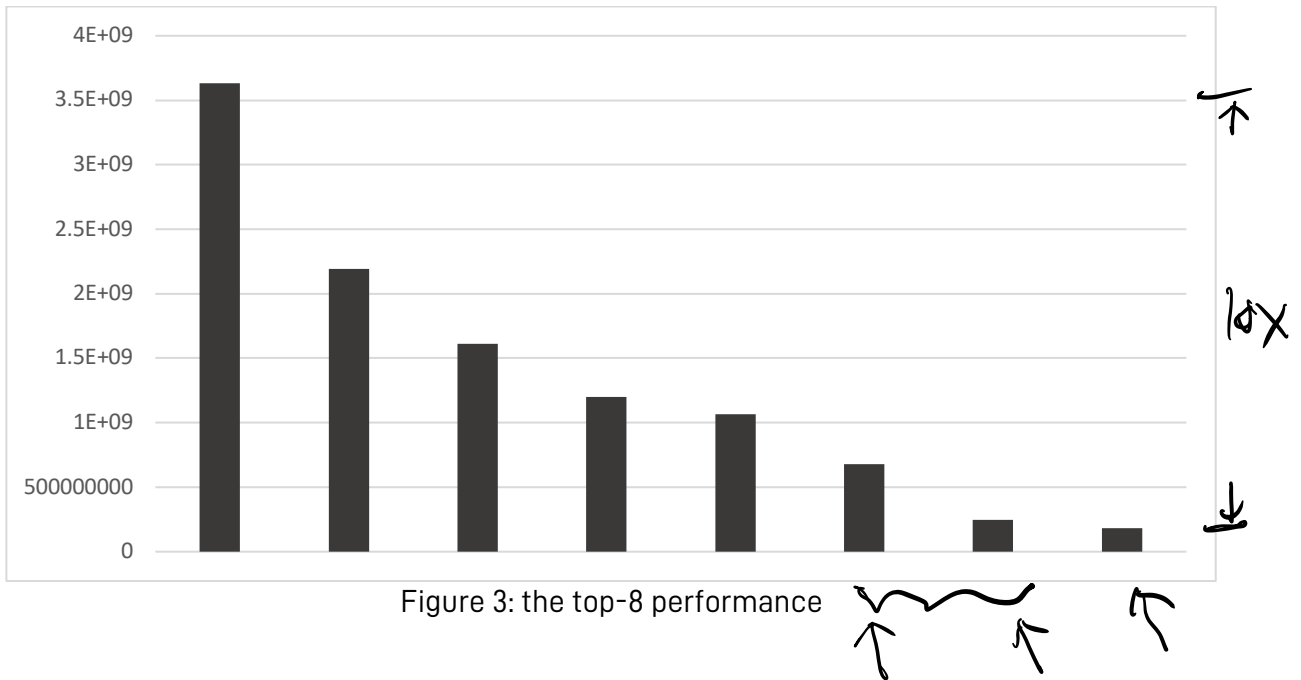


Lab3 challenge statistics

- 16 attendees, 3 timeout
- Runtime for 13 finished ones below





Take-aways:

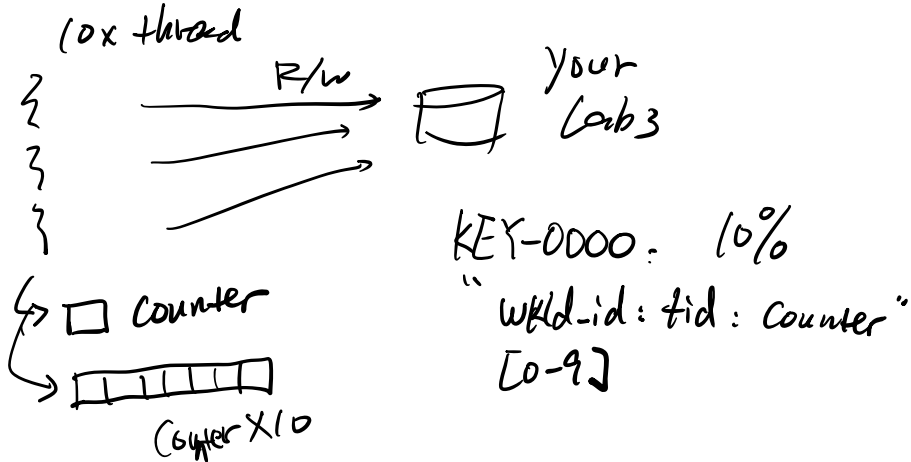
- Concurrency incurs significant performance gap between implementations, even for a "simple" KV-store.
- In concurrency programming, performance and correctness are sometimes in tension. ↗?
- See some implementations balancing performance (top-3 in challenge) and correctness ($\geq 97/100$ in normal tests)

• hash table + array of locks.

• ~~frag~~ + one mutex
trie

- 0. Lab3
 - 1. Last time ←
 - 2. Access control (Unix) ←
-

Lab3.



