Reference Monitor Concept

#reference_monitor

Reference Monitor

- **purpose** - ensures enforcement of security goals
  - *mandatory protection state* defines goals
  - reference monitor ensures *enforcement*
- every components that you **depend** on to enforce your security goals must be enforced by a **reference monitor**
- **components**
  - reference monitor interfaces
    - e.g. Linux Security Modules
  - authorization module
    - e.g. SELinux
  - policy store
    - e.g. policy binary

Guarantees

- ***complete mediation, tamperproof, and verifiable***
- **complete mediation** - reference validation mechanism must always be invoked
  - every security-sensitive operation must be *mediated*
    - *security-sensitive operation* - an operation that enables a subject of one label to access an object that may be a different label
  - **validating**
    - every security-sensitive operation must be identified
    - then check for *dominance* of mediation
  - **main questions**
    - does interface mediate correctly?
    - on all resources?
    - verifiably?
- **tamperproof** - reference validation mechanism must be secure against modification
  - prevent modification by untrusted entities
    - interface, mechanism, and policy of a reference monitor
    - code and policy that can affect reference monitor

    - detecting
        - *transitive closure* of operations
        - often some untrusted operations are present, posing a challenge
    - **main questions**
        - is reference monitor protected?
        - is system TCB protected?
- **verifiable** - reference validation mechanism must be subject to analysis and tests, the completeness of which must be assured
    - test and analyze
        - reference validation mechanism
        - tamperproof dependencies
        - security goals the system enforces
    - determining the correctness of the code and policy
        - how do we define correctness for each?
    - **main questions**
        - is TCB code base correct?
        - does the protection system enforce the system's security goals

Evaluation

- evaluation based on the **main questions**
    - mediation - does interface mediate correctly?
    - mediation - on all resources?
    - mediation - verifiably?
    - tamperproof - is reference monitor protected?
    - tamperproof - is system TCB protected?
    - verifiable - is TCB code base correct?
    - verifiable - does the protection system enforce the system's security goals?

Multiple Reference Monitors

- original reference monitor concept approached designed with a centralized reference validation mechanism n mind
- what happens if we have several of these mechanisms grouped together?
    - how to reason their composability?