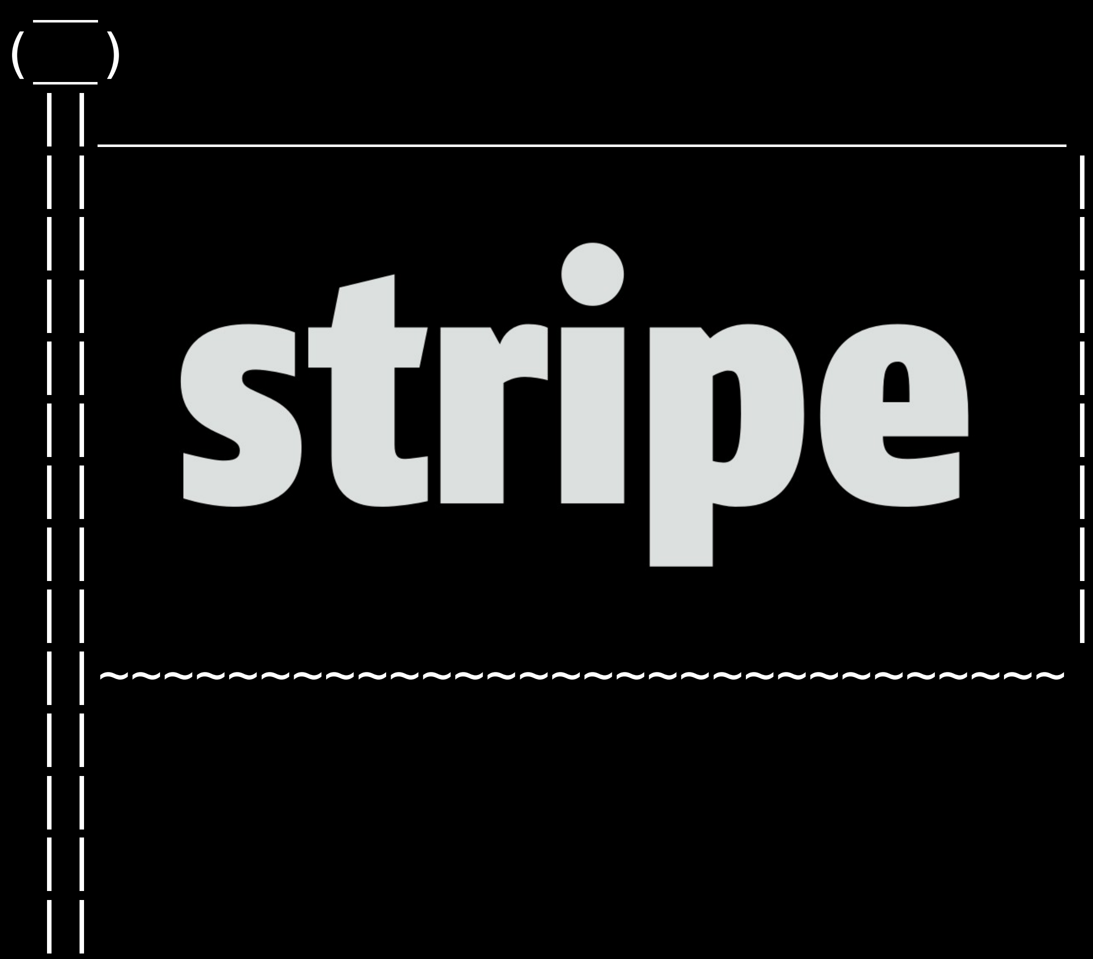
Andy Brody
@alberge

Greg Brockman
@thegdb

Siddarth Chandrasekaran
@sidd



Stripe makes it easy to start accepting credit cards on the web today.

Why a CTF?

