SENG 460

Practice of Information Security and Privacy

Security Architecture and Design

Overview

- System Architecture
- Computer System Architectures
- Why Security at Architecture & Design Phase
- Security Policy
- Information Security Models
- Security Evaluation
- Security Certification and Accreditation

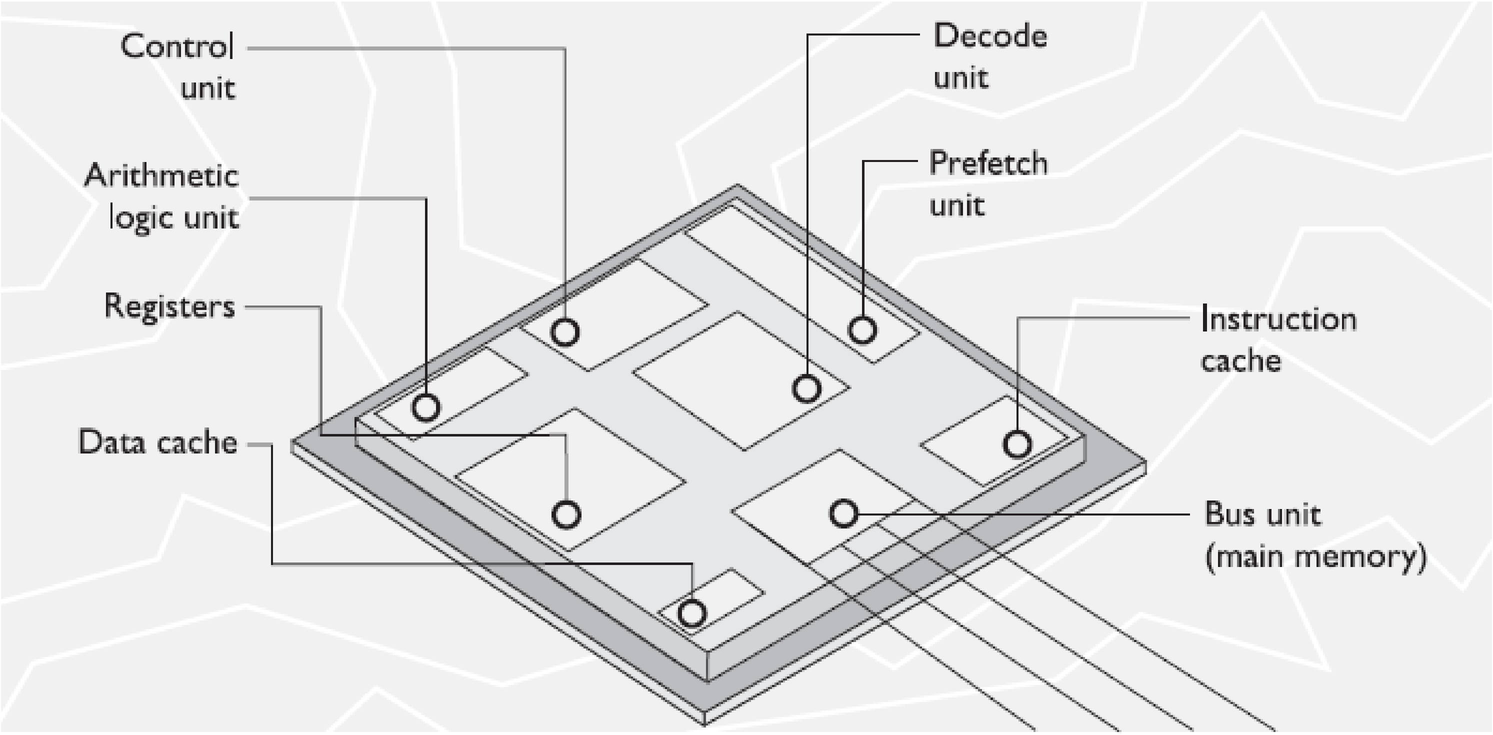
System Architecture

Architecture is the fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.

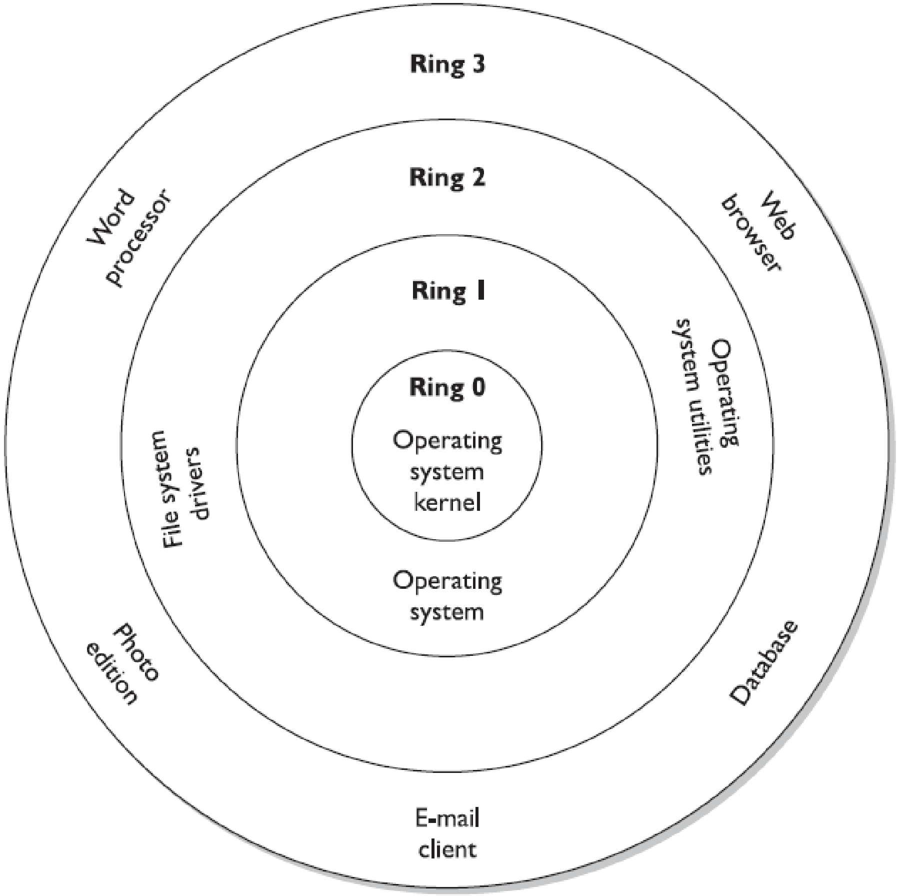
- **Architectural description (AD**): Collection of document types to convey an architecture in a formal manner.
- **Stakeholder** : Individuals, teams, and departments, including groups outside the organization with interests or concerns relative to, a system.
- **View** : The representation of the system from the perspective of a stakeholder or a set of stakeholders.
- **Viewpoint:** A template used to develop individual views that establish the audience, techniques, and assumptions made.

