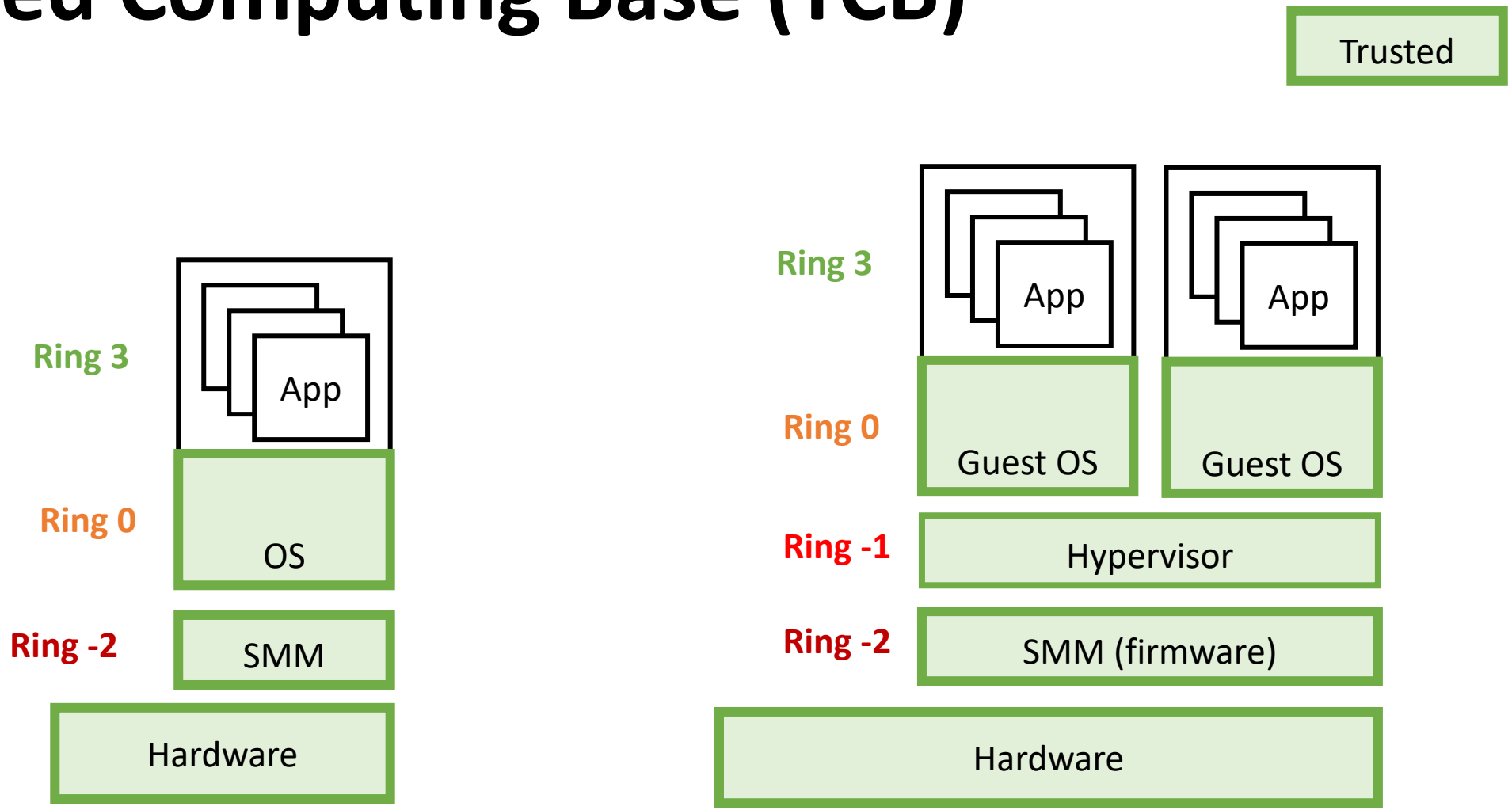
Trusted Execution Environment and Confidential Computing

Mengjia Yan

Spring 2022

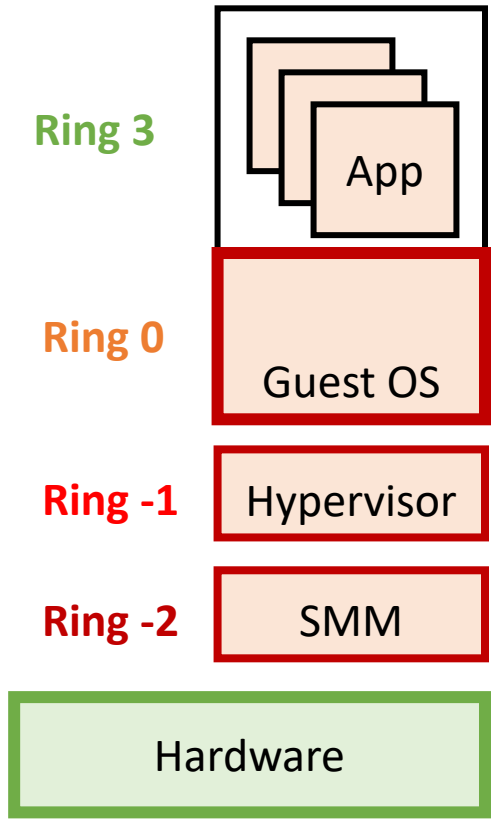
Based on slides from Intel SGX Tutorial

Trusted Computing Base (TCB)



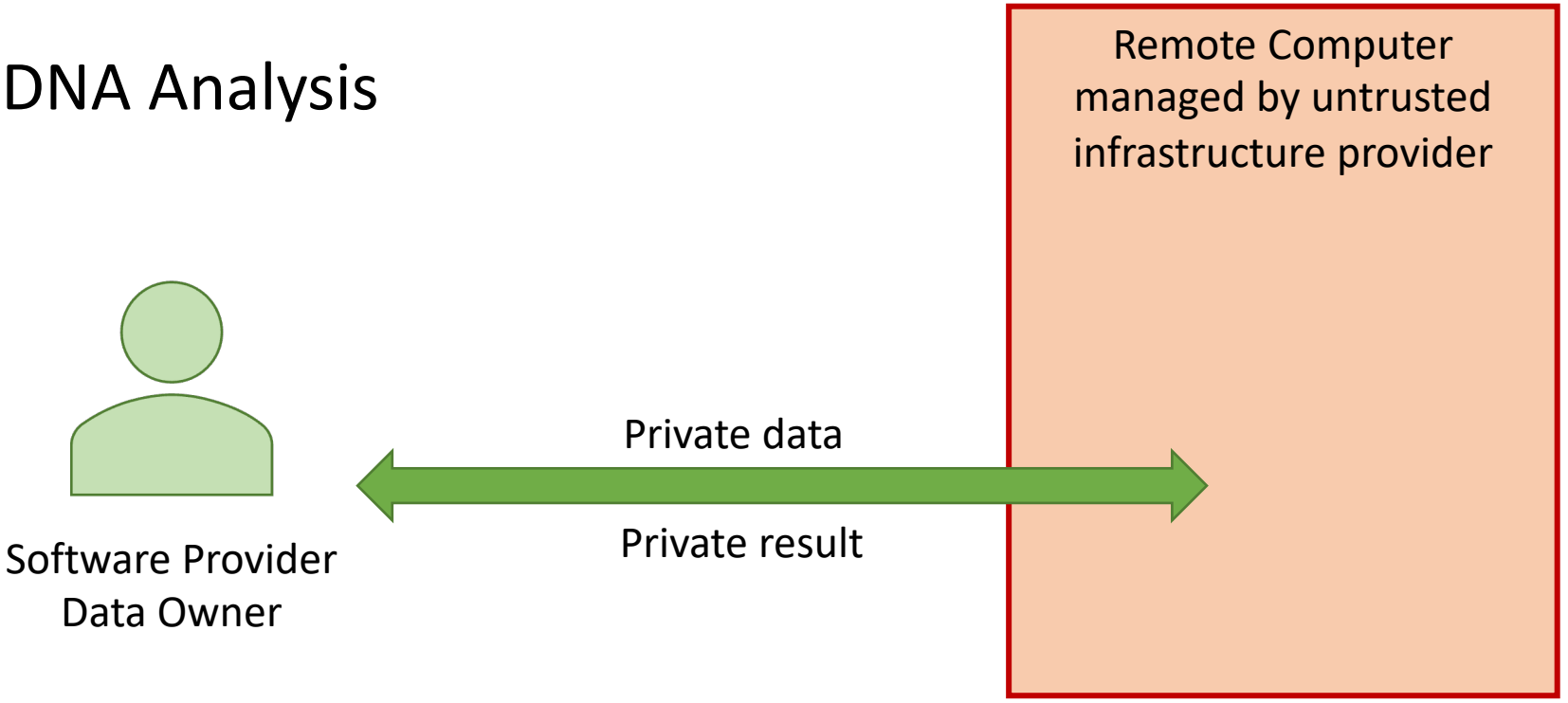
Why Shrink TCB?

- Software bugs
  - SMM-based rootkits
  - Xen 150K LOC, 40+ vulnerabilities per year
  - Monolithic kernel, e.g., Linux, 17M LOC, 100+ vulnerabilities per year
- Remote Computing
  - Remote computer and software stack owned by an untrusted party
  - Why outsource computation?
  - What security problems do we have?



Secure Remote Computing

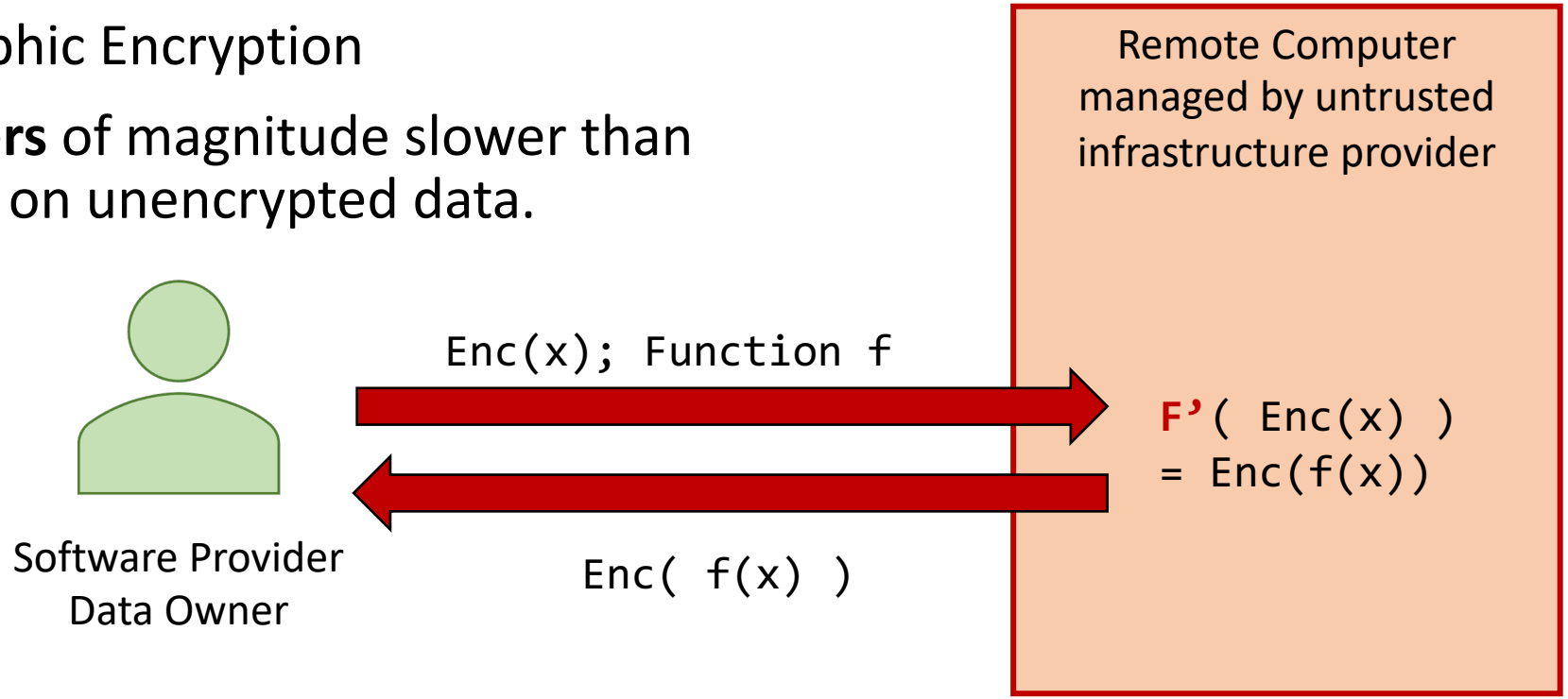
- Example: DNA Analysis



How to keep my data private without trusting the host OS/hypervisor/SMM?

