

Hardware & System Infrastructure

Processor States

Single State Processors	Multi-State Processors
Processors restricted to one security level at a time.	Processors capable of managing data at multiple security levels simultaneously.
A system exclusively processing confidential data, unable to handle different security levels concurrently.	A military system processing top-secret, secret, and unclassified data concurrently while maintaining isolation and security for each level.

MultiX Concepts

Multitasking	Multithreading	Multiprocessing	Multiprogramming
Concurrently running multiple applications with the operating system handling task switching.	Running multiple threads within a single program to enhance responsiveness and performance.	Utilizing multiple processors or cores to enhance computing power and performance.	Allowing multiple programs or tasks to share system resources, commonly on mainframe systems.
E.g. Listening to music while browsing the web on a personal computer.	E.g. A word processor with threads for typing, auto-saving, and spell checking.	E.g. Desktop computer with a quad-core CPU processing several tasks at once.	E.g. Mainframe managing jobs like data processing, printing, and calculations simultaneously.

Memory

Read-Only Memory (ROM)

- **Definition:** A non-volatile memory with data that is permanently written during its manufacturing.
 - **Characteristics:** It provides permanent storage, with contents ingrained during the manufacturing process.
-
- **Programmable Read-Only Memory (PROM):** This type of memory allows users to program it once after manufacturing.
 - **Erased Programmable Read-Only Memory (EPROM):** A memory chip that can be programmed and subsequently erased and reprogrammed via ultraviolet light.

- **Ultraviolet Erasable PROM (UVEPROM):** Characterized by a small window that exposes the chip, enabling erasure through UV light.
 - **Electrically Erasable PROM (EEPROM):** This version can be erased by administering specific electrical voltages, facilitating more intricate data manipulation than what UVEPROM offers.
-

Random Access Memory (RAM)

- **Definition:** This is the main volatile memory used for temporary storage when a computer operates. Its contents are lost when the device is powered off.
 - **Static RAM (SRAM):** Relies on flip-flops to store each bit of data.
 - **Dynamic RAM (DRAM):** Utilizes capacitors for storing data bits and necessitates periodic refreshing.

Flash Memory

- **Definition:** Evolved from EEPROM, flash memory is non-volatile and permits electronic erasure and reprogramming.
 - **Characteristics:** Due to its durability and swift access times, it's extensively used in USB drives, SSDs, and memory cards.
-

Storage

1. Primary Storage (Memory):

- **Definition:** Directly accessible by the CPU. This is where the operating system, application software, and data in current use are kept so they can be quickly reached by the computer's processor.
- **Examples:** RAM (both SRAM and DRAM).

Secondary Storage:

- **Magnetic:** Hard disk drives (HDDs).
- **Flash:** Solid-state drives (SSDs) and USB drives.
- **Optical:** CDs, DVDs, Blu-ray discs.
- **Definition:** Non-volatile storage mediums that store data until it is deleted or overwritten. Data from secondary storage needs to be loaded into primary storage before being processed.
- **Types:**

Access Types:

- **Random Access:** Storage devices where data can be read or written at any location at any time.
- **Sequential Access:** Storage devices where data has to be read or written sequentially. Accessing specific data means going through the data stored before it.

Security Issues with Secondary Storage

1. Unauthorized Data Extraction with Removable Media:

- Implementing policies to restrict the use of removable media.
- Deploying Data Loss Prevention (DLP) solutions to monitor and control data transfers.