Architecture focuses on "what you need to have", while Design focuses on "how you do it".

Computer System Architectures
- CPU Architecture (Structure View)

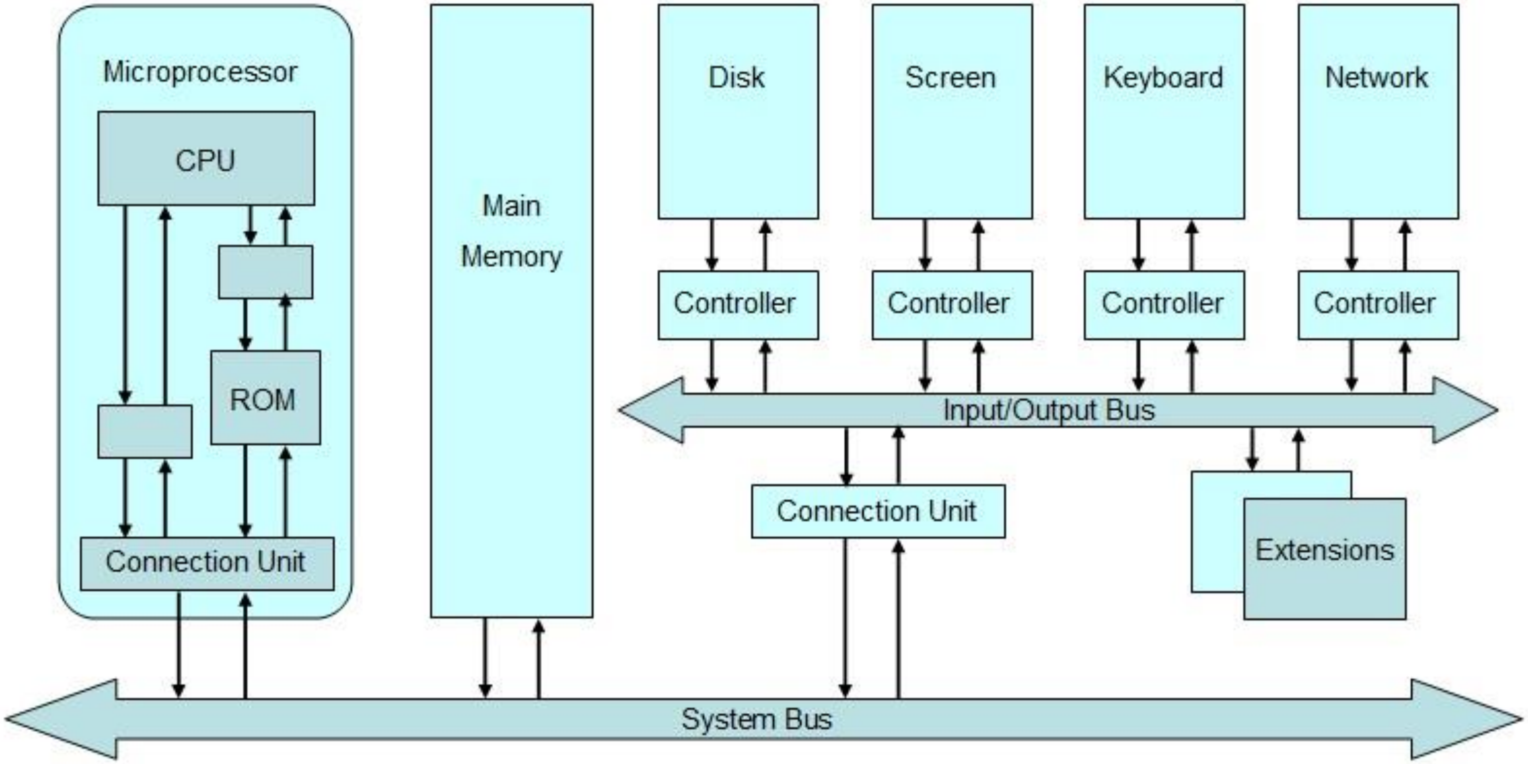


Computer System Architectures
- CPU Architecture (Security View)

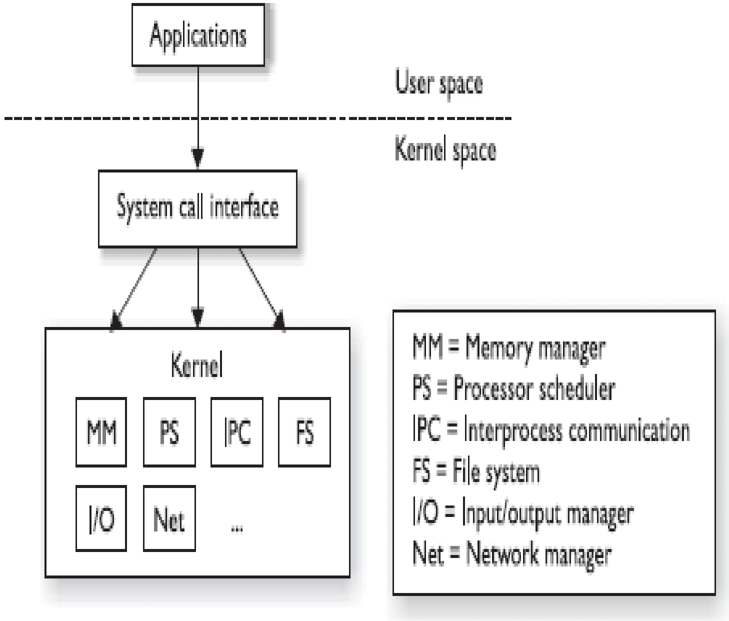


The actual ring numbers available in a CPU architecture are dictated by the CPU itself. Some processors provide four rings and some provide eight or more. The operating systems do not have to use each available ring in the architecture; for example, Windows commonly uses only rings 0 and 3 and does not use ring 1 or 2. The vendor of the CPU determines the number of available rings, and the vendor of the operating system determines how it will use these rings.