Solutions

- Homomorphic Encryption
- **4 to 5 orders** of magnitude slower than computing on unencrypted data.

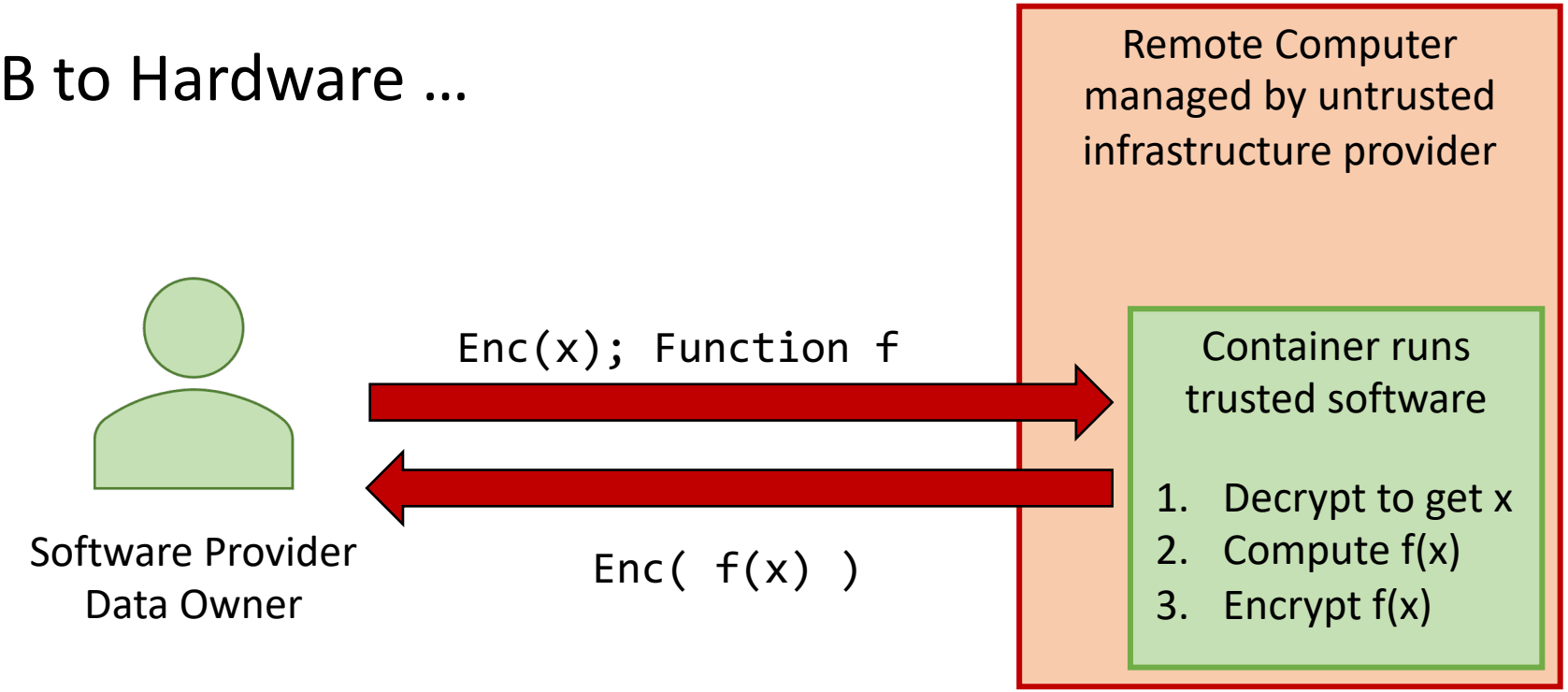


- Performance? Accelerators?

F1: A Fast and Programmable Accelerator for Fully Homomorphic Encryption; Axel Feldmann, Nikola Samardzic et al. MICRO'21

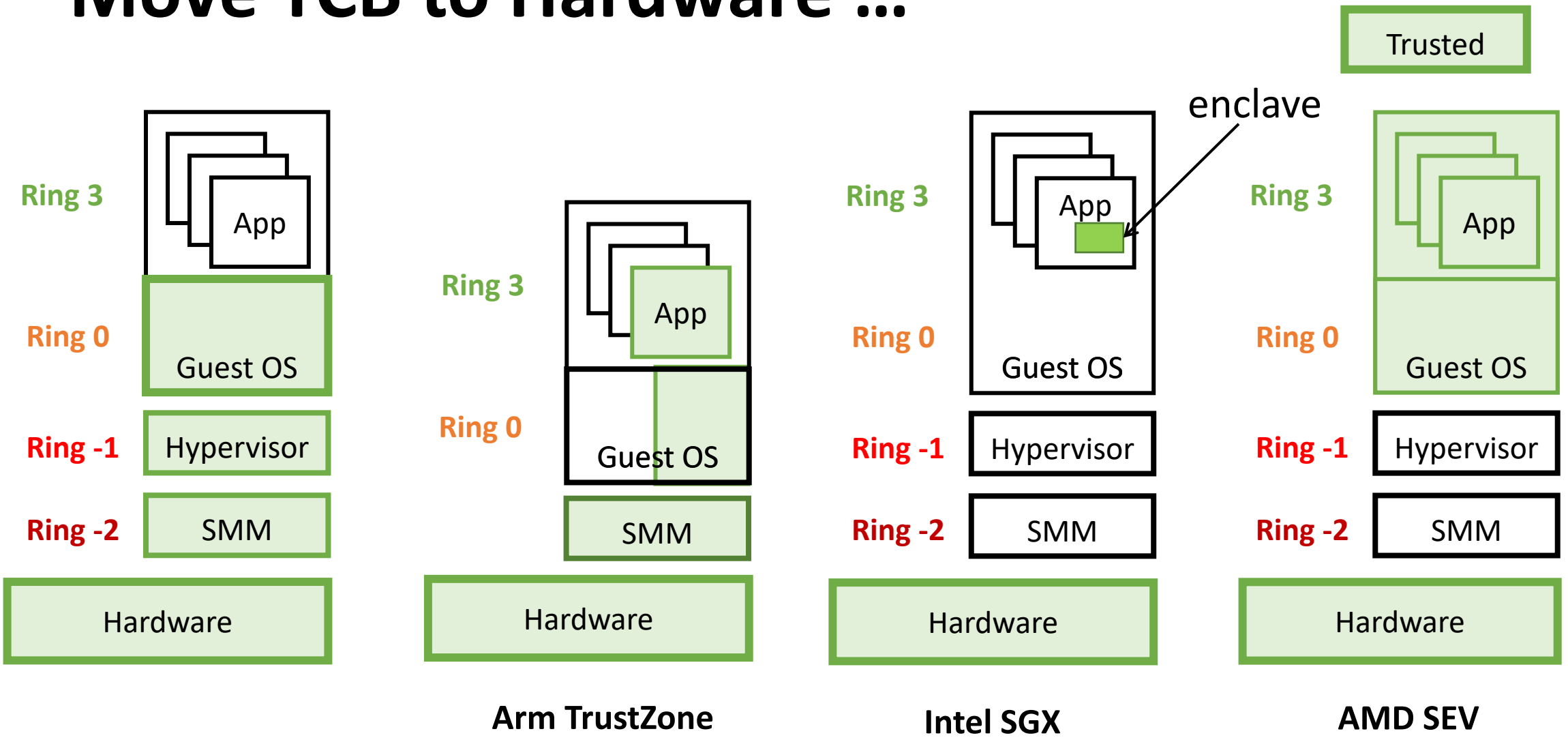
Solutions

- Move TCB to Hardware …



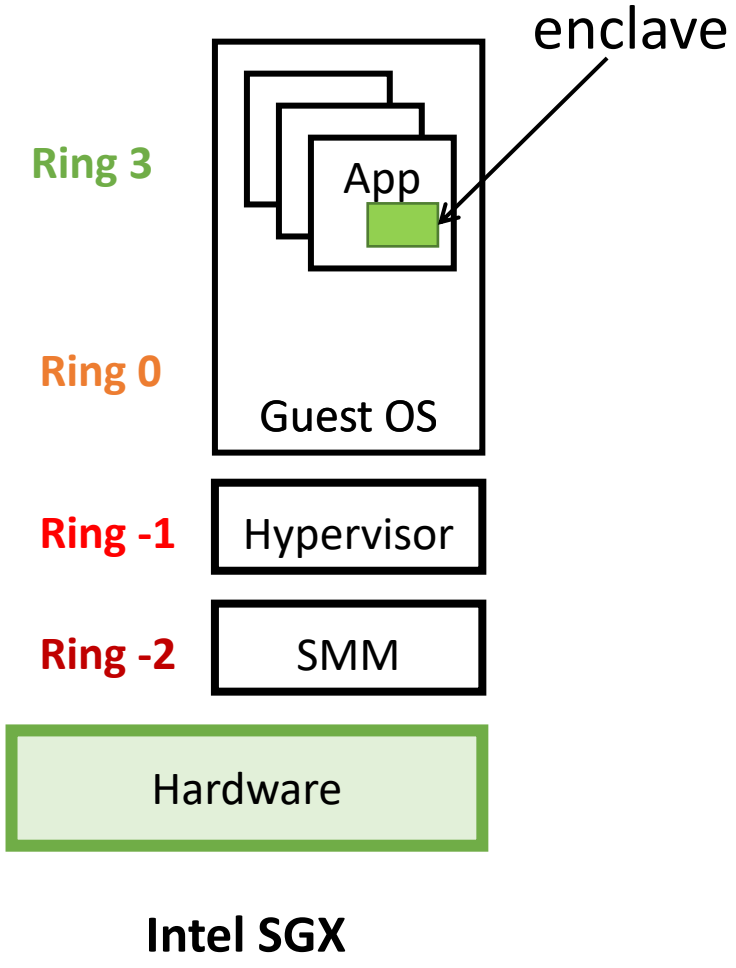
- Performance?
- Need to trust hardware. How to achieve it?

