Setuid

Examples

- `passwd` – changes user's password
- `su` – acquire new user ID (given correct password)
- `sudo` – run one command as root
- `ping` (historically) – uses raw IP sockets to send/receive ICMP

Have to be very careful when writing `setuid` code

- Attackers can run `setuid` programs any time (no need to wait for root to run a vulnerable job)
- Attacker controls many aspects of program's environment

➡ You will write such attack in CSCD27

Linux capabilities

Linux subdivides root's privileges into 40 capabilities, e.g.

- `cap_net_admin` – configure network interfaces (IP address, etc.)
- `cap_net_raw` – use raw sockets (bypassing UDP/TCP)
- `cap_sys_boot` – reboot
- `cap_sys_time` – adjust system clock

For instance ping needs raw network access, not ability to delete all files

```
$ ls -al /usr/bin/ping
-rwxr-xr-x 1 root root 61168 Nov 15 23:57 /usr/bin/ping
$ getcap /usr/bin/ping
/usr/bin/ping = cap_net_raw+ep
```

See also: `getcap(8)`, `setcap(8)`,`capsh(1)`