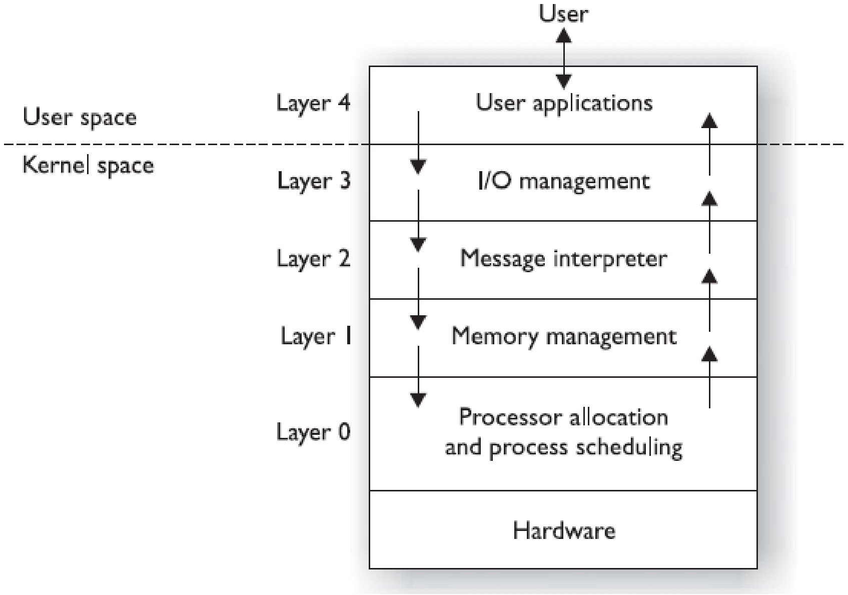
Computer System Architectures
- Computer Architecture



Computer System Architectures
- Operating System Architectures

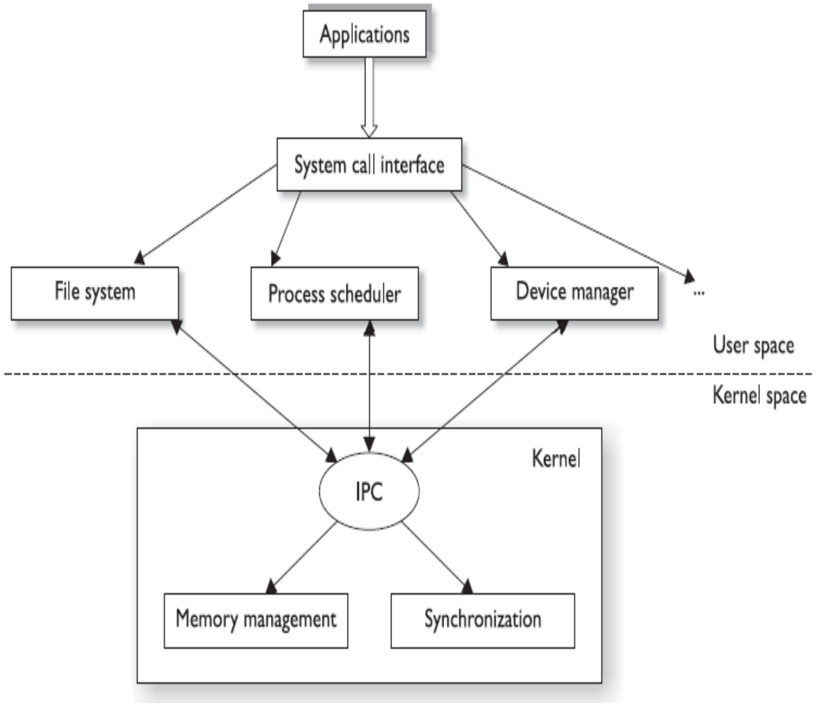


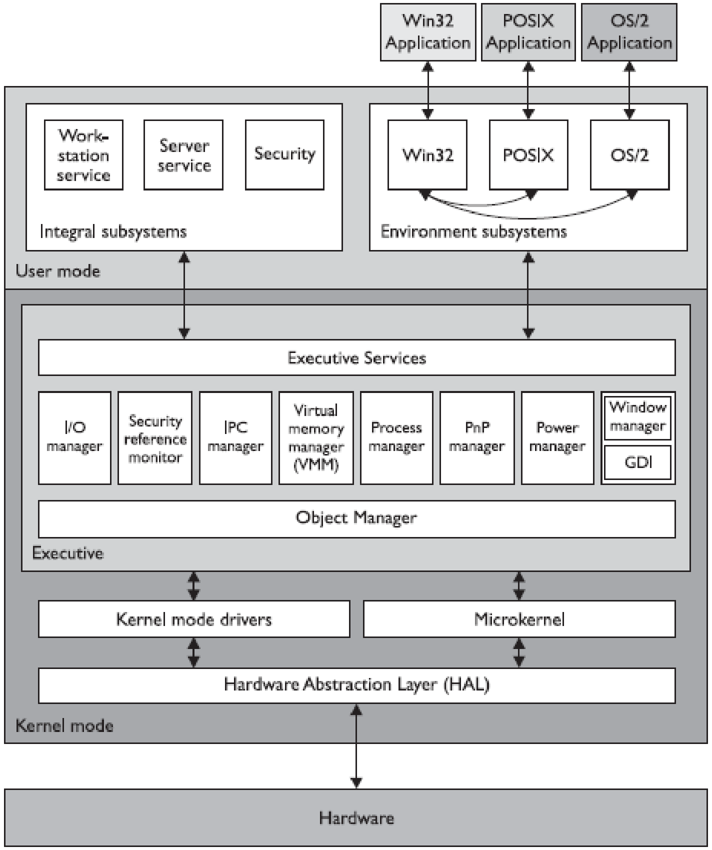
Monolithic Architecture: All system processes run in kernel mode.



Layered Architecture: All system processes run in a hierarchical model in kernel mode.