Move TCB to Hardware …



Privileged Software Attacks

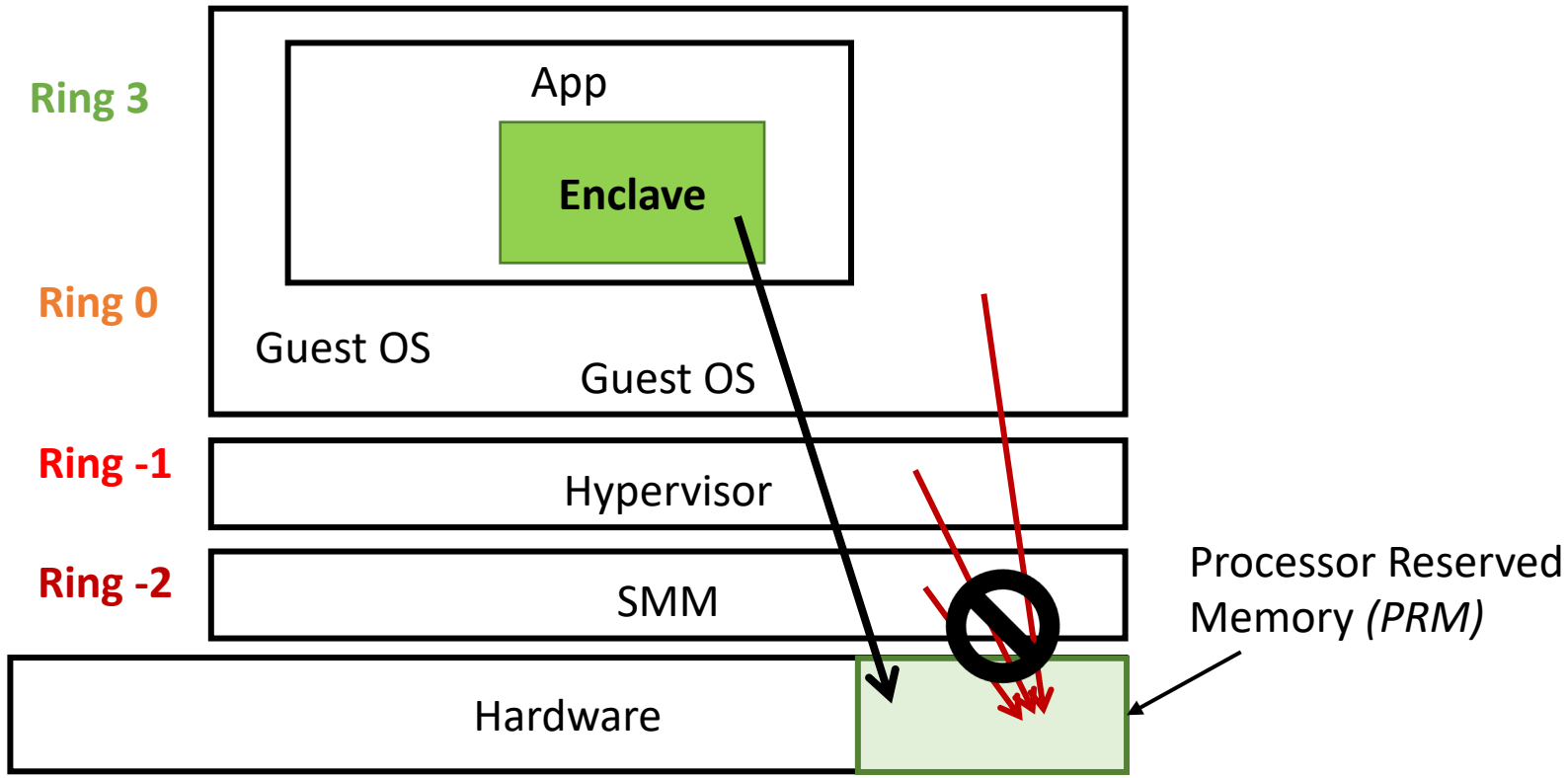
- Manipulate everything
- Directly see and modify application code and data
  - → Need to encrypt secret data
  - → Need to verify integrity (software attestation)
- Mess up with
  - Address translation
  - Process initialization and context switch
  - Interrupts, I/Os
  - etc.



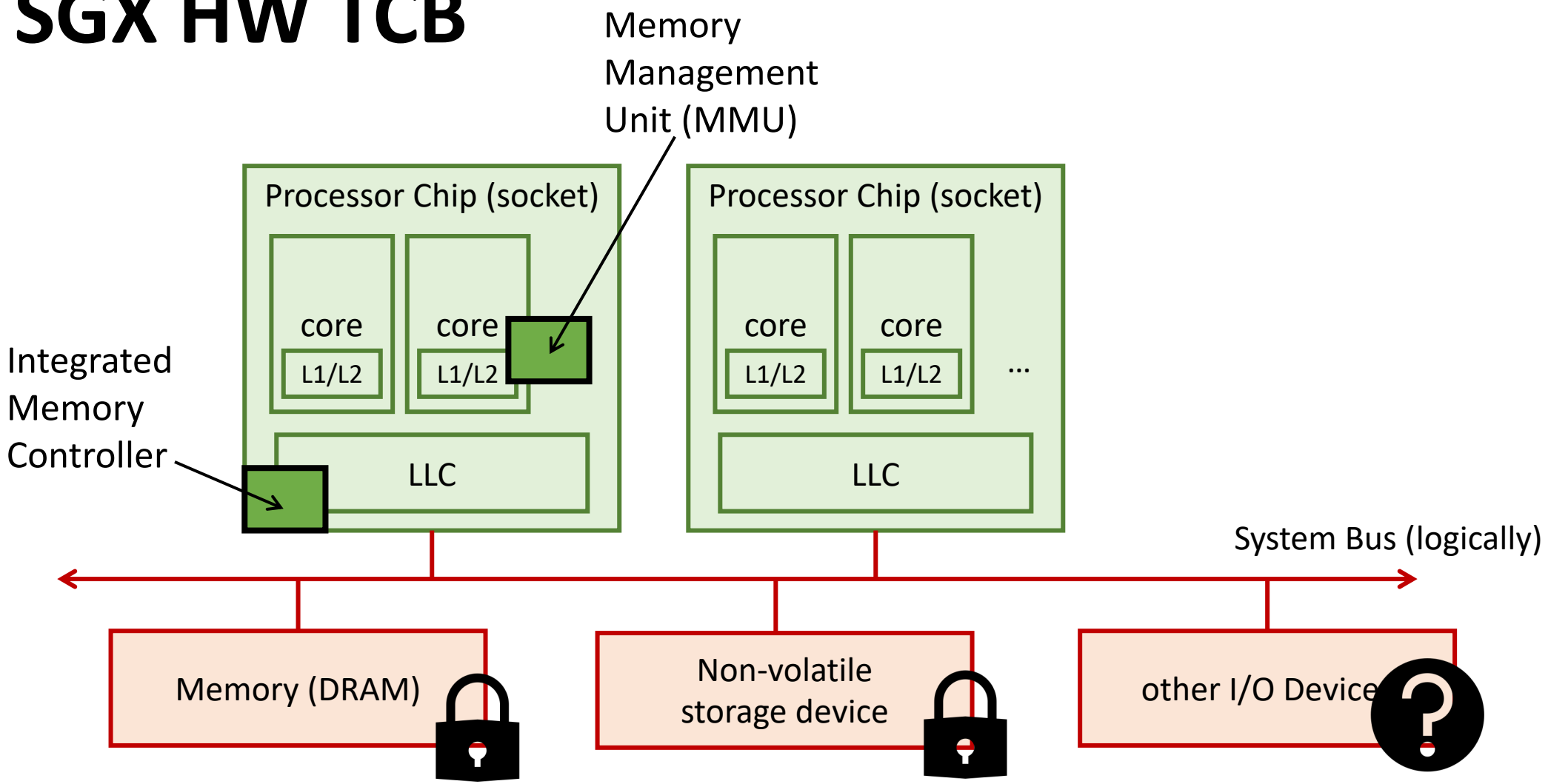
Intel SGX

Enclave High-level View

- Goal: A protected environment that contains the code and data of a security-sensitive computation.

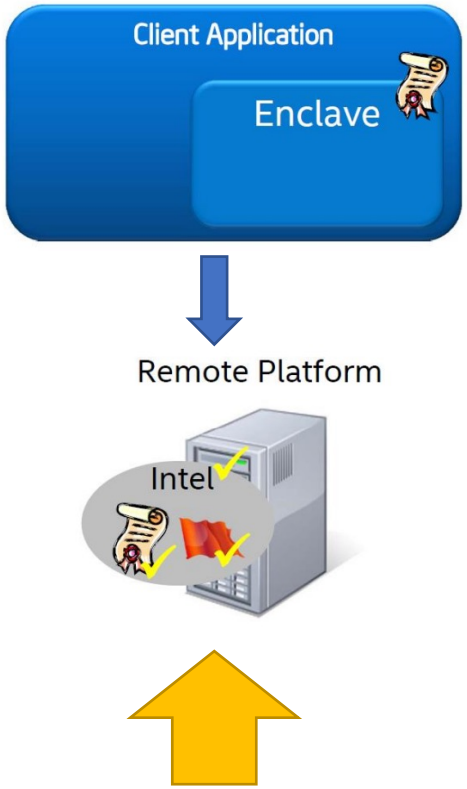


SGX HW TCB

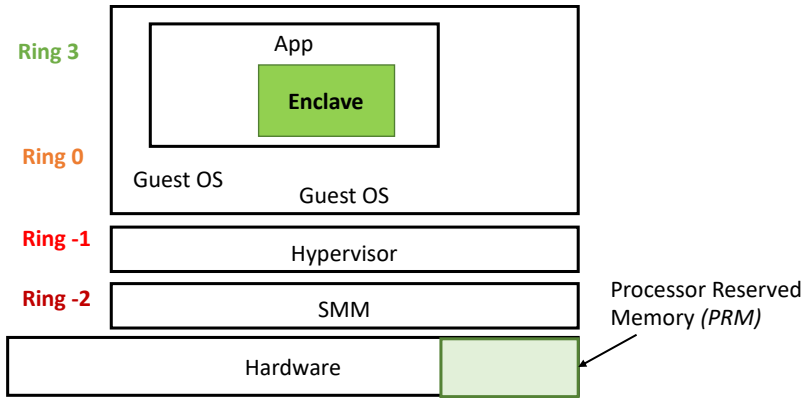

Memory
Management
Unit (MMU)
Processor Chip (socket)
core
L1/L2
core
L1/L2
LLC
Processor Chip (socket)
core
L1/L2
core
L1/L2
...
LLC
Integrated
Memory
Controller
System Bus (logically)
Memory (DRAM)
Non-volatile
storage device
other I/O Device
?

