ECS 235B Module 3 Reference Monitors

Entities

- Subject: active entity
  - Causes information to flow or system state to change
  - Examples: processes, some devices
  - At a higher layer of abstraction: users, other computers
- Object: passive entity
  - Contains or receives information
  - Examples: files, some devices
  - At a higher layer of abstraction: file server, network

Reference Monitor

- *Reference monitor* is access control concept of an abstract machine that mediates all accesses to objects by subjects
- *Reference validation mechanism* (RVM) is an implementation of the reference monitor concept.
  - Tamperproof
  - Complete (always invoked and can never be bypassed)
  - Simple (small enough to be subject to analysis and testing, the completeness of which can be assured)
    - Last engenders trust by providing evidence of correctness
- Note: RVM is almost always called a reference monitor too

Examples

- *Security kernel* combines hardware and software to implement reference monitor
- *Trusted computing base* (*TCB*) consists of all protection mechanisms within a system responsible for enforcing security policy
  - Includes hardware and software
  - Generalizes notion of security kernel

Policy and Reference Monitor

- Reference monitor implements a given policy
  - It has a tamperproof authorization database
  - Also maintains an audit trail (record of security-related events) for review

- More on this later; we need some background first