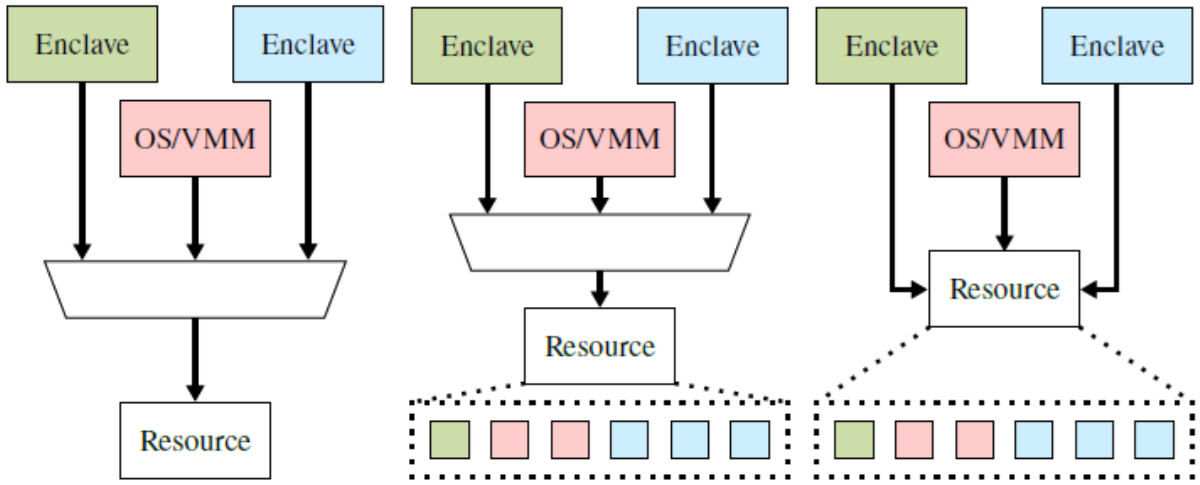
Run-time Isolation

- Run-time isolation protects the confidentiality and integrity of sensitive computations and data during enclave execution.
- This requires isolating both CPU and memory resources.
- Isolation strategies
  - **Resource Partitioning**:
    How resources are divided (temporal, spatial, or spatio-temporal)
  - **Isolation Enforcement**:
    How isolation is enforced (logical or cryptographic)

Resource Partitioning Strategies



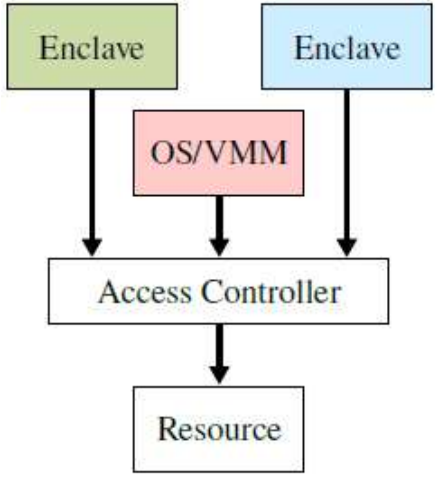
Temporal Partitioning

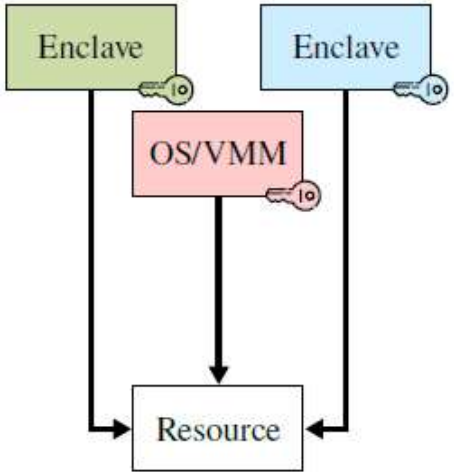
Spatio-temporal Partitioning

Spatial Partitioning

- Temporal
  - Securely multiplexes the same resource among multiple execution contexts over time.
  - At any point, a single context has exclusive access.
- Spatio-temporal
  - Leverages both temporal and spatial aspects.
  - Resources can be spatially partitioned but these partitions may change over time.
- Spatial
  - Resources are split so trusted and untrusted contexts use separate, dedicated partitions.
  - Enables concurrent access without interference.

Isolation Enforcement Strategies





- Logical Isolation
  - Uses access control mechanisms to prohibit unauthorized access
  - Intercepts data accesses and checks against access control information
  - Access control information must be protected
  - Efficient for software adversaries

- Cryptographic Isolation
  - Uses encryption for confidentiality
  - Uses MACs for integrity protection
  - Requires anti-replay schemes for complete integrity
  - Effective against physical adversaries

CPU Isolation

Existing TEEs use temporal partitioning with logical enforcement for CPU state isolation. This approach:

Implementation

Secure context switch routine that saves, purges, and restores execution contexts

Requirements

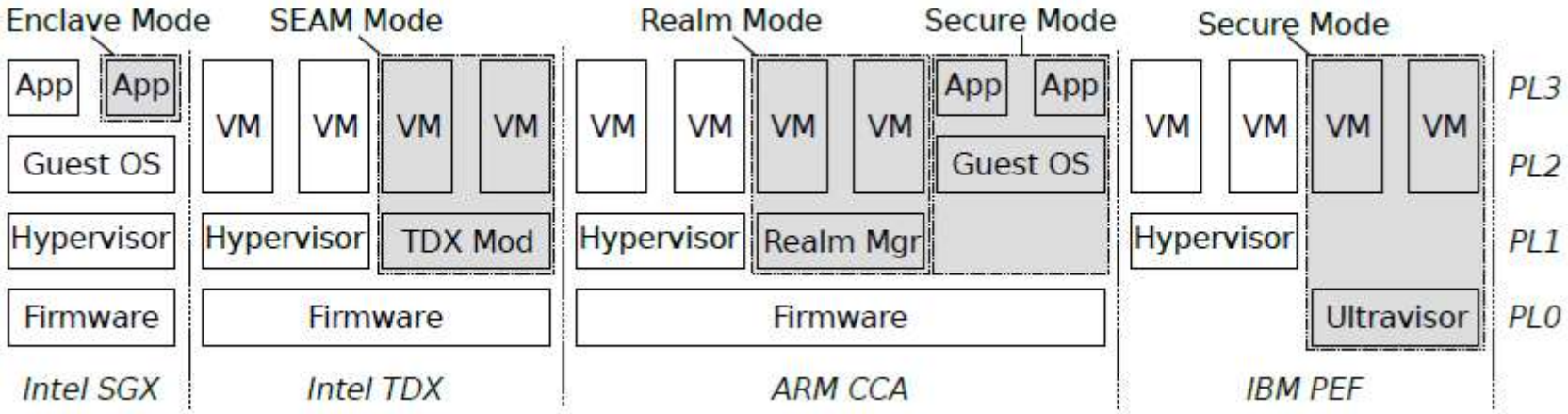
TCB must fully mediate every context switch using CPU modes and privilege levels

Advantages

Minimal performance overhead compared to other approaches

Other approaches like spatial partitioning (dedicating cores to enclaves) or cryptographic enforcement have significant downsides in terms of resource utilization or performance.

CPU Modes



- Commercial processors often add new execution modes to support TEEs.
- In contrast, most academic TEEs rely on existing privilege levels and firmware for secure context switching.