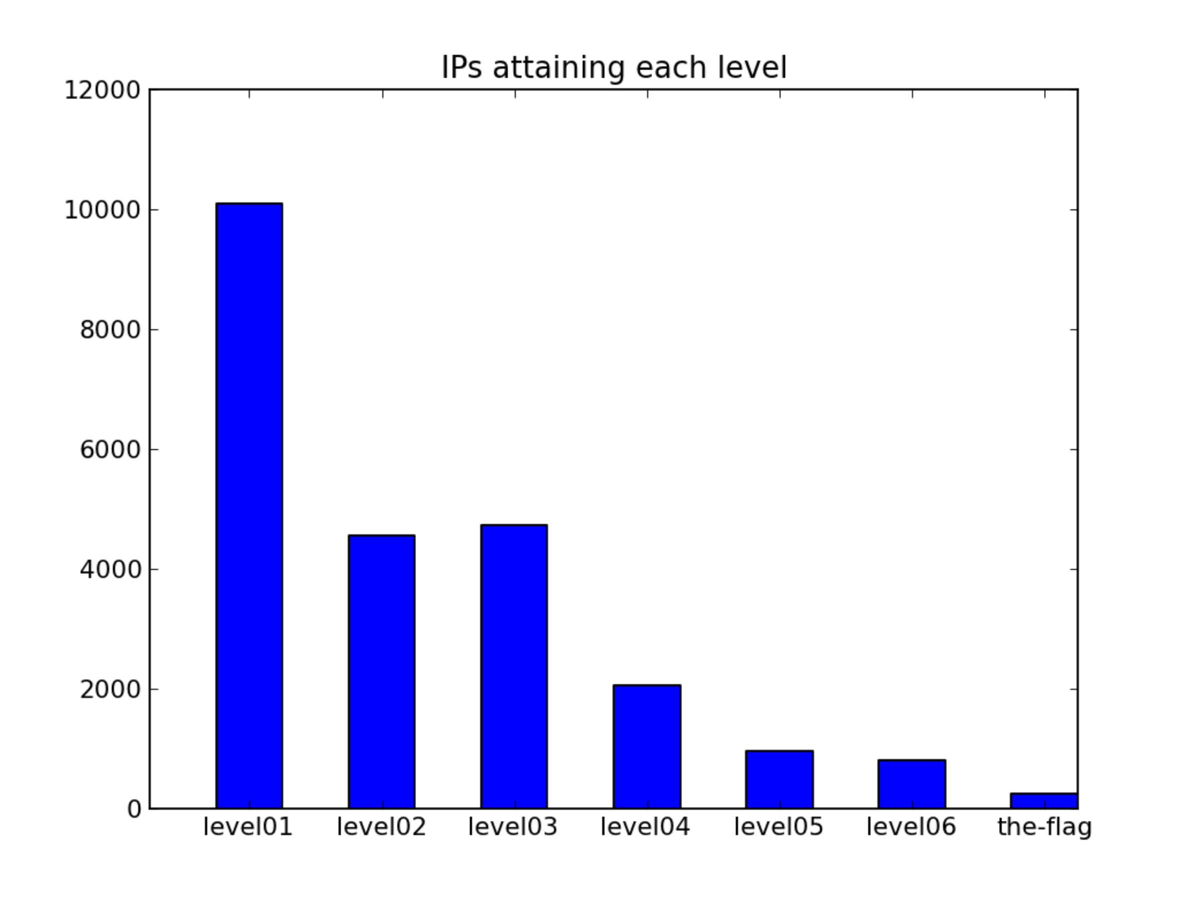
Educational