Computer System Architectures
- Operating System Architectures

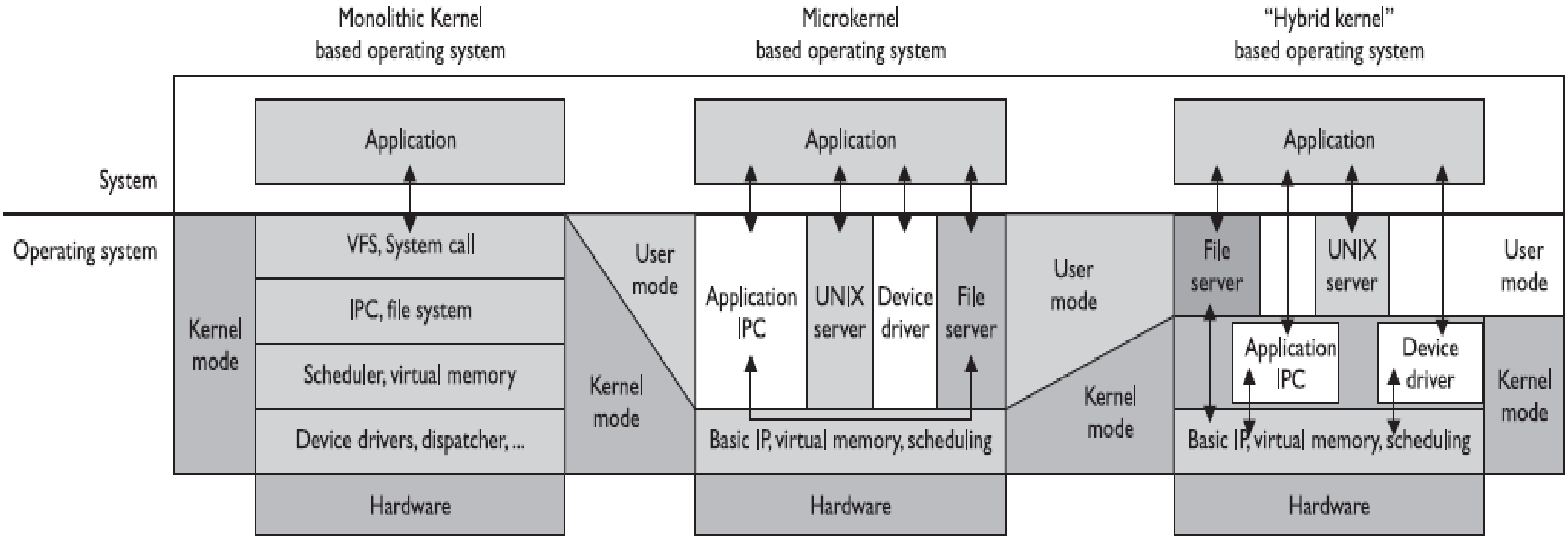




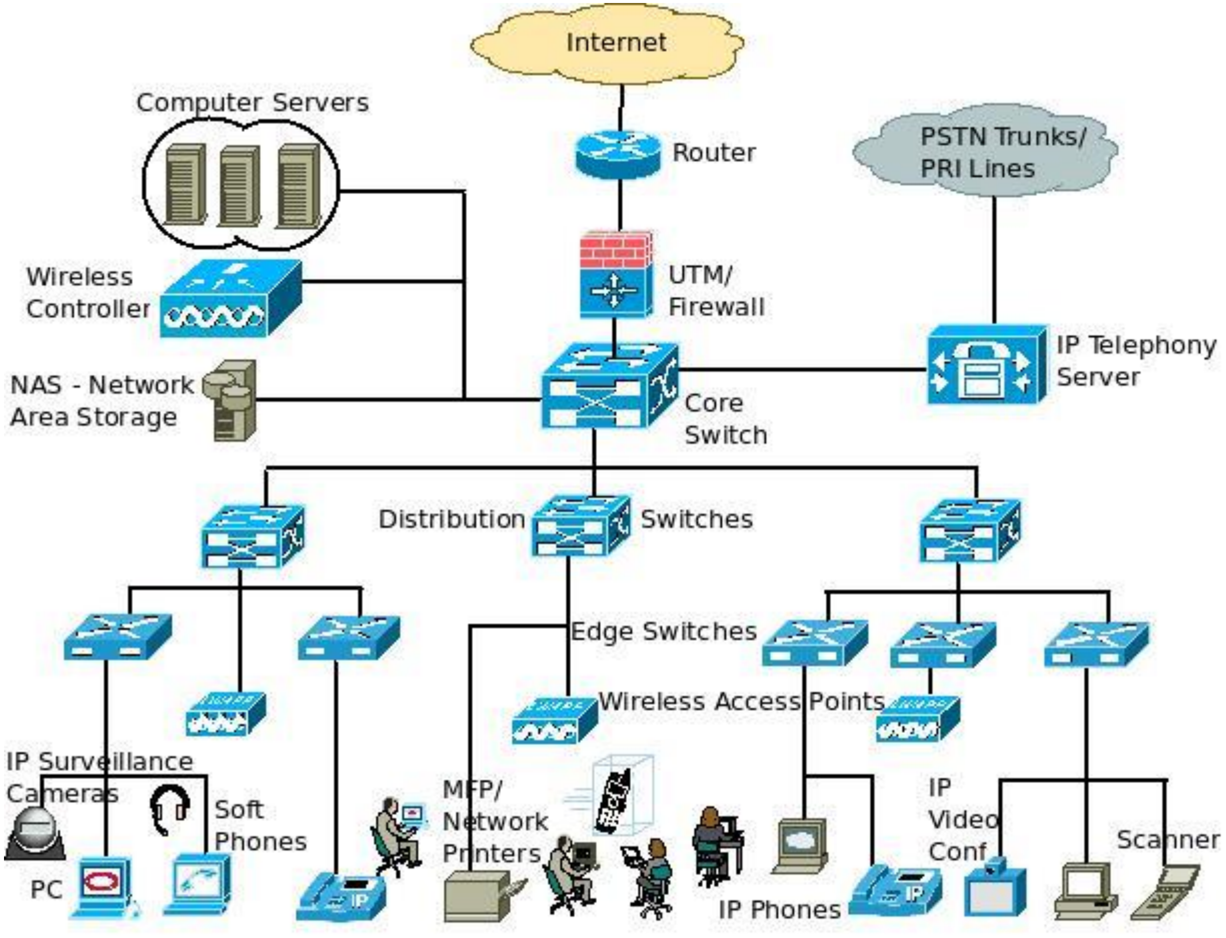
Microkernel Architecture: Core operating system processes run in kernel mode and the remaining ones run in user mode.

Hybrid Microkernel Architecture: All operating system processes run in kernel mode. Core processes run within a microkernel and others run in a client\server model.

Computer System Architectures
- Operating System Architectures (Comparison)



Computer System Architectures
- Network Architecture



Why Security at Architecture & Design Phase

The “patch-in” approach (which deals with security problems in later stages of system development lifecycle) has been proven to be ineffective, costly, and unreliable.

- Patches may introduce new vulnerabilities into the system
- Fixing security bugs is usually more expensive
- Architecture or design security vulnerabilities can be fixed easily at later software development stages.

Security goals have to be defined before the architecture of a system is created, and specific security views of the system need to be created to help guide the design and development phases.

Security Policy

A **security policy** represents the objectives and goals a system must meet and accomplish to be deemed secure and acceptable.

- A security policy expresses exactly what the security level should be by setting the goals of what the security mechanisms are supposed to accomplish.
- The security policy is a foundation for the specifications of a system and provides the baseline for evaluating a system after it is built.