Intel SGX Security Mechanisms

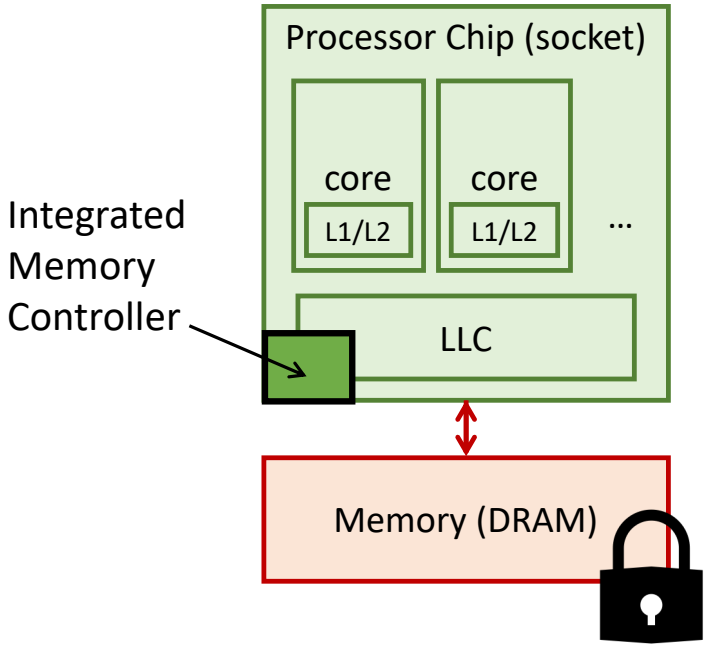
Attestation



Isolation

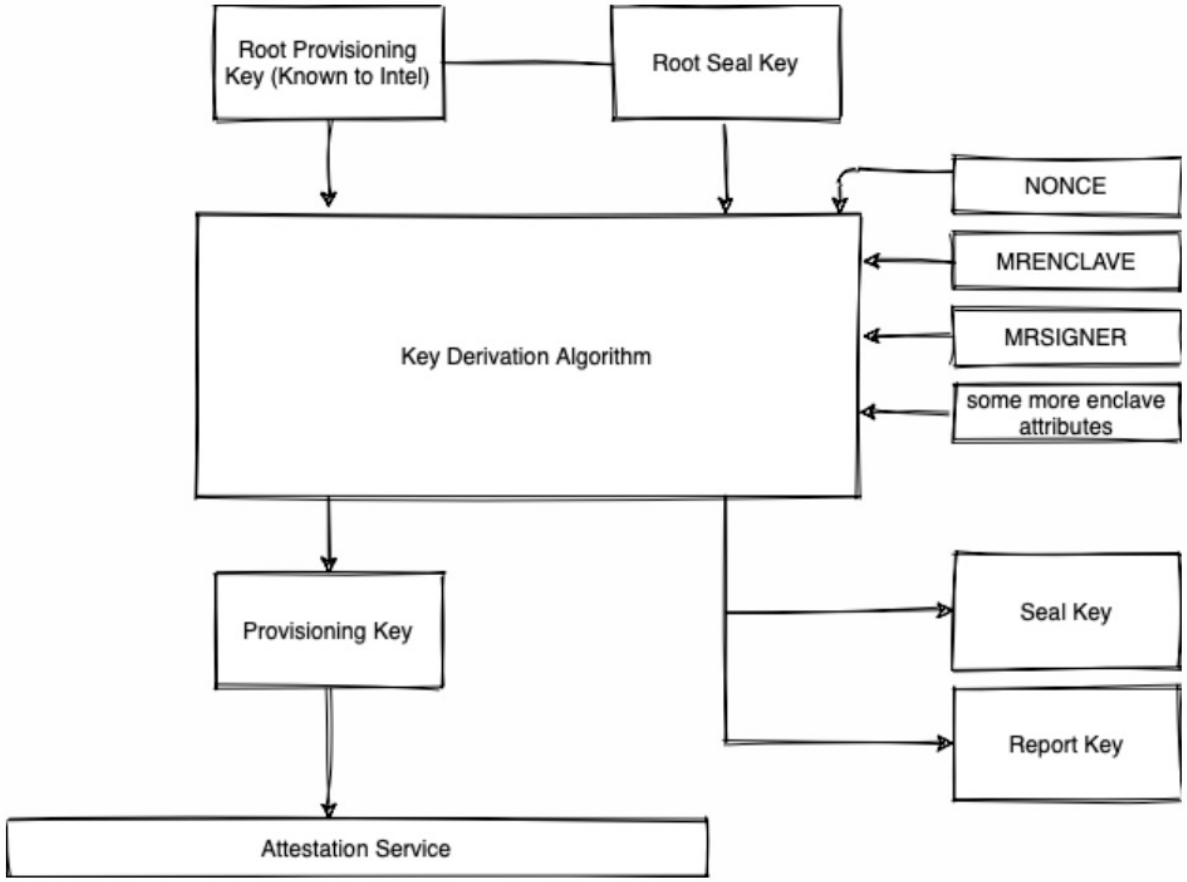


DRAM Protection



Attestation

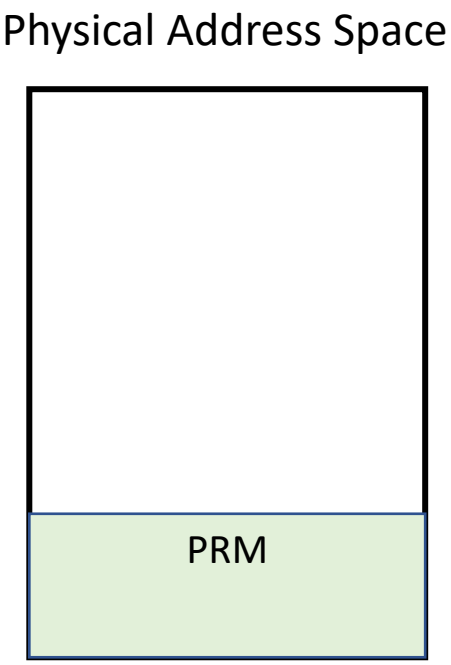
- Platform Attestation
- Enclave Measurement



https://www.conclave.net/blog/decrypting-enclaves-encryption-key-hierarchy/

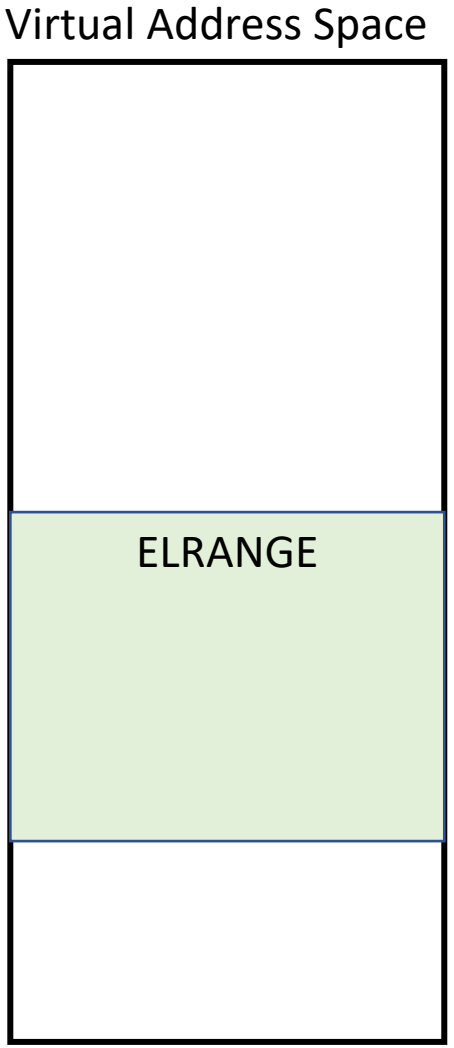
Enclave Initialization

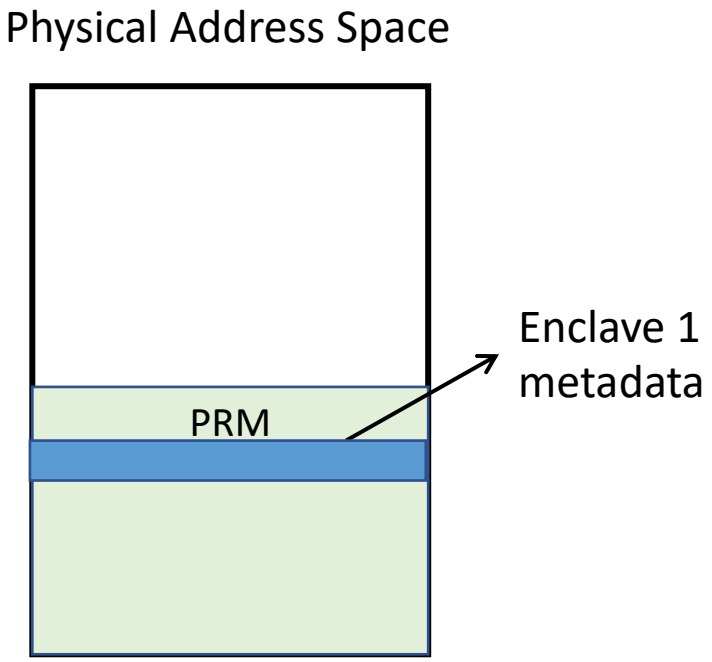
- BIOS setup PRM region



Enclave Initialization

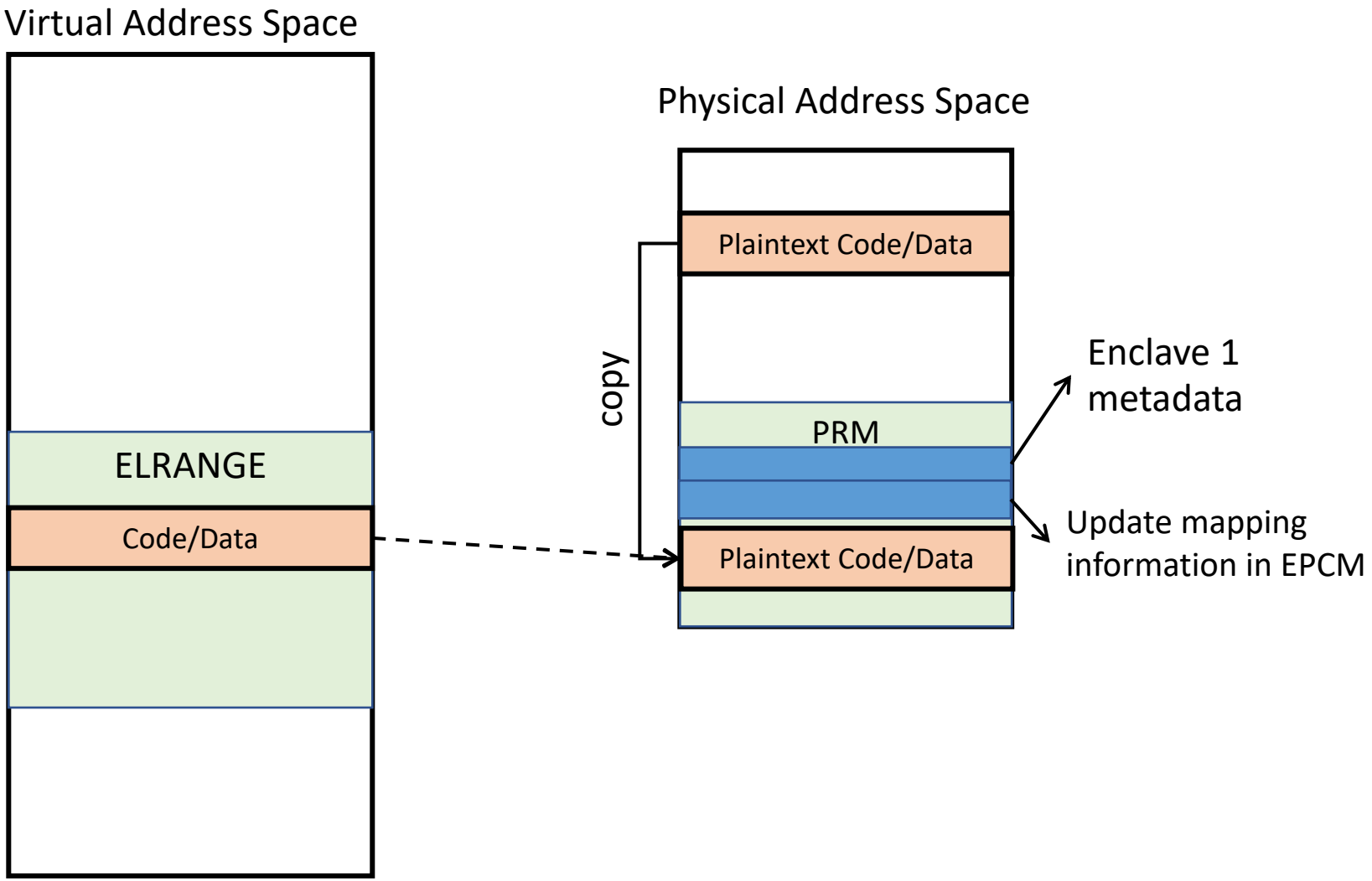
- Enclave creation (ECREATE)