Challenging

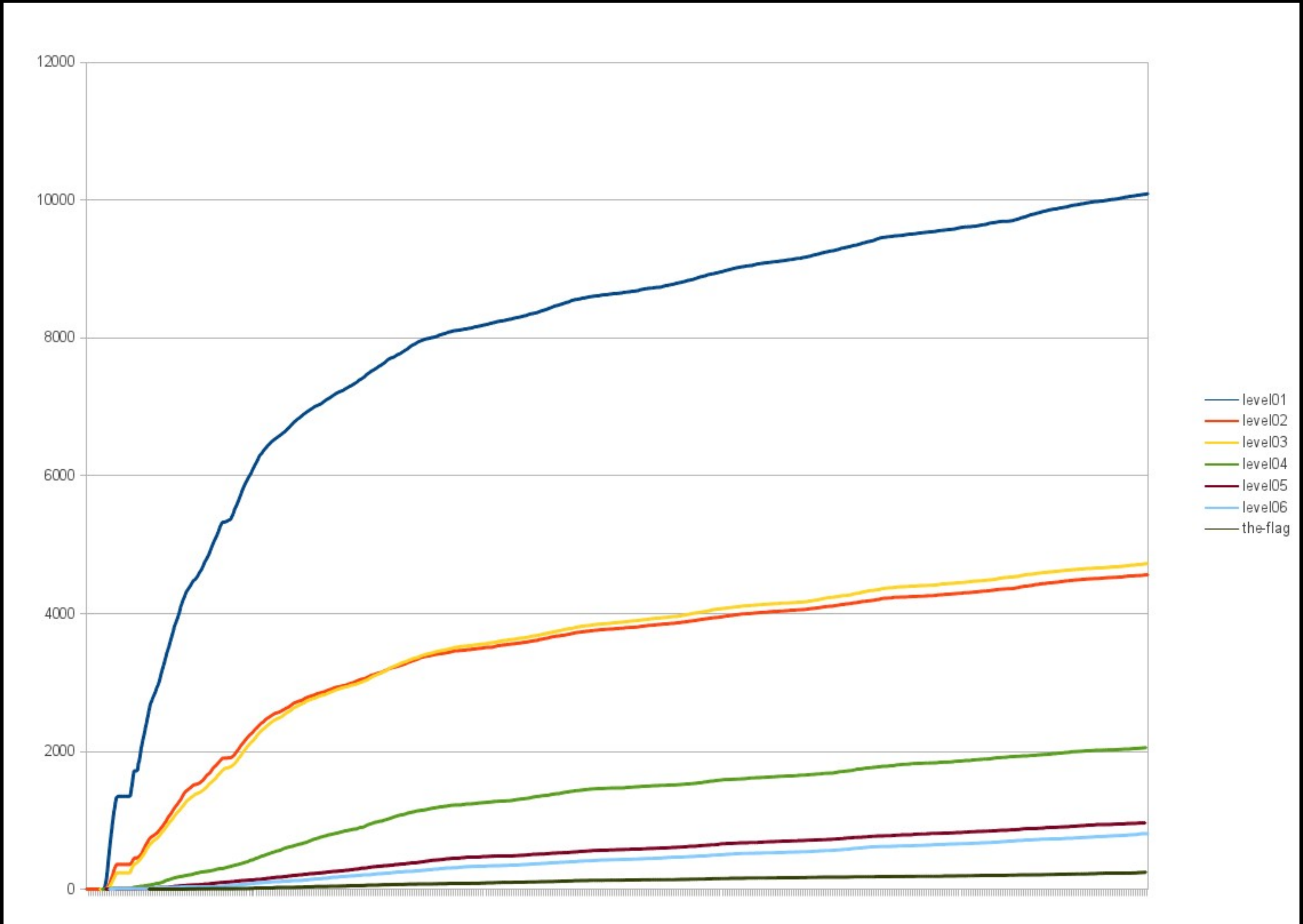
Fun!