Examples of Security Policy Statements

- *Discretionary access control–based operating system*
- *Provides role-based access control functionality*
- *Capability of protecting data classified at “public” and “confidential” levels*
- *Does not allow unauthorized access to sensitive data or critical system functions*
- *Enforces least privilege and separation of duties*
- *Provides auditing capabilities*
- *Implements trusted paths and trusted shells for sensitive processing activities*
- *Enforces identification, authentication, and authorization of trusted subjects*
- *Implements a capability-based authentication methodology*
- *Does not contain covert channels*
- *Enforces integrity rules on critical files*

Information Security Policy Templates: http://www.sans.org/security-resources/policies/

Information Security Models

An **information security model** maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications (system design).

- **State Machine Models**
- **Bell-LaPadula Model**
- **Biba Model**
- **Clark-Wilson Model**
- **Noninterference Model**
- ***Chinese Wall Model***

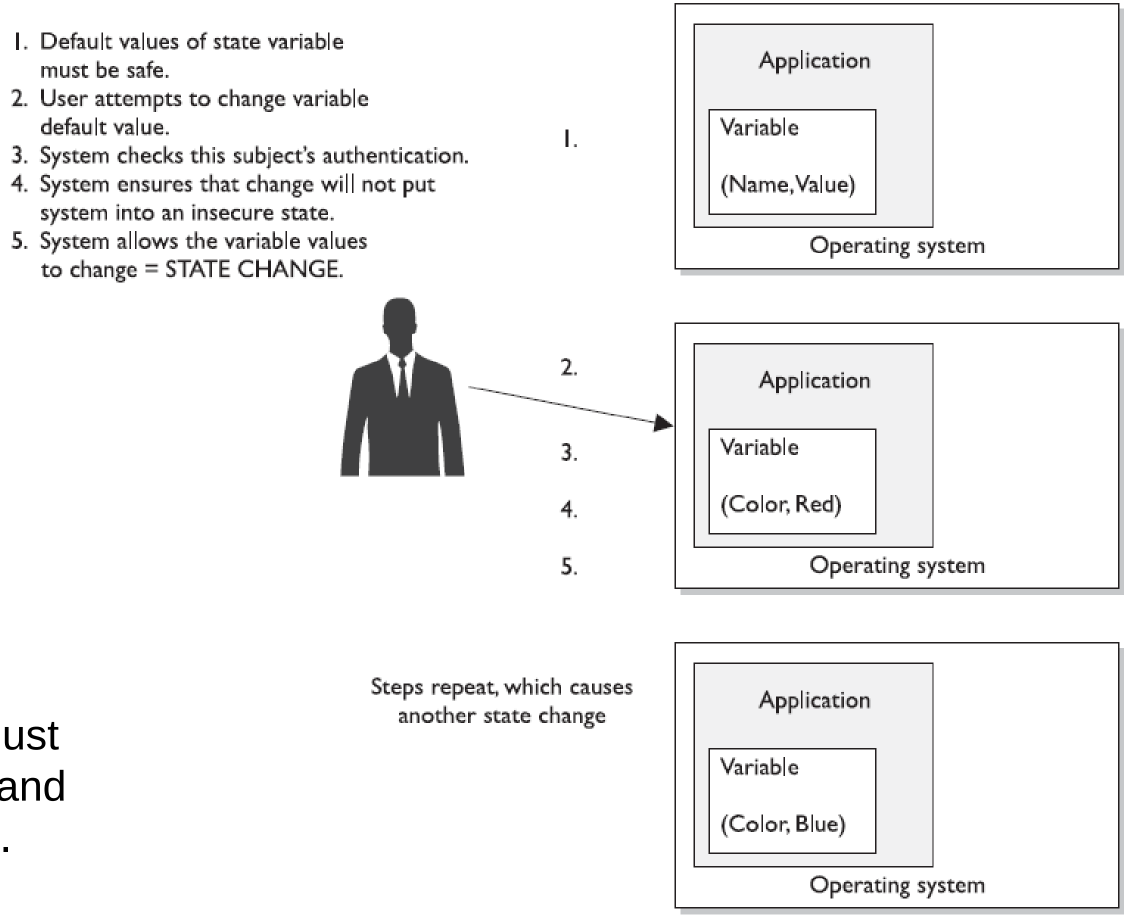
Security Policy vs. Security Model

The security policy provides the abstract goals, and the security model provides the do's and don'ts necessary to fulfill these goals. Security Model is the design of security policy.

Information Security Models

- State Machine Model

In state machine models, to verify the security of a system, the state is used, which means that all current permissions and all current instances of subjects accessing objects must be captured.



1. Default values of state variable must be safe.
2. User attempts to change variable default value.
3. System checks this subject's authentication.
4. System ensures that change will not put system into an insecure state.
5. System allows the variable values to change = STATE CHANGE.

Steps repeat, which causes another state change

Security Policy: The system must stay in a secure state in each and every instance of its existence.

Information Security Models

- Bell-LaPadula Model

In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns.

This model requires both subjects and objects in the system assigned with classification levels. It incorporates three basic rules with respect to the flow of information in a system:

- *The **simple security rule:** A subject cannot read data located at a higher security level than that possessed by the subject (also called no read up).*
- *The ***- property rule:** A subject cannot write to a lower level than that possessed by the subject (also called no write down or the confinement rule).*
- *The **strong star property rule:** A subject can perform both read and write functions only at the same level possessed by the subject .*

Security Policy: Secret information must be prevented from being leaked to unauthorized parties.

Limitations:

- Only addresses confidentiality
- covert channels leakage is possible

Information Security Models

- Biba Model

The Biba model was developed after the Bell-LaPadula model, but focuses on **information integrity**.

*This model requires both subjects and objects in the system assigned with **integrity** levels, and has three main rules to provide integrity protection:*

- **** integrity axiom:** A subject cannot write to a higher integrity level than that to which he has access (no write up).*
- ***Simple integrity axiom**: A subject cannot read to a lower integrity level than that to which he has access (no read down).*
- ***Invocation property**: A subject cannot invoke (request service) of higher integrity.*

Security Policy: no one can mess up the data.

Information Security Models

- Goals of Integrity Models

- Prevent unauthorized users from making modifications.
- Prevent authorized users from making improper modifications.
- Maintaining internal and external consistency of data and programs. (it must always do what the users or owners expect it to do.)