Enclave Initialization

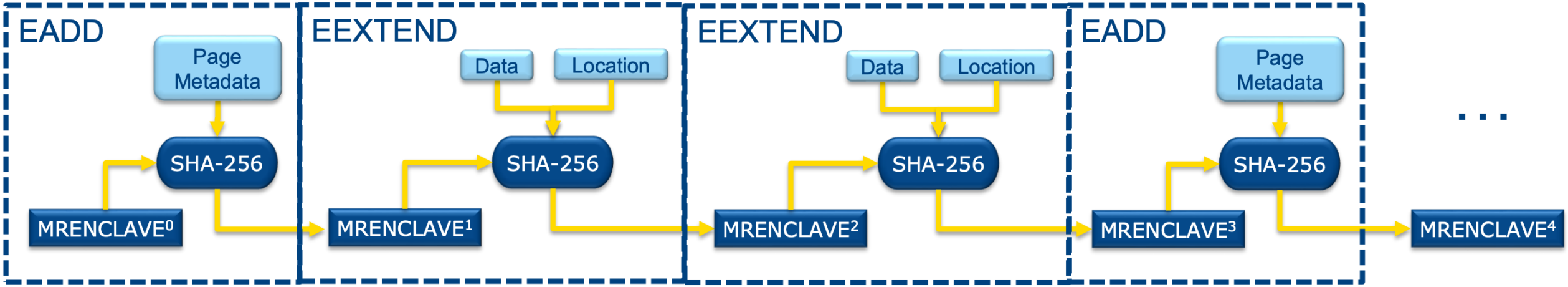
- Add page (EADD)
- Measure (EEXTEND)



Enclave Measurement

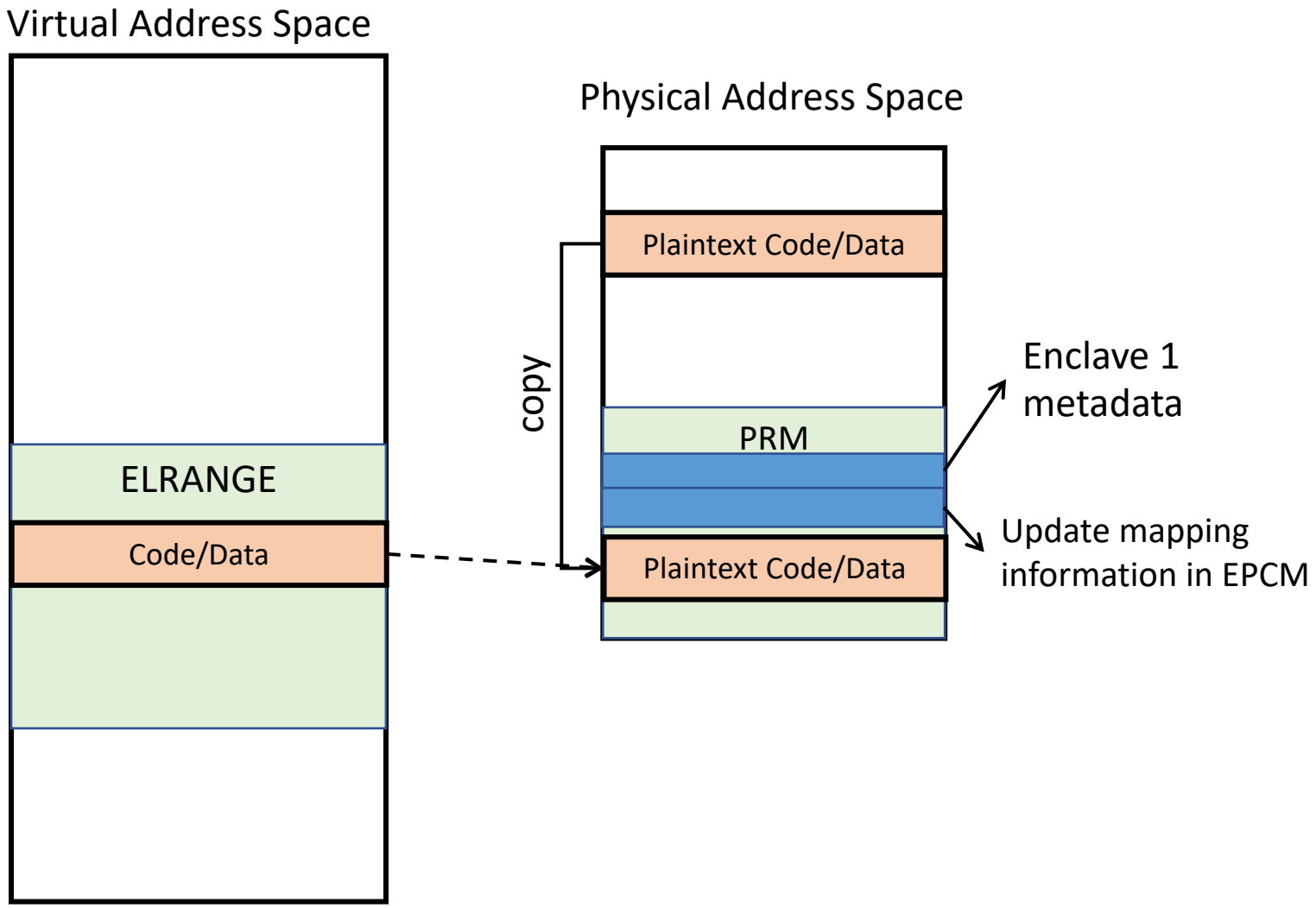
- Hardware generates a cryptographic log of the build process
  - Code, data, stack, and heap contents
  - Location of each page within the enclave
  - Security attributes (e.g., page permissions) and enclave capabilities

- Enclave identity (MRENCLAVE) is a 256-bit digest of the log that represents the enclave



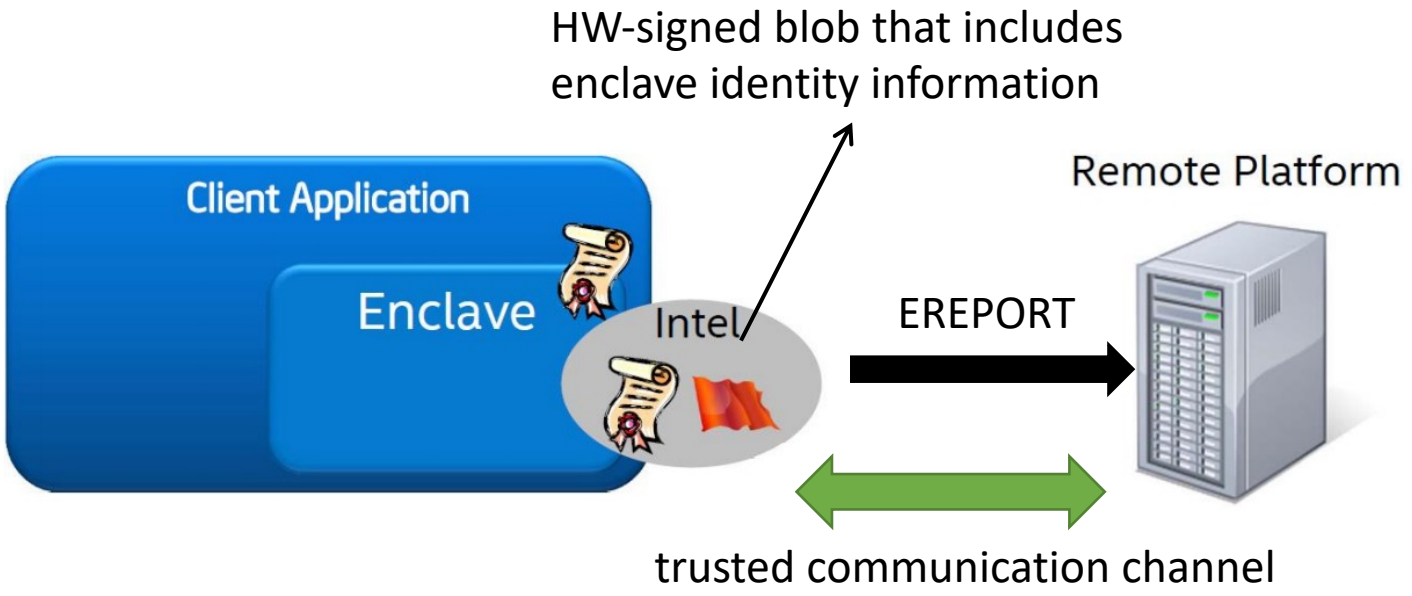
Enclave Initialization

- Add page (EADD)
- Measure (EEXTEND)
- Init (EINIT)
  - Finalize measurement
- Active (EENTER)
  - Switch to enclave mode



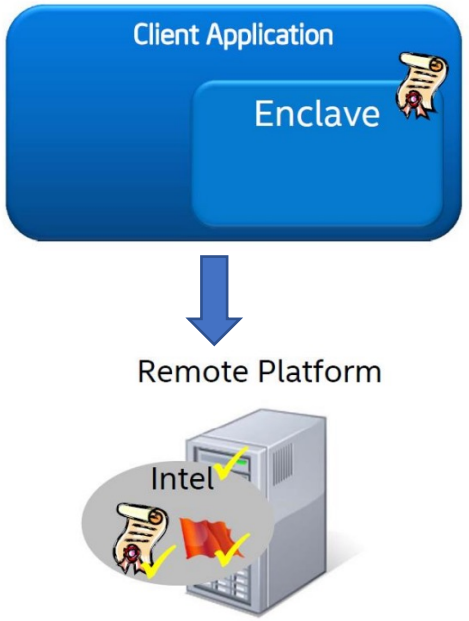
Enclave Attestation and Sealing

- HW based attestation provides evidence that “this is the right application executing on an authentic platform” (approach similar to secure boot attestation)