Some Numbers

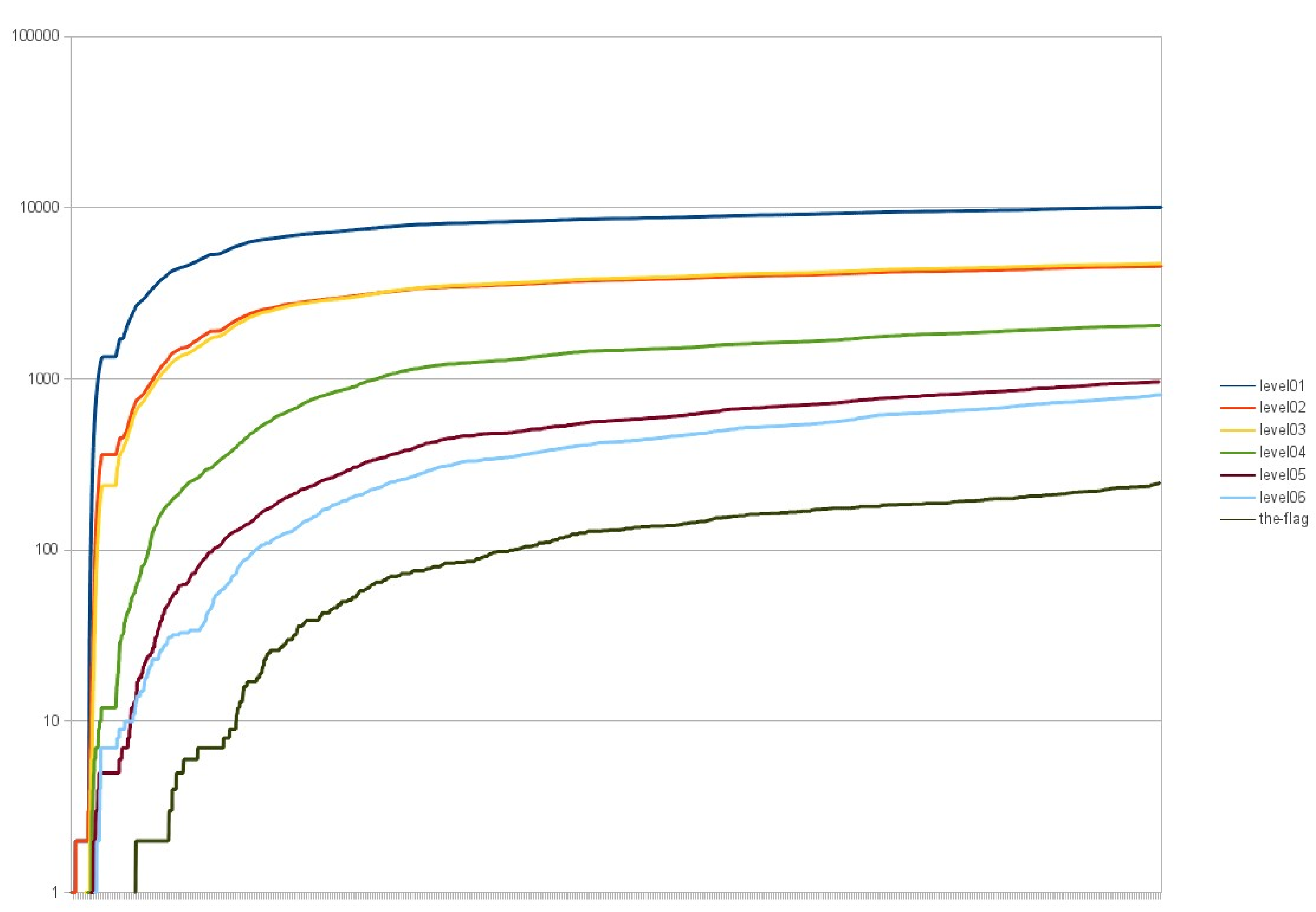
Numbers: IPs at each level



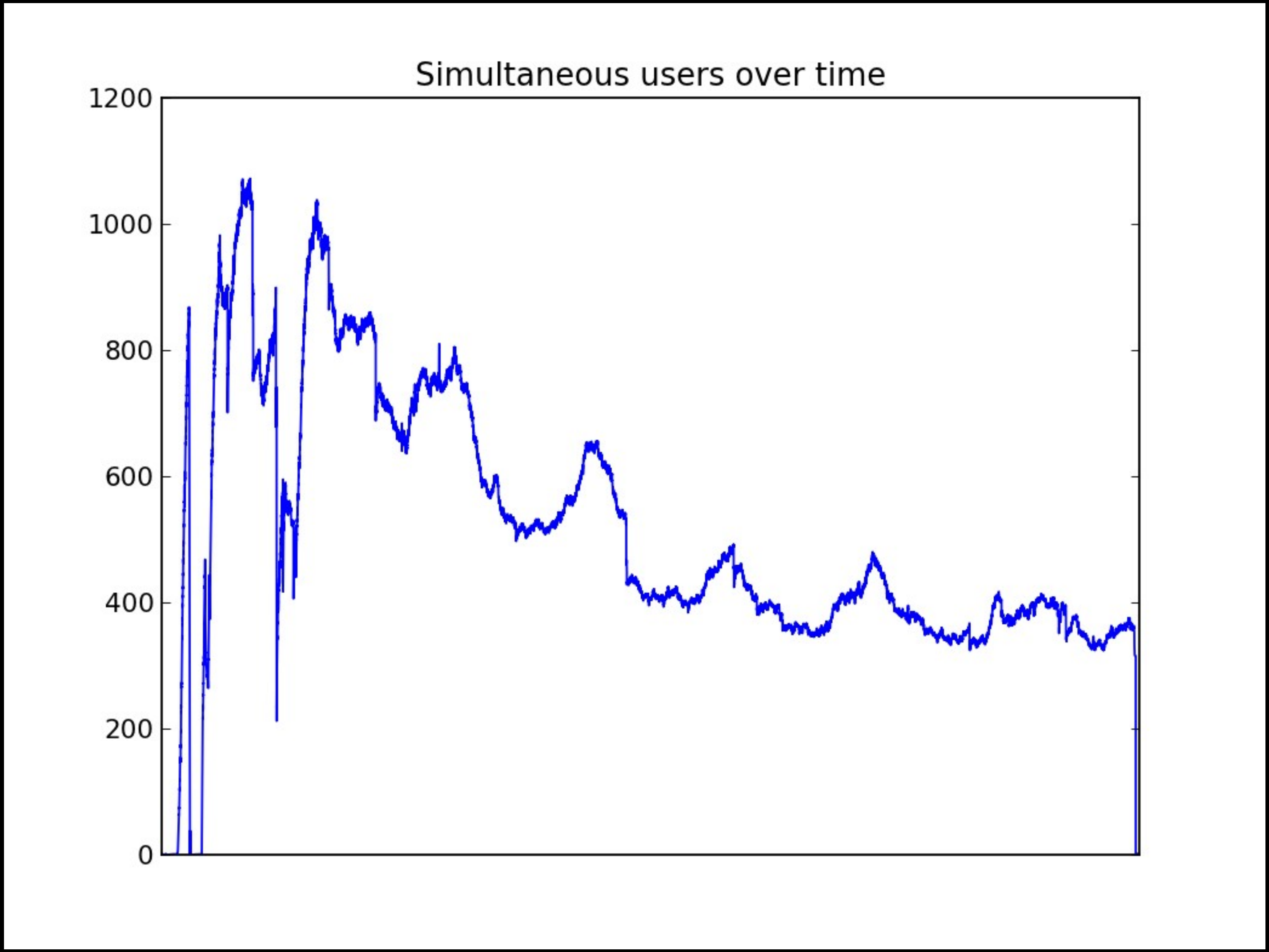
Numbers: cumulative IPs / level



Numbers: cumulative IPs / level



Numbers: concurrent logins

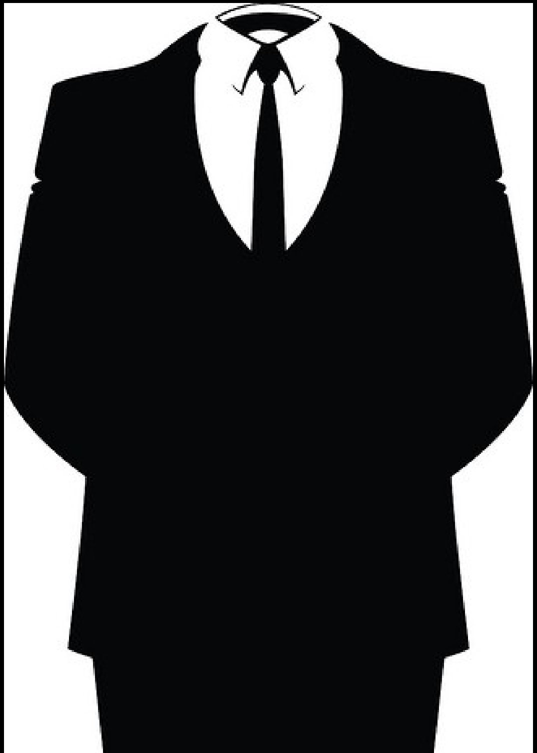


CTF Security

Oh, UNIX has multiuser in its bones — this will be easy.

CTF Security

Support for *anonymous* users isn't great.



CTF Security

Services vulnerable to execution of arbitrary code!

Goal: per-user sandbox

Goal: per-user sandbox

- lightweight spin-up
- locked down environment
- blissful unawareness of other users

Implementation: chroot jail

Implementation: chroot jail

User for each level

Debootstrap full install inside chroot

Separate filesystem for writable data

No /proc, no setuid binaries in /bin
Limited nodes in /dev

Implementation: chroot enforcement

chroot by user group with ssh

chroot with suPHP

Implementation: R/O FS

Great for security — even root can't modify without remounting.

Terrible for maintenance: can't make changes on the fly.

