## System Architecture

Central processing unit

* Conversion of raw input data into useful information called output
* Controls system’s devices
* Multitasking, multiprocessing, multithreading

Storage devices

* Primary storage is memory, cache, or registers; also where data waits for the CPU: RAM, synchronous dynamic RAM (SDRAM), ROM
* Secondary storage, non-volatile, data not currently being processed by the CPU: fixed disks, floppy diskettes, flash memory, any mountable device
* Virtual memory, simulates main memory with virtual addresses
* Random vs. Sequential

Peripherals

* Scanners, printers, modems, etc.

## ISO/IEC 17799:2005,

## BS 7799:2, ISO 270001

ISO/IEC 17799:2005 is the “Code of Practice for Information Security Management”

* Set of internationally recognized best practises for information security
* No certification / accreditation

BS 7799:2 "Information Security Management Systems - Specification with guidance for use."

* Instructions for how to apply ISO 17799:2005
* Certification is provided against this spec

ISO 27001 is the updated ISMS standard, 2005

* Replaces BS 7799:2
* Certification is provided

## Design principles

Diskless workspaces, thin clients

* Workstations without a hard drive
* Uses a central server for booting, data and applications
* Downside: not usable during a network outage

**Operating system security protection mechanisms**

Privilege levels, ring protection

Controls access from less privileged to more privileged levels

Priority, privilege and memory segmentation

Layering – assign each process to a specific layer

Data hiding – prevents data at one security level from being seen by processes operating at other security levels

Abstraction – users do not need to know particulars of an objects functions

### Hardware, Software, Firmware

Hardware

* Mainframes, desktops
* PDAs, Smart Phones
* CPUs are multitasking, multiprocessing, multi-threading

Software

Operating systems

* System kernel – provides access to system resources
* CPU has 2 states: supervisor state (privilege or kernel mode) and problem state (nonprivileged or user mode)
* Middleware is software that enables multiple processes on one or more machines to interact
* Firmware – programs or instructions in read only memory. Usually written to electronically erasable programmable read-only memory (EEPROM)

## Trusted Computer Base

* Defined by The Orange Book (The DoD TCSEC)
* Combination of hardware, software and firmware responsible for enforcing the security policy
* Reference Monitor – abstract machine that moderates all access to objects by subjects, must be auditable to be sure it doing what it is supposed to

## Types of Security Models

State machine models

* Rule set is determined by the security policy
* Automated information system’s (AIS) security state can change only when an event occurs or a clock triggers it
* AIS boots in secure state, and because every access is in accordance with security policy, AIS remains in a secure state.

Research Models

* Non-interference model: high level actions (inputs) cannot determine what low level users can see (outputs)
* Access Control Matrix

## State Machine Security Models

Bell-LaPadula (BLP) Confidentiality

* Defined by The Orange Book (The DoD TCSEC)
* State machine model
* Confidentiality of an automated information system is ensured
* Uses mandatory access control based on security labels on assets, and security clearance on subjects
* Simple security: no read up
* property: no write down
* Discretionary Security property: system uses an access matrix to enforce discretionary access control
* *Example: military secrets. Low ranking officers cannot read up about matters of national security, and cannot accidentally leak out information to soldiers by writing down.*

Biba Integrity

* Higher levels of integrity are more trusted than lower ones
* Assign integrity levels to objects and subjects.
* Simple integrity property: no read down
* integrity property: no write up
* *Example: clean water. No write up prevents dirtier water from tainting cleaner water. No read down would stop the inflow of dirty water into a cleaner stream*

**Clark Wilson Integrity**

Addresses the 3 goals of integrity…

* Well formed transactions, and separation of duties
* Subject – program – object bindings

**Access Control Matrix**

* This table is for discretionary access control
* Mandatory access control table would replace “role” for userid

**Information Flow Security Models**

* objects are labeled with security classes in the form a of a lattice, and information may flow from one data set to another without concern for direction
* Graham-Denning
* Harrison-Ruzzo-Ullman

**Brewer-Nash (Chinese Wall)**

* Access control changes with duties
* Security domains are sensitive to conflict of interest
* Uses principle of data isolation
* *Example: when testing a product for Company B, do not allow access to data for Company C*

## Security Product Evaluation Methods

**TCSEC Rainbow Series**

|  |  |
| --- | --- |
| A Verified protection | Mandatory Access Controls |
| A1 Verified design |
| B Mandatory protections |
| B3 Security domains |
| B2 Structured protections |
| B1 Labeled security |
| C Discretionary protection | Discretionary access controls |
| C2 Controlled access |
| C1 Discretionary protection |
| D Minimal security |  |

**ITSEC**

* Primarily used in Europe.
* Functionality rating (F1 to F10)
* Assurance rating (E0 to E6)

|  |  |
| --- | --- |
| E0 | D |
| F1 + E1 | C1 |
| F2 + E2 | C2 |
| F3 + E3 | B1 |
| F4 + E4 | B2 |
| F6 + E5 | B3 |
| F6 + E6 | A1 |
| F6 – high integrity | |
| F7 – high availabilty | |
| F8 – data integrity during communications | |
| F9 – high confidentiality | |
| F10 – networks with high demands on confidentiality | |
| and integrity | |

* Security Product Evaluation Methods

## Common Criteria

Evaluation of protection profiles (PPs)

There are seven evaluation assurance levels

|  |  |
| --- | --- |
| EAL1 | product functionality tested |
| EAL2 | structurally tested |
| EAL3 | methodically tested and checked |
| EAL4 | methodically designed, tested and reviewed |
| EAL5 | semiformally designed and tested |
| EAL6 | semiformally verified, designed and tested |
| EAL7 | formally verified, designed and tested |