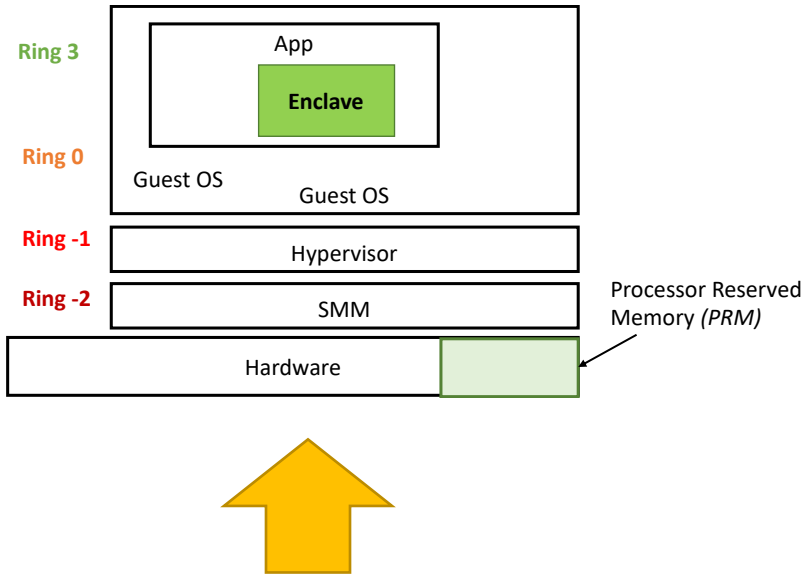


Intel SGX Security Mechanisms

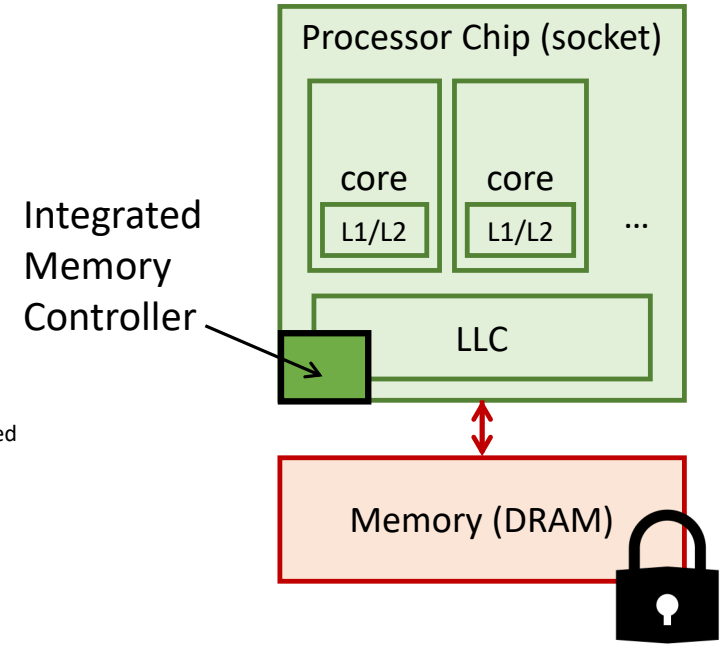
Attestation



Isolation

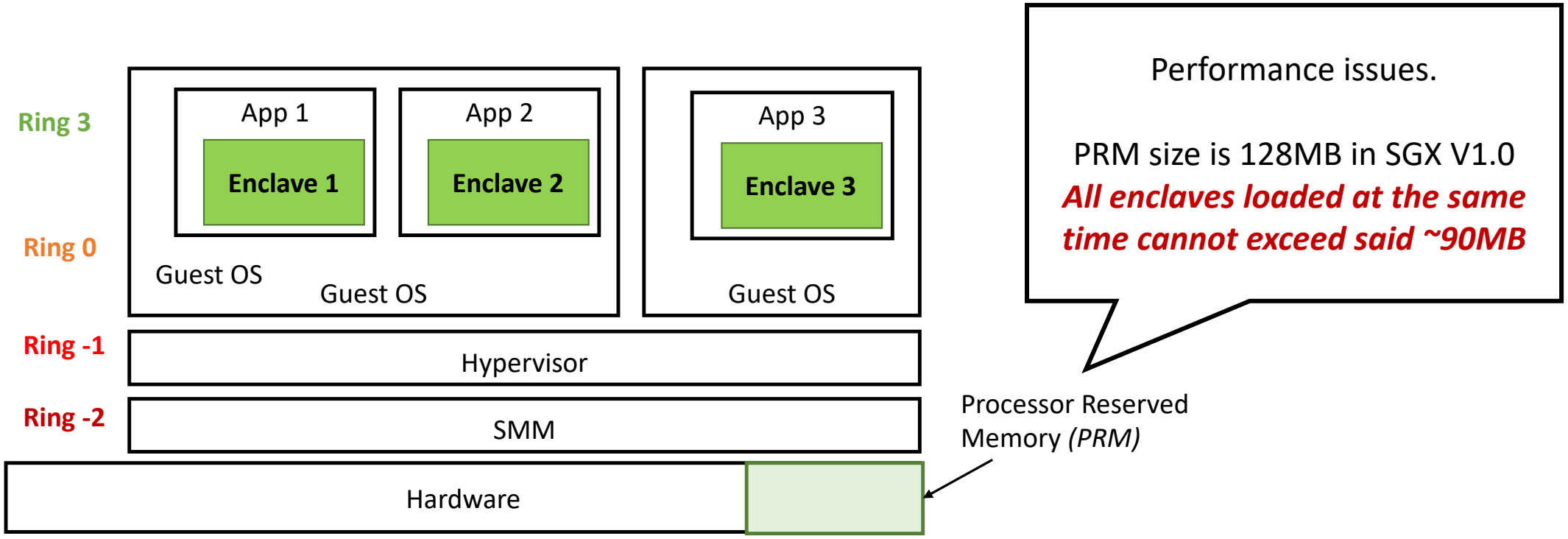


DRAM Protection

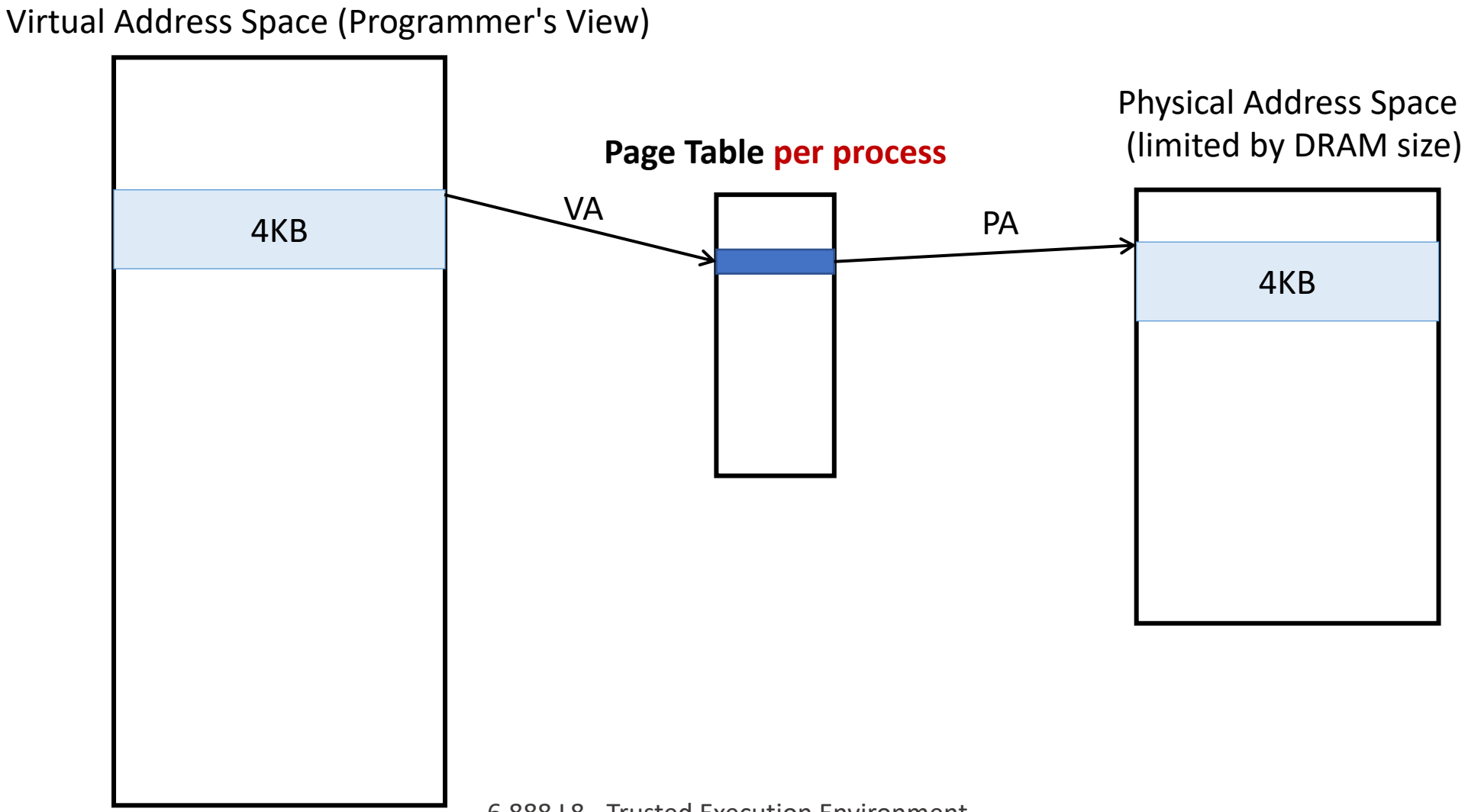


SGX Access Control

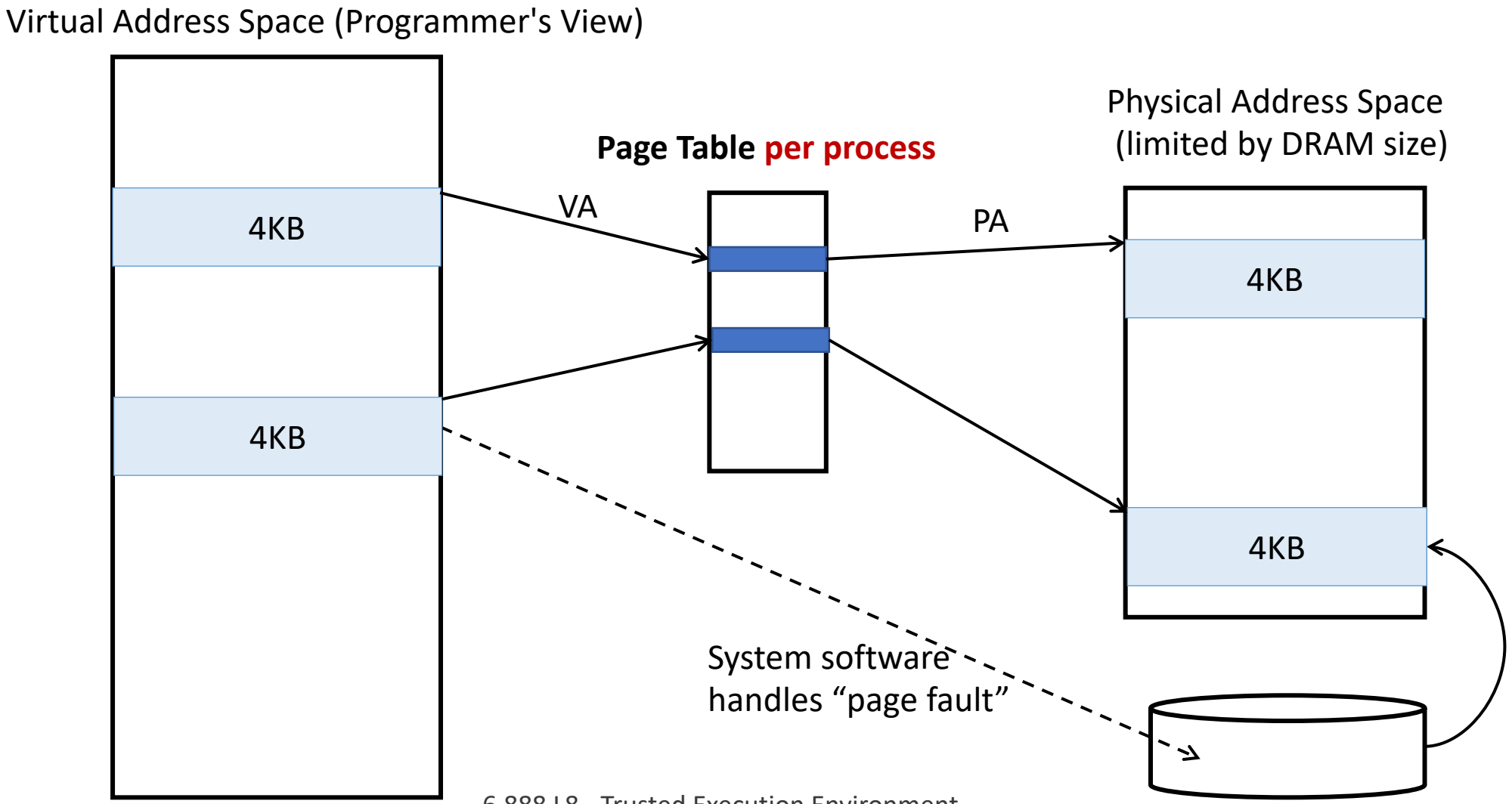
- Assume software attestation is done
- Can have multiple enclaves