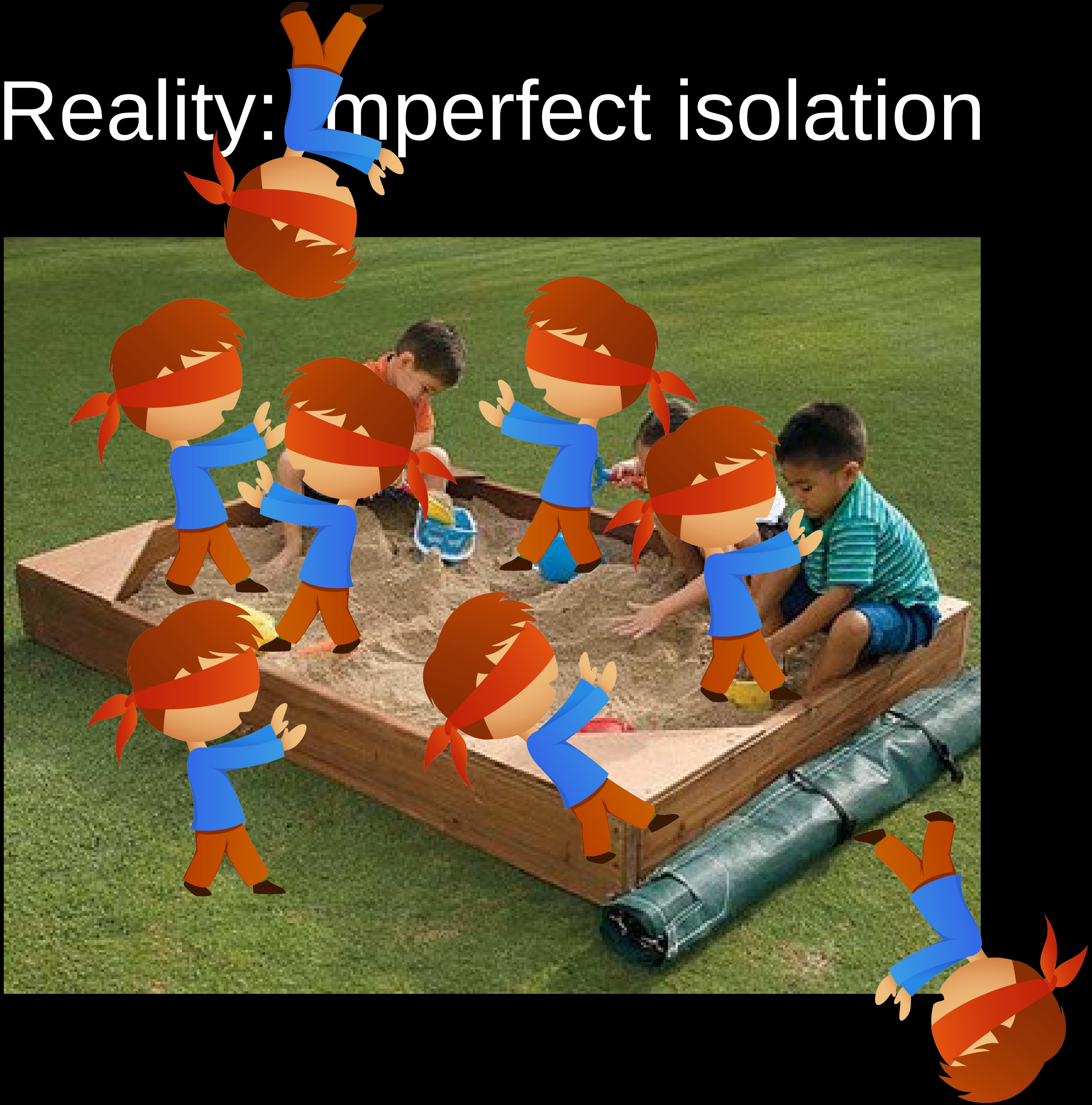
Implementation: R/O FS

Next time:

Mount the filesystem R/W elsewhere.

Bind mount it R/O inside the chroot.

Reality: Imperfect isolation



Isolation: fork bombs

```
perl -e 'fork while fork'
```

Isolation: fork bombs

Causes

- script kiddies
- people trying to brute force level06
- process exhaustion from lots of users

Isolation: fork bombs

Mitigation

- cgroups
- ulimits
- `killall -STOP …; killall -KILL …`
  - by tty
  - by pgid or sid
  - by user + process name
  - send `CONT` to innocent bystanders

Isolation: others

- disk exhaustion
- memory exhaustion
- greedy I/O
- level05 server
    - Didn't want setuid for python
    - Arbitrary code execution
    - Cron job to kill & restart

Next time

make user accounts!

let built-in user isolation do the work

control level access with groups, setgid

Cloud supported

Cloud supported

Completely isolated from the rest of our servers

Outbound traffic open during spin-up, but firewalled off in production

Spin up capacity to handle unexpected load

Questions?