Security Architecture

Covert Channel
- A way to receive information in an unauthorise way
  - Storage Covert Channel — process communication via storage space on the system
  - Covered Timing Channel — On process relay on another

Models
- **Matrix** — ACL used in DAC
- **BELL LAPADULLA** — Confidently Model
  - Developed by DOD
  - Simple e user can not read up
  - * Preterite Can not write down
  - Strong Star : Should remain in the same level
- **BIBA** — Integrity Model
  - Simple e user can not read down
  - * integrity User can not write up
  - Lattice Model
- **CLARK WILSON** — Integrity Model
  - Cannot be tampered, logged and Consistency
  - Enforce Separation of Duties
  - Require Auditing
  - Commercial use
  - Access to Object only Trough Program
- **BREWER and NASH**
  - AKA Shiness Wall
  - Prevent Conflict of Interest
  - Dynamic Access Control based on the user previous action
  - Subtopic 4

Evaluation Criteria
TCSEC
- **D** — Minimum Security
- **C1** — DAC
- **C2** — C1+ Control Access, Object Reuse, Audit Trail
- **B1** — MAC, BLP, Process Isolation
- **B2** — B1+ Trusted path,covert Channel analysis , management
- **B3** — B2+ Trusted recovery, Monitor
- **A1** — verified design
- **A** — Verified Protection
ITSEC
- Evaluate Functionally and Assurance Together
- Evaluate Functionality and Assurance Spirality
- Assurance E0 to E6 highest
- Functionality F1 to F10 highest
Common Criteria ISO 15408
- Define a Protection Profile that include security requirement and the protection of the product that need to be evaluated
- **EAL0** — Inadequate Assurance
- **EAL1** — Functional Tested
- **EAL2** — Structural Tested
- **EAL3** — Methodically Tested and Checked
- **EAL4** — Methodically designed, Tested and reviwed
- **EAL5** — Semi formally Designed and Tested
- **EAL6** — Semi Formally verified Designed, and Tested
- **EAL7** — Formal Designed and Tested
- **TOE** — Target of Evaluation
- **Protection Profile PP** — Security Requirement for a class of security devices
- **Security Target** — Identify the security Properties of the TOE
- **Security Function Requirment** — Specify different security function

Certification
- Evaluation of Security features and Safeguards
- **DTSCAP**
  - US Goverment and Defense
  - Phase 1 Defination
  - Phase 2 Verification
  - Phase 3 Validation
  - Phase 4 Aggradation
- **NIACAP** — National Security Certificates

Aggradation
- The formal acceptance outcome of the society by management

Frameworks
- ISO
- Zackman
- ITIL
- Cobit

Assurance
- Degree of Confidence in satisfaction of security requirement

Recovery Procedure
- **Fault tolerant** — Continue to function despite failure
- **Fail Safe System** — Progorm execution is terminated and secure from beeing compromissed
- **Fail Soft or Resilient System** — Selected non cortical process is terminated

MAC Security Modes
- **Dedicated security mode**
  - All user in the same level
  - All user can access all data
  - Need to know for all user
- **System High Security**
  - Need to know
  - USe the Information Label
- **Compartment security**
  - Need to Know
  - Approval
  - Information label
- **Multilevel Security**
  - Need to know
  - Approval
  - Clearance
  - Information label

Protection Rings
- Ring 0
- Ring 1
- Ring 2
- Ring 3

Protection Mechanism
- **Protection Domain** — Memory location to each sperate process
- **Trusted Computer base (TCB)** — Protection System that include HW/ SW/ FW that allow security policy to be implemented
  - **Security Kernel** — Hardware, Software , Firmware of the TCB that implement the reference monitor
    - **Reference Monitor** — Monitor the Isolation