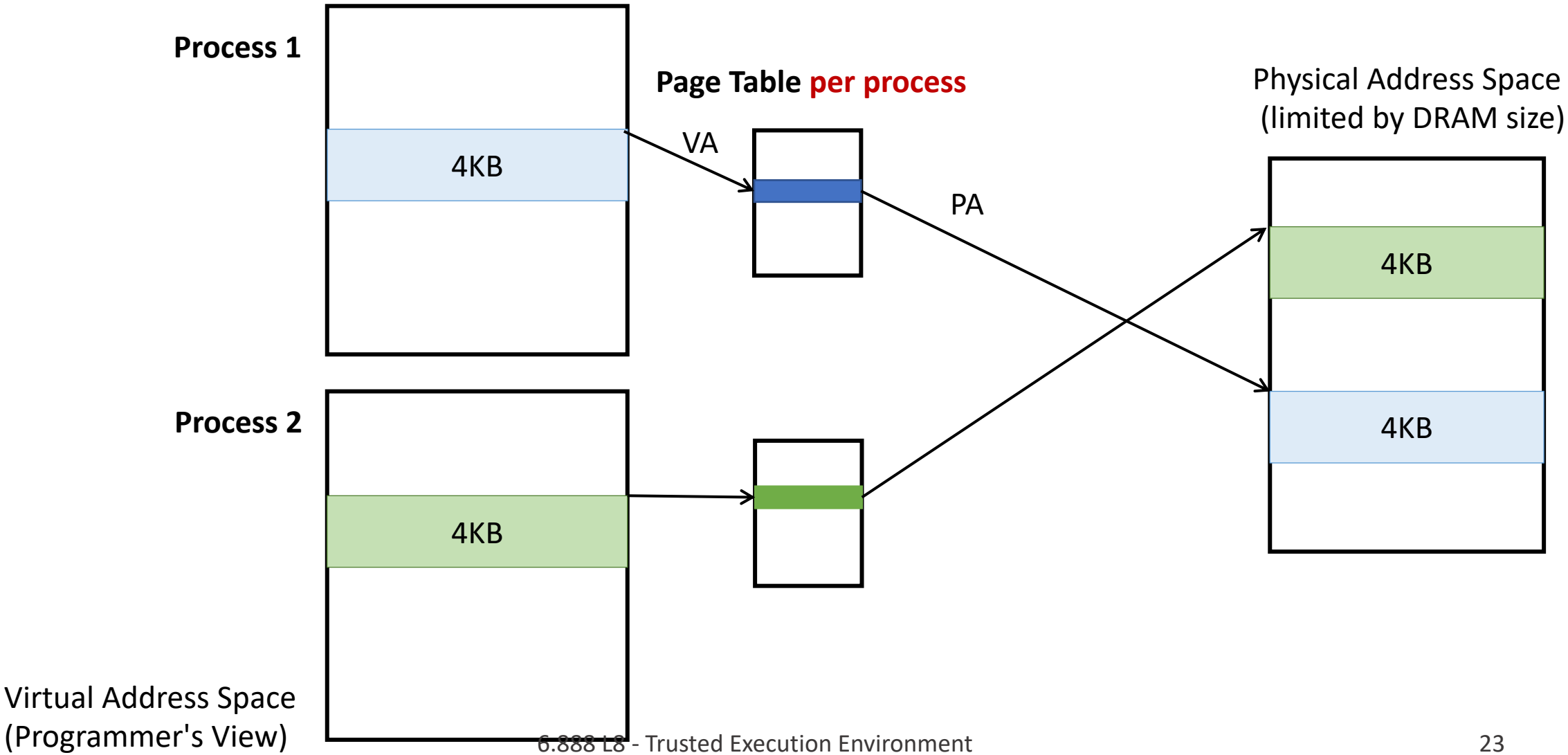
Recap: Virtual and Physical Address



Recap: Virtual and Physical Address

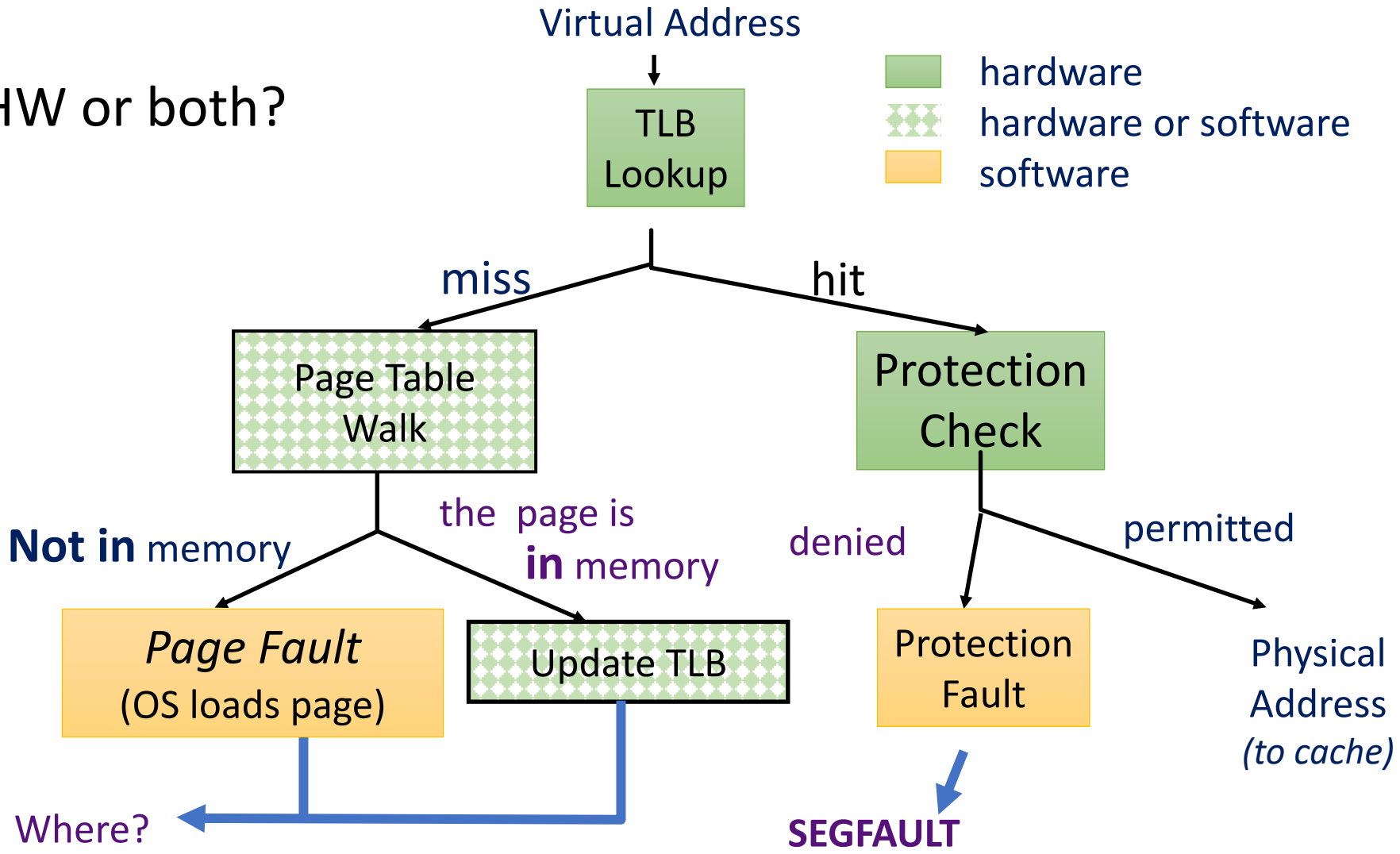


Recap: Virtual and Physical Address

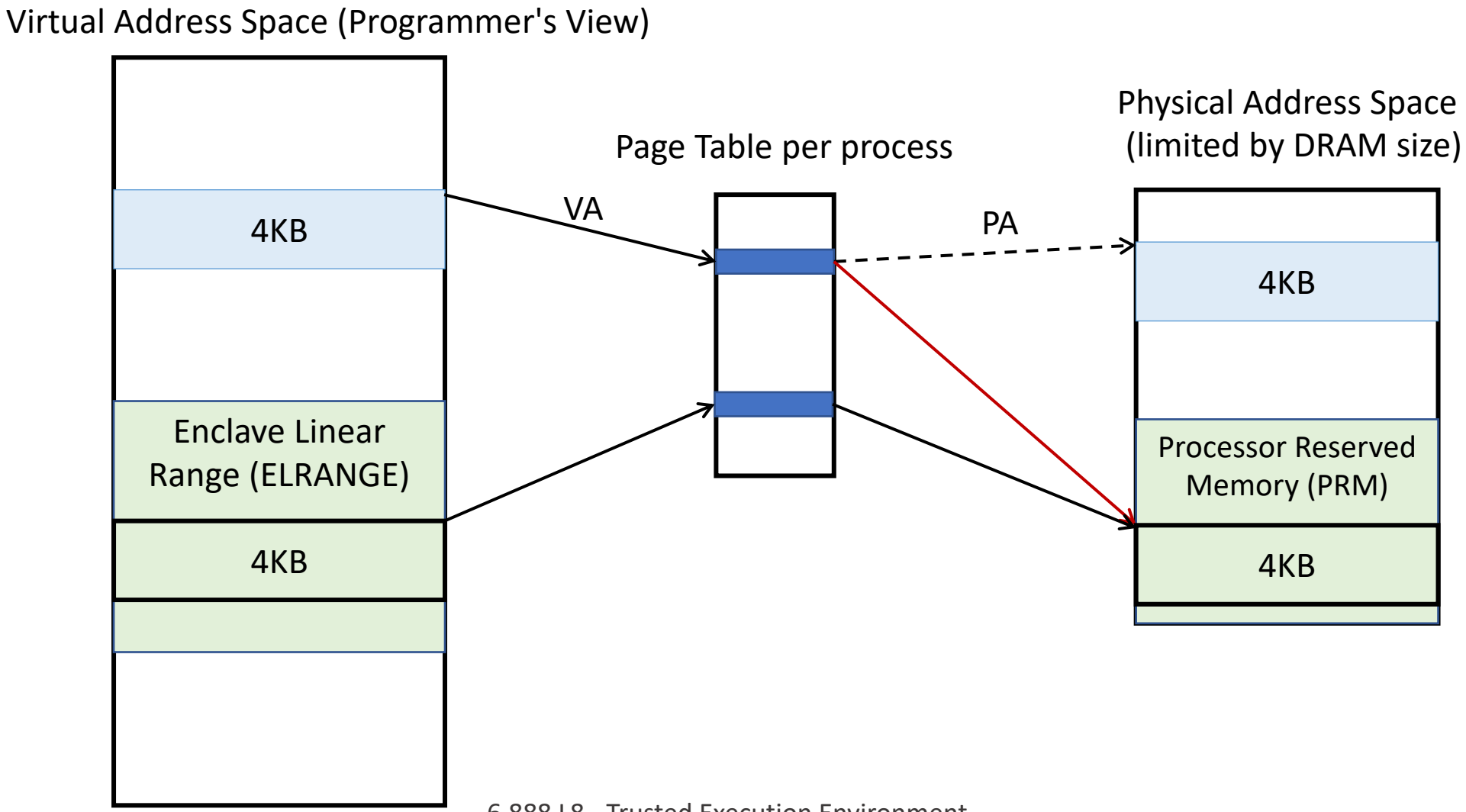


Address Translation