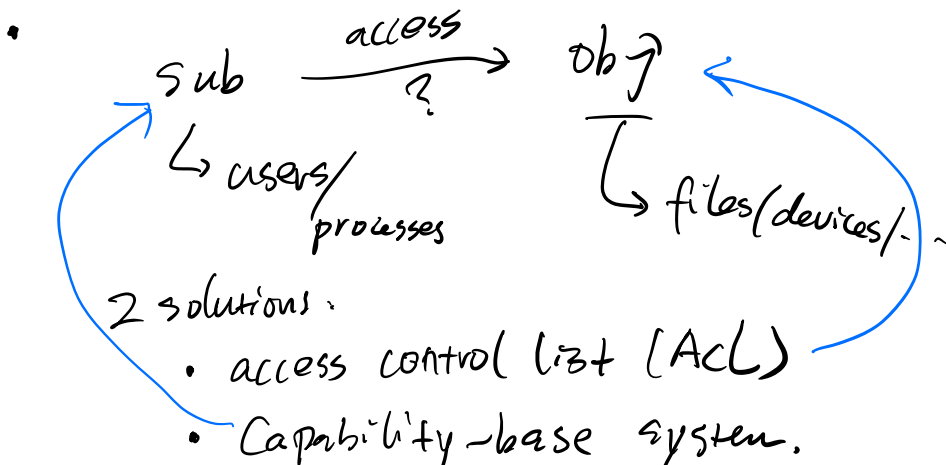
- authentication

- Q:

option 1: 50% losing \$500 (6.)

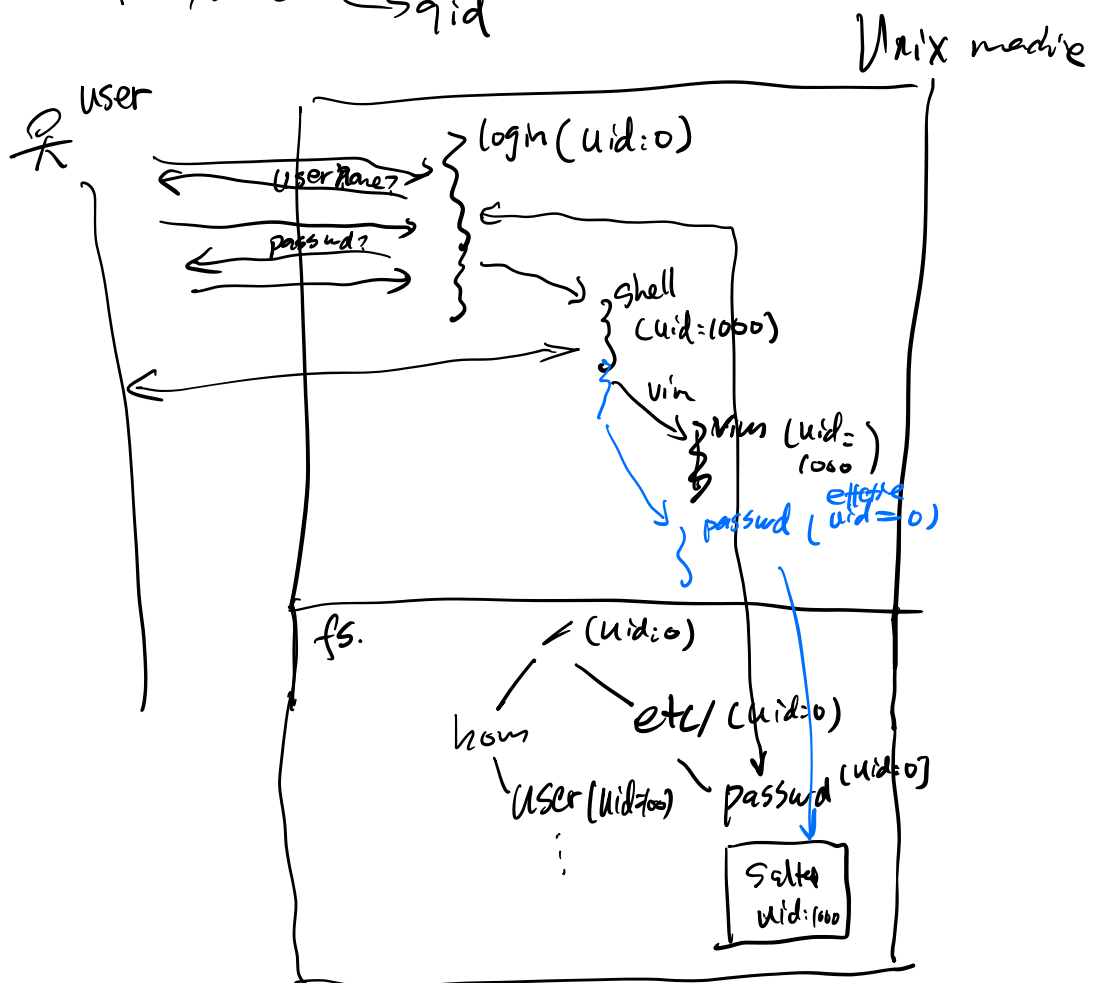
option 2: 0.1% losing all your money (40)

option 2 H/H



• Unix access control.