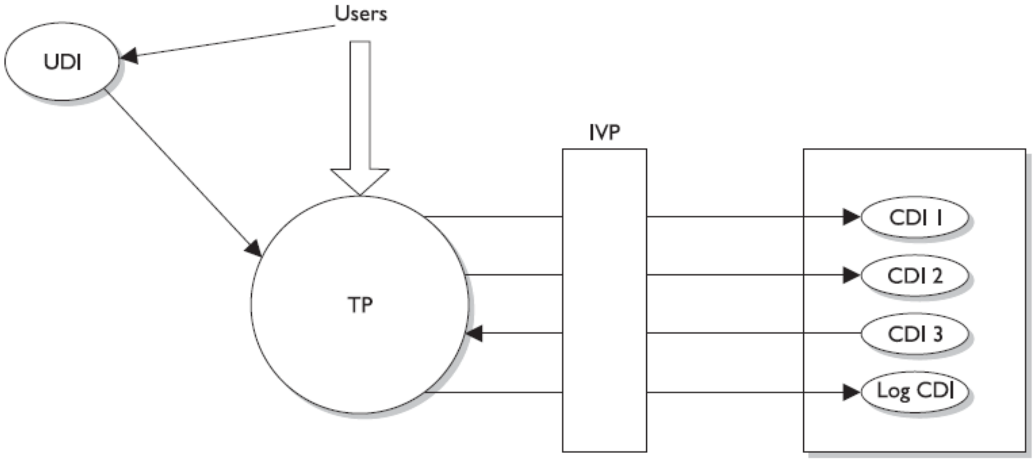
Does Biba Model address all three goals?

Information Security Models

- Clark-Wilson Model

The Clark-Wilson model was developed after Biba and takes some different approaches to protecting the integrity of information. This model uses the following elements:

- **Users:** Active agents
- **Transformation procedures (TPs):** Programmed abstract operations, such as read, write, and modify.
- **Constrained data items (CDIs):** data items that can be manipulated only by TPs.
- **Unconstrained data items (UDIs):** data items that can be manipulated by users via primitive read and write operations.
- **Integrity verification procedures (IVPs):** Check the consistency of CDIs with external reality



Clark-Wilson Model address all three Integrity goals.

Information Security Models

- Noninterference Model

The noninterference model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level.

> *The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a* ***covert channel****.*

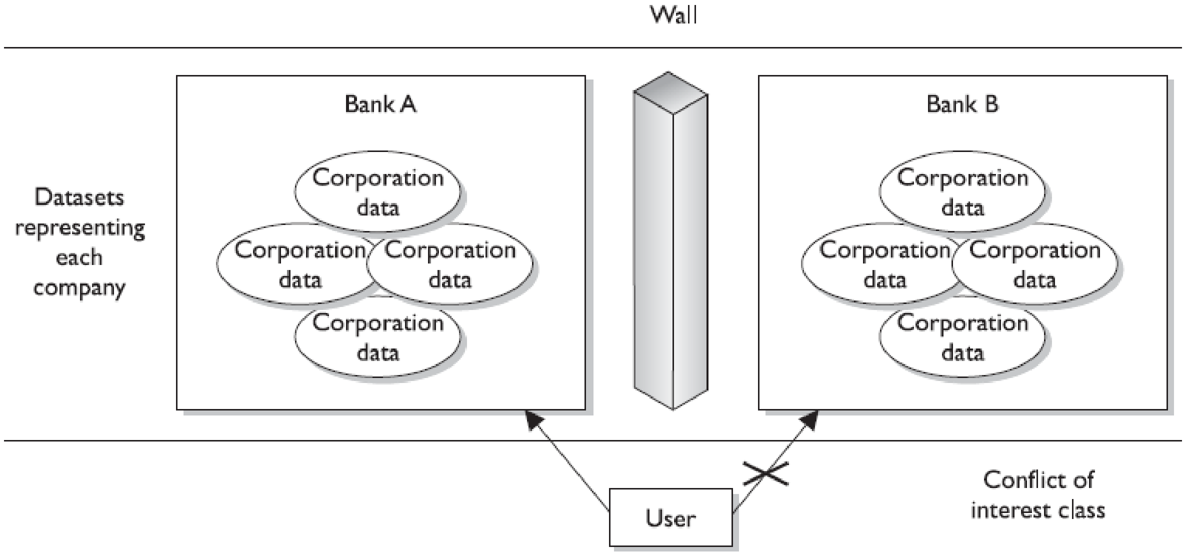
Security Policy: no cover channel exists in the system.

Information Security Models

- Chinese Wall Model

The **Brewer and Nash model**, also called the **Chinese Wall model**, was created to provide access controls that can change dynamically depending upon a user's previous actions. The model ensures that a subject can write to an object if, and only if, the subject cannot read another object that is in a different dataset.

The main goal of the model is to protect against conflicts of interest by users' access attempts.



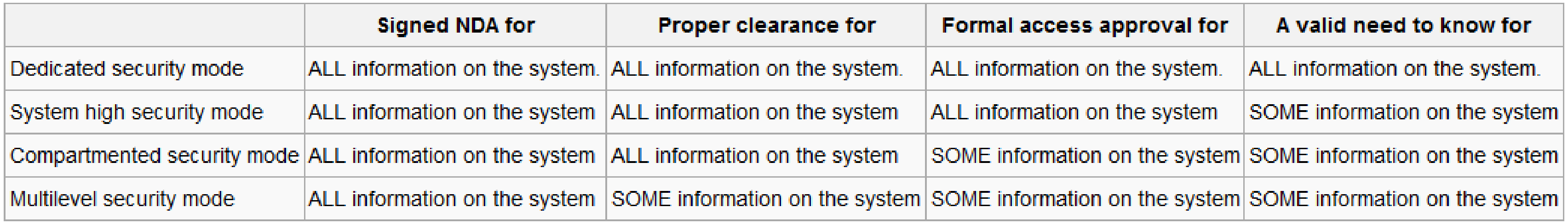
Security Policy: unethical actions are not allowed.

Information Security Models

- Security Modes of Operation

In Mandatory Access Control (MAC) systems (e.g Bell-LaPadulamodel, Biba Model, etc), the mode of operation describes the security conditions under which the system actually functions.

- **Dedicated Security Mode:** Employs a single classification level. All users can access all data, but they must sign a **nondisclosure agreement** (NDA) and be formally approved for access on a need-to-know basis.
- **System High Security Mode:** All users have the same security clearance (as in the dedicated security model) but they do not all possess a need-to know clearance for all the information in the system.
- **Compartmented Security Mode: All** users must possess the highest security clearance (as in both dedicated and system high security), but they must also have valid need-to-know clearance, a signed NDA, and formal approval for all information to which they have access.
- **Multilevel Security Mode:** System allows two or more classification levels of information to be processed at the same time.



	Signed NDA for	Proper clearance for	Formal access approval for	A valid need to know for
Dedicated security mode	ALL information on the system.	ALL information on the system.	ALL information on the system.	ALL information on the system.
System high security mode	ALL information on the system	ALL information on the system	ALL information on the system	SOME information on the system
Compartmented security mode	ALL information on the system	ALL information on the system	SOME information on the system	SOME information on the system
Multilevel security mode	ALL information on the system	SOME information on the system	SOME information on the system	SOME information on the system

Security Evaluation

System/Product security can be evaluated and assigned a **Trust or Assurance Rating**.

