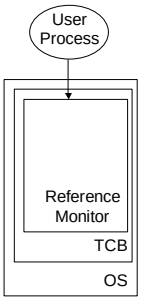
Security Models

Emin Gun Sirer

Trusted Computing Base

- The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security
- Typically, all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges
- Desirable properties:
  - Small
  - Separable, well-defined
  - Independently-auditable

Reference Monitor



- A reference monitor is a separable module that enforces access control decisions
- All sensitive operations are routed through the reference monitor
- The monitor then decides if the operation should proceed
- Most commercial OSes do not have a reference monitor

Access Control

- Discretionary Access Control
  - Individual users may determine the access controls
  - E.g. unix file system implements DAC
  - This model works well in commercial and academic environments, not so well in the military, hospitals, private web sites, etc.
- Mandatory Access Control
  - A site-wide security policy is enforced by the system in addition to the discretionary access controls
  - Better suited to environments with rigid information access restrictions

Sample Covert Channel

- The spymaster sits in a loop monitoring its own progress, e.g. how high can it count within a given amount of time
- The mole either computes ferociously or sits idle for a certain period
- The spymaster can divine mole's behavior based on his own progress
  - Information leaked through system behavior
- There are many other covert channels
  - Steganography, hidden messages in innocuous messages, e.g. in low-order bits of images

Multilevel Security

- "Multilevel" security refers to environments where users form a hierarchy
  - Hierarchy may be linear, as in the military
  - E.g. "unclassified," "confidential," "secret," and "top secret."
  - Or it could possibly be a lattice, as with roles
  - E.g. presidential security advisor
- Multilevel security models are designed to restrict information flow in environments where users at multiple levels interact
  - Military sites, hospitals, web sites, etc.

Bell-La Padula Model

- Security property: A user at security level k can read only objects at level j, where j <= k
  - General can read lieutenant's documents
  - But not the other way around
- The * property: A user at level k can write only objects at level j, where j >= k
  - A lieutenant can send a message to a general
  - But not the other way around
- Can read down and write up
- Counterintuitive, but makes sense – information cannot leak from a higher level to a lower level
- Bell-La Padula was designed to keep secrets, not to protect data integrity
  - Lieutenant can overwrite general's files

Biba Model

- Integrity property: A user at security level k can write only objects at level j, j <= k
- The integrity * property: A user at level k can read only objects at level j, j >= k
- No write up, no read down
- Want Bell-La Padula and Biba in the same system, for different types of objects
  - But Bell-La Padula and Biba are in direct conflict
- In practice, a mix of discretionary and mandatory access controls are used

Covert Channels

- Confinement problem: Would like to confine secret information to users with an appropriate clearance
  - Possible to use a reference monitor on overt accesses between processes
- A reference monitor is necessary but not enough
  - Consider a system with a high-clearance mole who would like to sell information to a low-clearance process
  - A reference monitor can prohibit direct calls
  - But the mole can leak information without a direct access

Orange Book

- DOD published a document to classify the security of operating systems
  - Introduced some terminology: Levels A through D
  - Classification technique to determine which OS goes where
- Level D: no requirements, catch all category
  - MSDOS, Windows 95/98/Me
- Level C: cooperating users
  - C1: protected mode OS, user authentication, discretionary access control, testing, documentation
  - C2: discretionary access control down to users, objects initialized to zeros, auditing. UFS access perms fail C2, need ACLs

Orange Book Levels

- Levels B & A: all users and objects carry a security label, system enforces Bell-LaPadula
  - B2: system designed top-down in a modular way, verifiable, covert channel analysis
  - B3: ACLs with users and groups, formal TCB, auditing, secure crash recovery
  - A1: formal model of protection, proof of correctness for model, demo that implementation follows model
- High ratings hard to attain
  - Some Unix and NT variants have C2 ratings
  - Custom OSes for the military have higher ratings

Orange Book Retrospective

- Good aspects:
  - Reasonable model
  - Underscores the importance of software engineering in constructing secure systems, eg. testing, modularity, auditing
- Has it worked ? No.
  - Cuts off secure OSes from mainline, commercial Oses
  - No economies of scale
- Result:
  - Aegis cruiser Yorktown running Windows NT towed to port when redundant, ruggedized computers divide by zero
  - CIA director goes home with classified data and connects to AOL