last time (1)

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

- time of check: can user access this thing
- time of use: access thing on behalf of user
- bug: “this thing” could be different each time
  - file moved, symbolic link, etc.

temporarily changing user IDs

capabilities

- can replace access control “on the side”
- processes can only access items they have “token” for
- example idea for token: file descriptor (per process)

last time (2)

system virtual machines:

- application on guest OS on host OS
- virtual machine monitor AKA hypervisor tightly coupled with host OS

virtual machines: trap-and-emulate

- virtual machine monitor: track pretend hardware state for system VM
- example pretend state: is it in kernel mode? are interrupts enabled?
- respond to exceptions by emulating what hardware would do
- might require interpreting machine code
- e.g. accessing device memory → simulate device control registers
- e.g. system call → run guest OS system call handler