- An assurance evaluation examines the security-relevant parts of a system.
- Assurance Rating tells the customer how much protection he can expect out of this system and the assurance that the system will act in a correct and predictable manner in each and every computing situation.
- Assurance Rating is usually used to compare security of similar products/systems.
- There are different methods of evaluating and assigning assurance ratings to systems.
  - **The Trusted Computer System Evaluation Criteria (TCSEC) (aka. The Orange Book)**
  - **Trusted Network Interpretation (TNI) T(aka. the Red Book)**
  - **Information Technology Security Evaluation Criteria (ITSEC)**
  - **Common Criteria**

Security Evaluation

- Some Concepts

- **Trusted Computing Base (TCB):** a collection of all the hardware, software, and firmware components within a system that provide some type of security and assurance. TCB components should be tamperproof.
- **Security Perimeter:** a boundary that divides the trusted environment from the untrusted environment. Communications cross the security perimeter must be controlled to ensure that the system stays stable and safe. (This control happens through APIs).
- **Reference Monitor:** an abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.
- **Security Kernel:** a collection of hardware, software, and firmware components that
- fall within the TCB, and it implements and enforces the reference monitor concept.
- **Open System:** Designs are built upon accepted standards to allow for
- interoperability.
- **Closed System:** Designs are built upon proprietary procedures, which inhibit interoperability capabilities.

Security Evaluation

- The Orange Book

The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book with an orange cover, which is called, appropriately, the ***Orange Book.***

The criteria breaks down into seven different areas:

- *Security policy*
- *Identification*
- *Labels*
- *Documentation*
- *Accountability*
- *Life-cycle assurance*
- *Continuous protection*

The Orange Book provides a classification system that is divided into hierarchical divisions of assurance ratings:

Division D: Minimal Protection
Division C: Discretionary Protection
    C1: Discretionary Security Protection
    C2: Controlled Access Protection
Division B: Mandatory Protection
    B1: Labeled Security
    B2: Structured Protection
    B3: Security Domains
Division A: Verified Protection
    A1: Verified Design

Security Evaluation

- The Red Book

The Orange Book addresses single-system security, The Trusted Network Interpretation (TNI), also called the Red Book, addresses security evaluation topics for networks and network components. It addresses isolated local area networks and wide area internetwork systems. The following is a brief overview of the security items addressed in the Red Book:

- ***Communication integrity***
    - ***Authentication***
    - ***Message integrity***
    - ***Nonrepudiation***
- ***Denial-of-service prevention***
    - ***Continuity of operations***
    - ***Network management***
- ***Compromise protection***
    - ***Data confidentiality***
    - ***Traffic flow confidentiality***
    - ***Selective routing***

Assurance is derived by comparing how things actually work to a theory of how things should work. Assurance is also derived by testing configurations in many different scenarios, evaluating engineering practices, and validating and verifying security claims.

Security Evaluation

- Information Technology Security Evaluation Criteria (ITSEC)

The Information Technology Security Evaluation Criteria (ITSEC) was the first attempt at establishing a single standard for evaluating security attributes of computer systems and products by many European countries. ITSEC evaluates two main attributes of a system's protection mechanisms:

- Functionality: whether the protection mechanisms are delivered or not.
- Assurance: the degree of confidence in the protection mechanisms, and their effectiveness and capability to perform consistently.

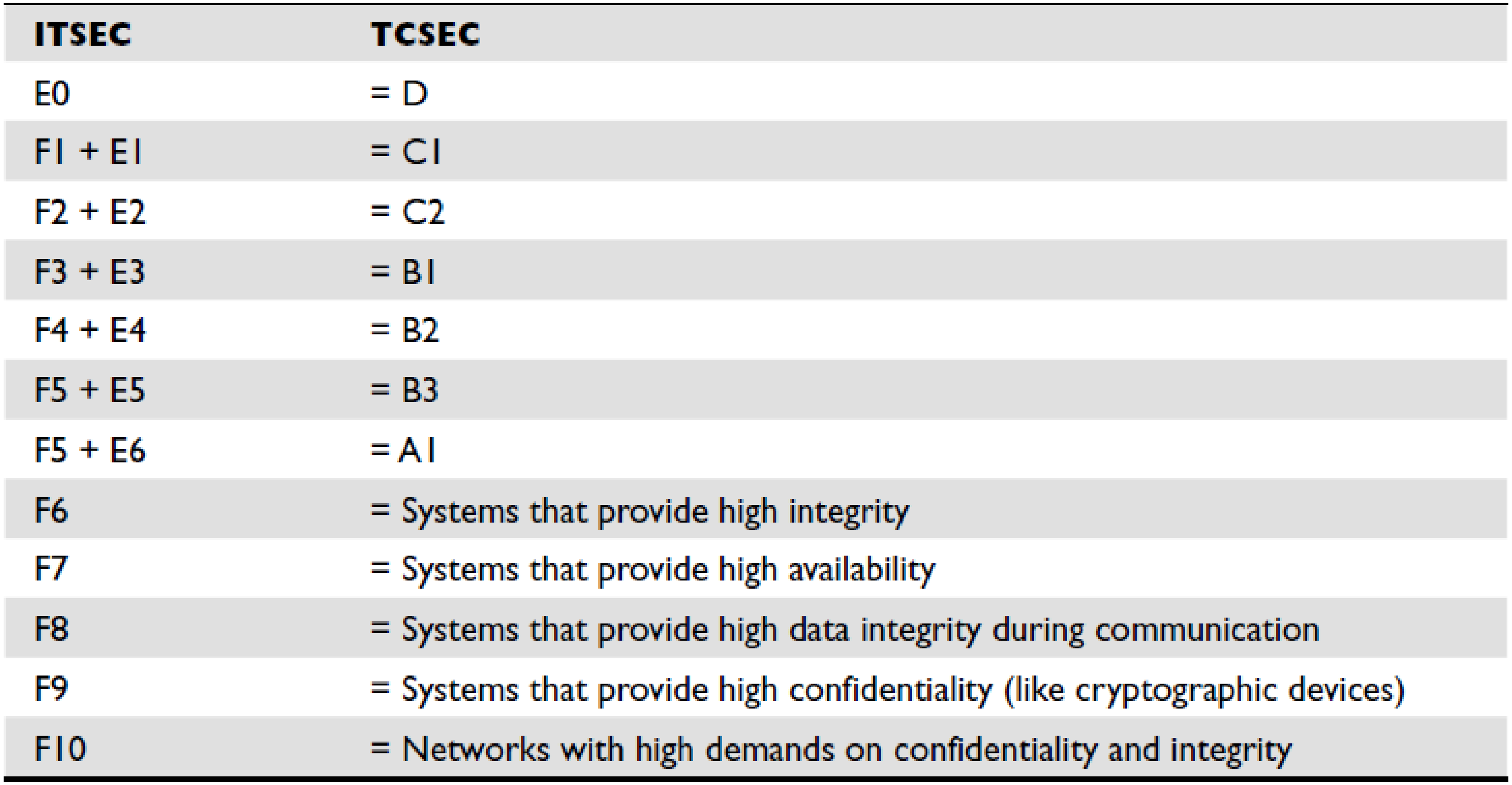
The set of functionalities and assurance items tested during an evaluation:

