Security Architecture and Design

Mike Smith

26/04/10 - Rev.28

Common Criteria

- Uses an Evaluation Assurance Level - EAL
- EAL1 - Functionally Tested
- EAL2 - Structurally Tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 - Semi-formally designed and tested
- EAL6 - Semi-formally verified design and tested
- EAL7 - Formally verified design and tested

ITSEC

- Evaluates on Functionality and Assurance
- Functionality rating F1 - F10
- Assurance rating E0 - E6

TCSEC Orange Book

- Trusted Computer Systems Evaluation Criteria - TCSEC
- A - Verified Protection
  - A1 - Verified Design
- B - Mandatory Protection
  - B1 - Labeled Security - Objects are classified
  - B2 - Structured Protection
  - B3 - Secure Domains
- C - Discretionary Protection
  - C1 - Discretionary Security
  - C2 - Controlled Access - reasonable commercial apps
- D - Minimal Security
  - Evaluated but fail

Issues

- Covert channels
- Race conditions
- Emanations
- Maintenance hooks
- Countermeasures
  - Reveal as little as possible
  - Limit access - need to know
  - Disable unused services and accounts
  - Use strong authentication

Terms

- Trusted Computer Base - TCB - the total combination of protection mechanisms within a computer system, including hardware, firmware and software to enforce security policy.
- Access Control - ability to permit or deny the use of an object by a subject
- Reference Monitor - system component that enforces access controls on an object
- Security Kernel - hardware, firmware and software that implement the reference monitor concept
  - Mediate all accesses
  - Be protected from modification
  - Be verified as correct

CPU Components

- Arithmetic Logic Unit - ALU - Performs computation
- Bus Interface Unit - BIU - I/O to CPU
- Control Unit - Coordinates other CPU components
- Floating Point Unit - FPU
- Memory Management Unit - MMU
- Pre-Fetch Unit
- Protection Test Unit

CPU States

- Operating (or Run)
- Problem (or Application)
- Supervisory - Privileged Instruction
- Wait

OS Terms

- Multiprogramming - can load more than one program in memory at one time
- Multitasking - can handle requests from several different processes loaded into memory at the same time
- Multithreading - can run multiple threads simultaneously
- Multiprocessing - has more than one CPU

Access Control Models

- Bell-LaPadula
  - 1973 - First formal confidentiality model
  - State-machine model
  - Simple security property - no read up
  - * property - no write down
  - Strong star property - subject's = object's clearance for RW
  - Discretionary property and trusted subject
- Biba
  - 1977 - First integrity lattice based model
  - Simple integrity property - no read down
  - * integrity property - no write up
- Clarke-Wilson
  - 1987 - commercial, e.g. banking
  - Unconstrained Data Item - UDI
  - Constrained Data Item - CDI
  - Integrity Verification Procedures - IVPs
  - Transformation Procedures - TPs
- Access Matrix
  - Object access rights to subjects
- Take Grant
  - Rights a subject can transfer to/from another subject or object
  - create, revoke, take, grant
- Information Flow Model
- Noninterference Model
- Brewer and Nash Model - dynamically changing access controls
- Graham-Denning Model - How subjects and objects should be created and deleted - access rights
- Confidentiality - Bell-LaPadula, Access Matrix and Take-Grant
- Integrity - Biba and Clarke-Wilson
- Three goals of integrity
  1. Prevent unauthorized modifications
  2. Prevent authorized users from improper modifications
  3. Maintain internal and external consistency - well-formed transaction