- UID/GID $\xrightarrow{\text{16bit}}$ uid: 0 root
- process $\begin{cases} \rightarrow \text{uid} \\ \rightarrow \text{gid} \end{cases}$
- files/dirs $\begin{cases} \rightarrow \text{uid} \\ \rightarrow \text{gid} \end{cases}$



Q:

Q: What if a user need to update passwd?

\$Vim /etc/passwd

- setuid

- passwd

(uid=0)

setuid=1

- ! passwd

→ {
 → real uid=1000
 → effective uid=0

sudo

setuid=0

- DANGEROUS

\$ cp /bin/sh /tmp/break-acct

\$ chmod 4755 /tmp/break-acct
 ↳ setuid. ↳ r-x.

\$ /tmp/break-acct (uid=YOUR)
 ↳ shell

passwd

environment

passwd:

⇒

fd = open("/etc/passwd" ...)

ask user for old passwd

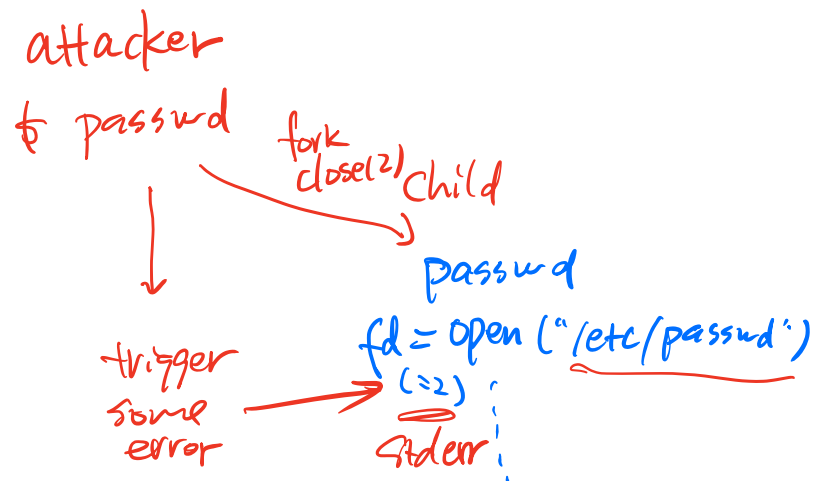
{
 • return the smallest fd
 • 0/1/2

```

    check
    ask for new passwd ⇐
    write (fd, new_passwd)
    close (stdout)
    ...

```

Q: what can go wrong?



• 'preverse' (setuid)

save a copy of some file

system("/bin/mail") \$ /bin/mail

⇒ IFS = ~~"X"~~ ' '"
(internal field separator)

→ \$ bin mail
local file.

• TOCTTOU attacks.

/ setuid program.

```

if (access(logfile, W_OK) < 0)
    return ERROR
fd = open(logfile, ..., O_WRONLY)

```

time-of-check-to-time-of-use

setuid process

attacker

```

if (access(logfile, W_OK) < 0)
    return ERROR

```

Create("/tmp/x")

unlink("/tmp/x")

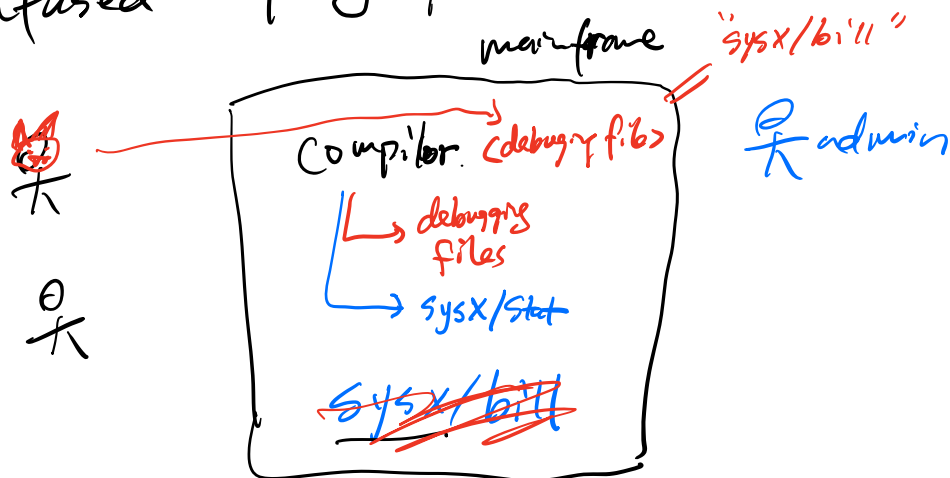
symlink("/tmp/x", "/etc/passwd")

```

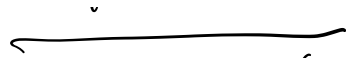
fd = open(logfile, ..., O_WRONLY)

```

- Confused deputy problem.



* Capabilities



↳ Linux

\$ man 7 capabilities