System Security Goals

#security_goals

Goals

- need to identify the problem
  - how do we eliminate it?
- paradigm of **penetrate-and-patch**
  - can we do better than this?
- security would be easy if we only had to isolate processes
- we can't isolate processes though because operating systems need process interaction
- challenge - ensure security goals are met given all means of interaction
- a secure operating system should provide security mechanisms that ensure that the system's security goals are enforced by trusted components despite threats from attackers
  - is this realistic?
- security goals have a lot of unsatisfying definitions
  - **safety** - users can perform only authorized operations
  - **least privilege** - processes perform only their necessary operations
  - **multilevel security** - operations can only permit information to be written to more secret levels
- defining practical and effective security goals is a difficult task

Models

- trust model is equivalent to trusted computing base (TCB) for operating systems
  - we want to trust as little as possible
- threat model describes the threats that an attacker can use to violate security goals
  - defines where the threats come from, the operations made possible by the threats, and what the threats threaten
  - secure operating system (TCB) must protect processes against threats
    - is this sufficient?