- Description: Portable secondary storage, like USB drives, can easily be used to copy and remove data from a system, leading to data breaches.
- Mitigation:

Inadequate Protection Mechanisms:

- Applying file and disk encryption.
- Implementing robust access control policies.
 - Description: Without proper access controls and encryption, sensitive data on secondary storage can be accessed by unauthorized users.
- Mitigation:

Data Persistence after Deletion or Formatting:

- Employing secure deletion tools that overwrite data multiple times.
- Physical destruction of storage for highly sensitive data.
 - Description: Even after files are deleted or media is formatted, data can often still be retrieved using specialized tools, posing a risk of unauthorized data recovery.
- Mitigation:

Eavesdropping and Tapping on I/O Devices:

- Using secure connections and protocols.
- Regularly inspecting physical devices and connections for tampering, such as unexpected or unauthorized vampire taps.
- Employing network monitoring tools to detect unusual data transfers or connections.
 - Description: Input/Output (I/O) devices connected to secondary storage can be vulnerable to eavesdropping or tapping, allowing malicious actors to intercept data or introduce unauthorized entry points. For instance, a "vampire tap" can be used to clandestinely connect to a network by piercing into a coaxial cable, enabling an attacker to monitor or inject data without being easily detected.
- Mitigation:

Firmware

- Firmware is essentially specialized software stored on a ROM chip.
- While ROM provides the foundational instructions to kickstart a device, firmware provides more specific instructions to ensure the device runs smoothly.
- Apart from computers, firmware is commonly found in peripheral devices like printers to guide their operations.

Embedded Systems & Static Environments

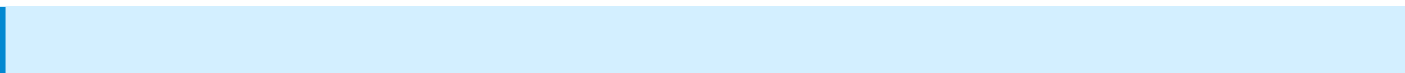
1. Embedded Systems:

- Motion systems (e.g., anti-lock braking system in cars)
 - Lighting systems
 - Cash registers
 - Digital signature pads
 - Wi-Fi routers
-
- Definition: These systems are designed for a specific function or set of functions within a larger system.
 - Examples:
 - They're integral to many devices and can be found in everyday appliances as well as specialized equipment.

Static Environments:

- Definition: Configurations like OSs, hardware, or networks set up for a particular purpose and remain unchanged despite interaction. They are resistant to alterations, even by authorized personnel like administrators.
- Example: An industrial control system (like those used in manufacturing plants) that's configured to manage machinery operations. Changes could disrupt the production process, so the environment remains static to ensure consistent performance.

Management & Security:

- Network Segmentation: Dividing network into various segments to keep critical systems separate and secure.
 - Security Layers: Using multiple security measures to protect systems, akin to having multiple barriers.
 - Application Firewalls: Protects against malicious inputs or attacks targeted at applications.
 - Manual Updates: Due to the sensitivity and specificity, updates might need to be manually reviewed and applied.
 - Firmware Version Control: Ensures only approved and tested firmware versions are in use.
 - Wrappers: Additional security layers around an application or system to shield it from potential threats.
 - Control Redundancy and Diversity: Having multiple controls in place, so if one fails, another can take over or compensate.
 - Both embedded systems and static environments, due to their specialized nature, require targeted security measures.
 - Security Measures:
- 

Remember: As technology evolves, the line between embedded systems and more flexible environments may blur, but the fundamental principles of securing these systems remain the same. Always prioritize the integrity and security of the system while accommodating for its intended function.

Trusted Computing Base (TCB)

:::information TCB is a combination of hardware, software, and controls. :::

- Its primary role is to enforce your security policy.
- TCB is a subset of the complete information system.
 - **Why?** It's the only portion that can be relied upon to adhere to and enforce the security policy.

:::success Only trust the TCB for policy enforcement. :::

Security Perimeter

- It's an imaginary boundary.
- Separates the TCB from the rest of the system.
- Protects subjects (users) from the rest of the system.

:::warning Security perimeter acts as a barrier between TCB and the rest of the system. :::

Reference Monitor

:::quote "Does the subject have the right?" :::

- It's the logical part of the TCB.
- Confirms whether a subject has the right to access a resource before granting that access.
- Primary duty: Enforces access control.

Security Kernel

- It's a collection of TCB components.
- Implements the functionality of the reference monitor.

:::danger Security Kernel is vital; it IMPLEMENTS access control. :::