- *Security functional requirements*
- *Identification and authentication*
- *Audit*
- *Resource utilization*
- *Trusted paths/channels*
- *User data protection*
- *Security management*
- *Product access*
- *Communications*
- *Cryptographic support*
- *Security assurance requirements*
- *Guidance documents and manuals*
- *Configuration management*
- *Vulnerability assessment*
- *Delivery and operation*
- *Life-cycle support*
- *Assurance maintenance*
- *Development*
- *Testing*

In the ITSEC criteria, classes F1 to F10 rate the functionality of the security mechanisms, whereas E0 to E6 rate the assurance of those mechanisms.

Security Evaluation

- ITSEC and TCSEC Mapping

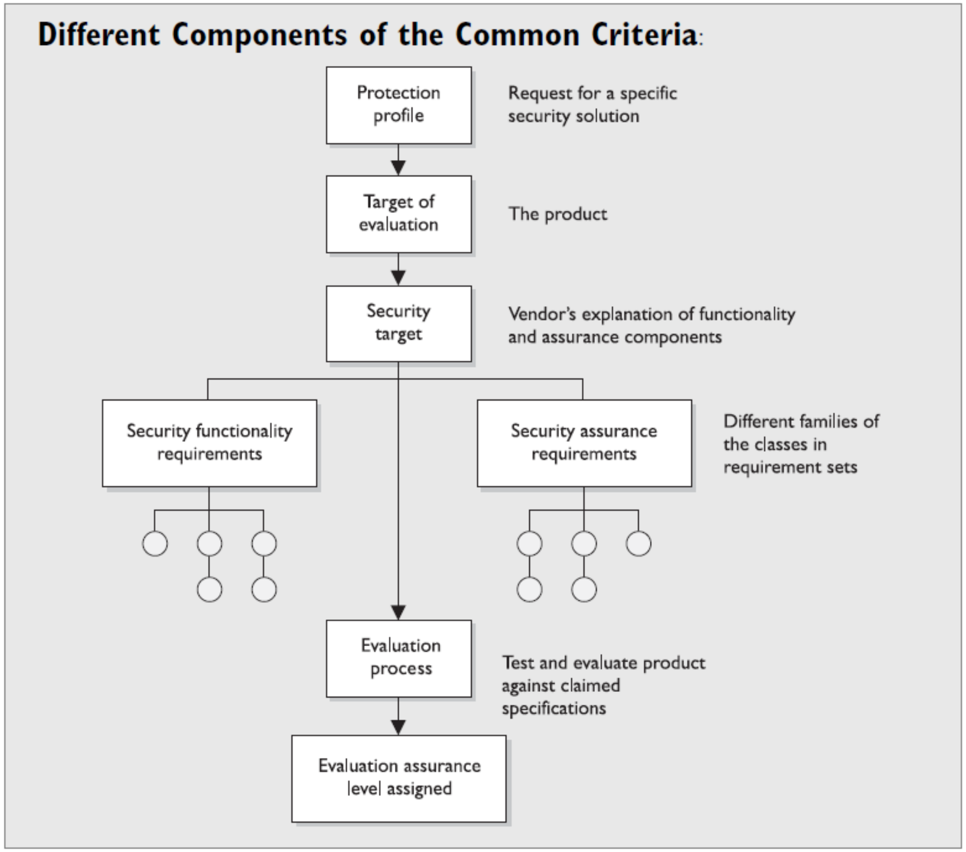


ITSEC	TCSEC
E0	= D
F1 + E1	= C1
F2 + E2	= C2
F3 + E3	= B1
F4 + E4	= B2
F5 + E5	= B3
F5 + E6	= A1
F6	= Systems that provide high integrity
F7	= Systems that provide high availability
F8	= Systems that provide high data integrity during communication
F9	= Systems that provide high confidentiality (like cryptographic devices)
F10	= Networks with high demands on confidentiality and integrity

Security Evaluation

- Common Criteria

In 1990, the International Organization for Standardization (ISO) identified the need for international standard evaluation criteria to be used globally. The end result is the Common Criteria. The Common Criteria evaluates a product against a **protection profile**.



Different Components of the Common Criteria:

Protection profile — Request for a specific security solution

Target of evaluation — The product

Security target — Vendor's explanation of functionality and assurance components

Security functionality requirements

Security assurance requirements — Different families of the classes in requirement sets

Evaluation process — Test and evaluate product against claimed specifications

Evaluation assurance level assigned

Under the Common Criteria model, an evaluation is carried out on a product and it is assigned an ***Evaluation Assurance Level (EAL):***

- EAL1 Functionally tested
- EAL2 Structurally tested
- EAL3 Methodically tested and checked
- EAL4 Methodically designed, tested, and reviewed.
- EAL5 Semiformally designed and tested
- EAL6 Semiformally verified design and tested
- EAL7 Formally verified design and tested

Protection Profile Lists: *https://www.commoncriteriaportal.org/pps/*

Security Certification and Accreditation

Assurance rating only indicates the security level of a product or system from development perspective, but can't assure security in operation. Security in operation is made up of system administration, physical security, installation, configuration mechanisms within the environment, and continuous monitoring.

- ***Certification*** is the comprehensive technical evaluation of the security components and their compliance for the purpose of accreditation. A certification process may use safeguard evaluation, risk analysis, verification, testing, and auditing techniques to assess the appropriateness of a specific system.
  - The certification process and corresponding documentation will indicate the good, the bad, and the ugly about the product and how it works within the given environment.
- ***Accreditation*** is the formal acceptance of the adequacy of a system's overall security and functionality by management.
  - Accreditation confirms that management understands the level of protection the system will provide in its current environment and understands the security risks associated with installing and maintaining this system.

Because software, systems, and environments continually change and evolve, the certification and accreditation should also continue to take place. Any major addition of software, changes to the system, or modification of the environment should initiate a new certification and accreditation cycle.