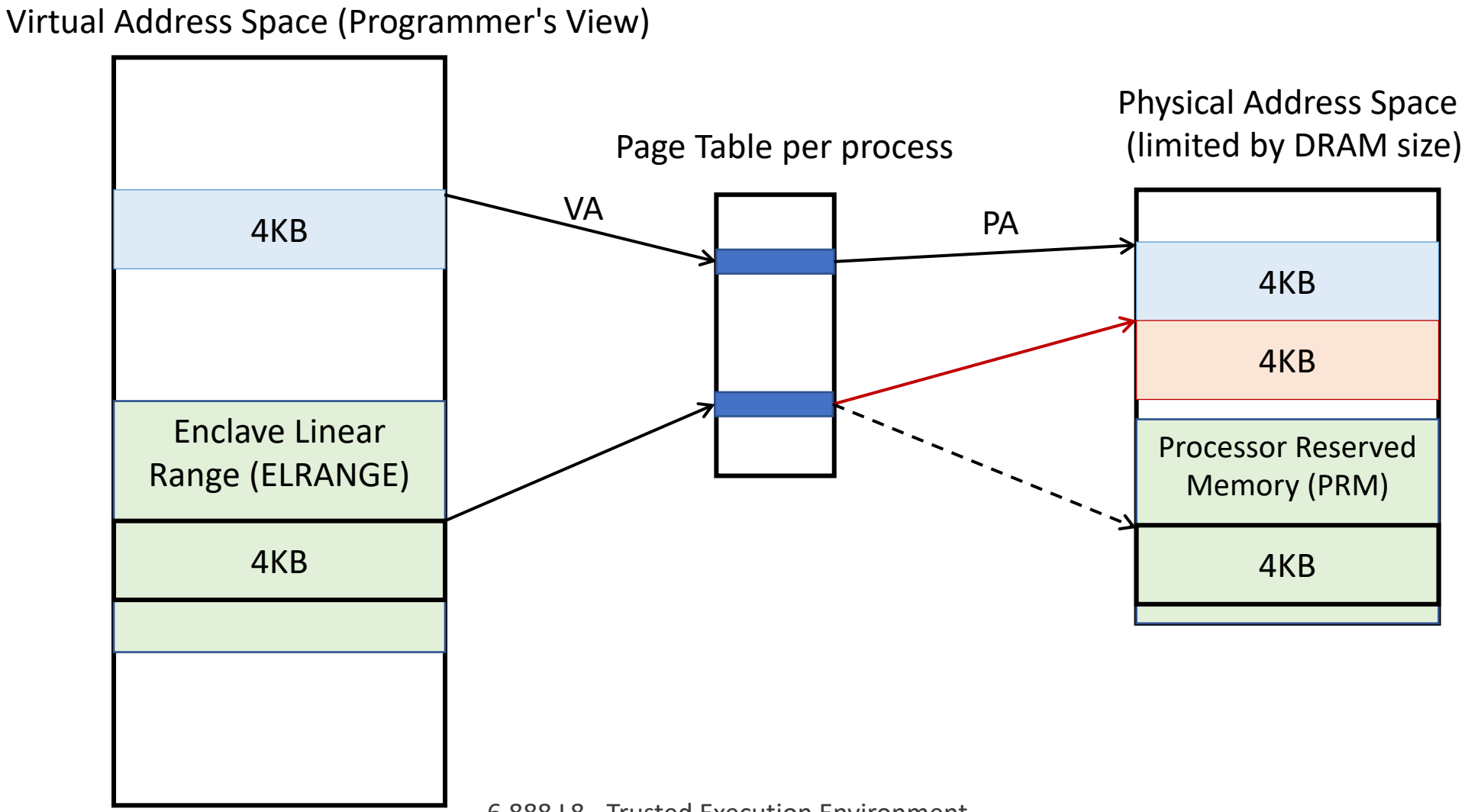
- SW or HW or both?



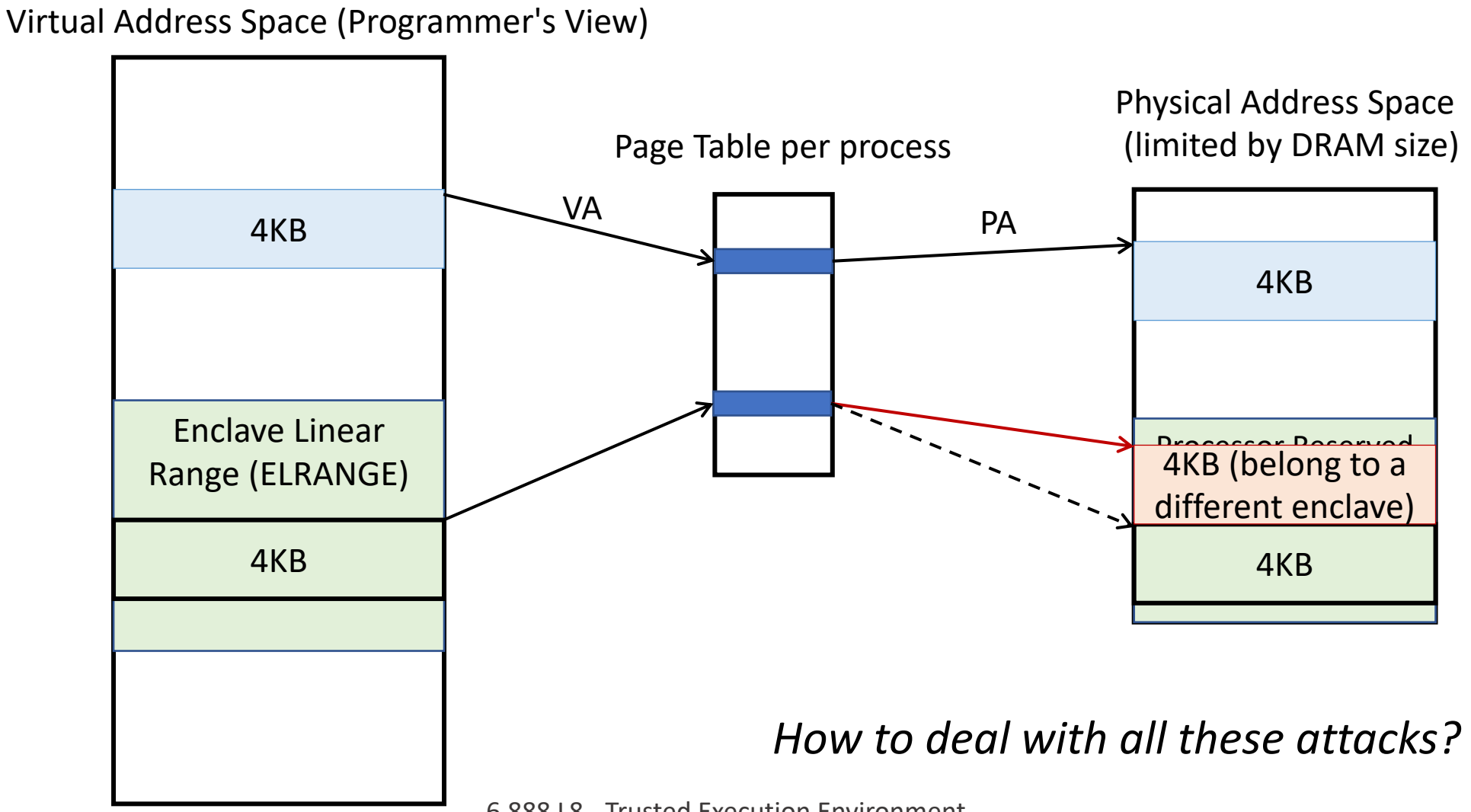
Malicious Address Translation



Malicious Address Translation

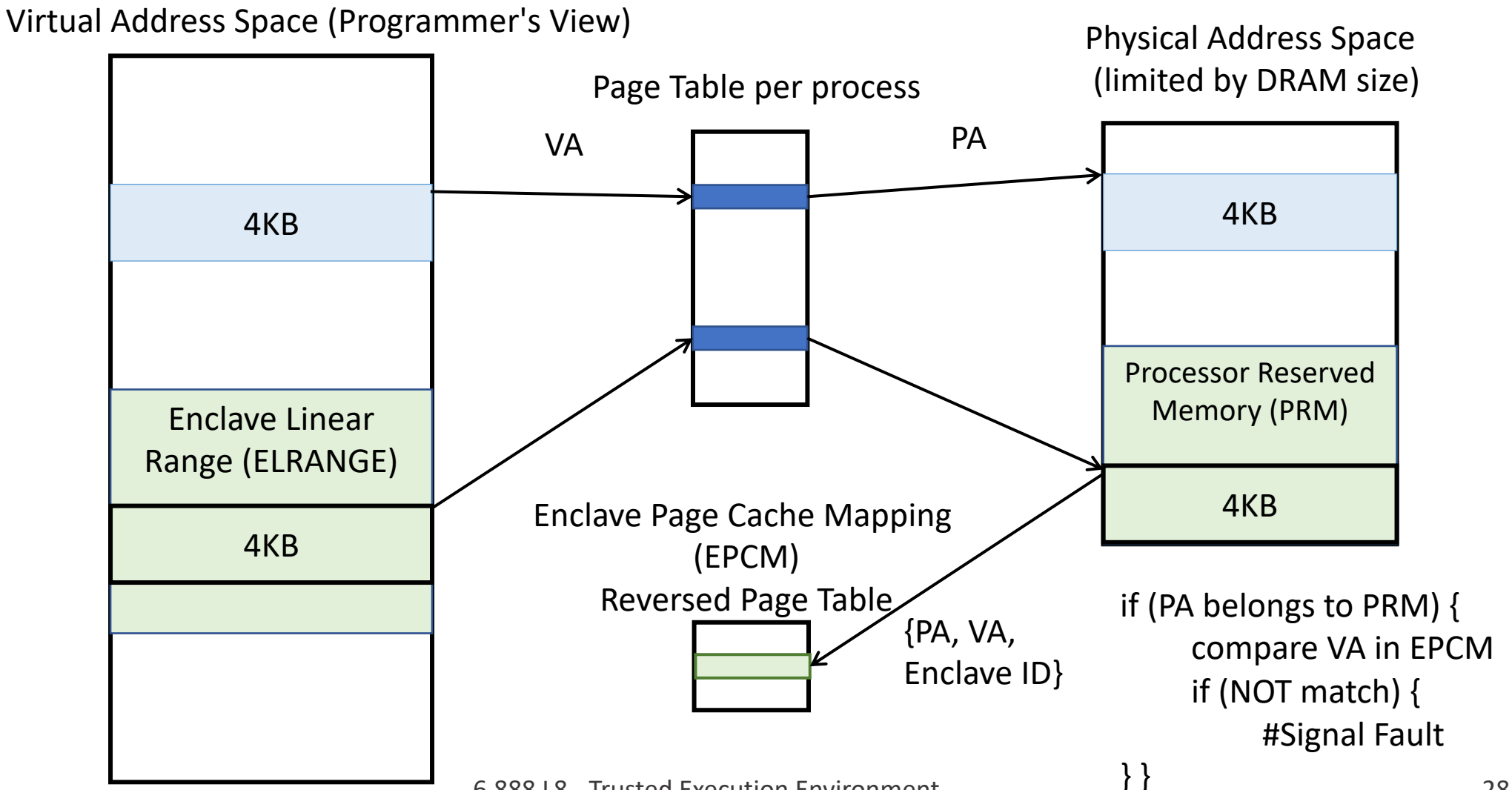


Malicious Address Translation



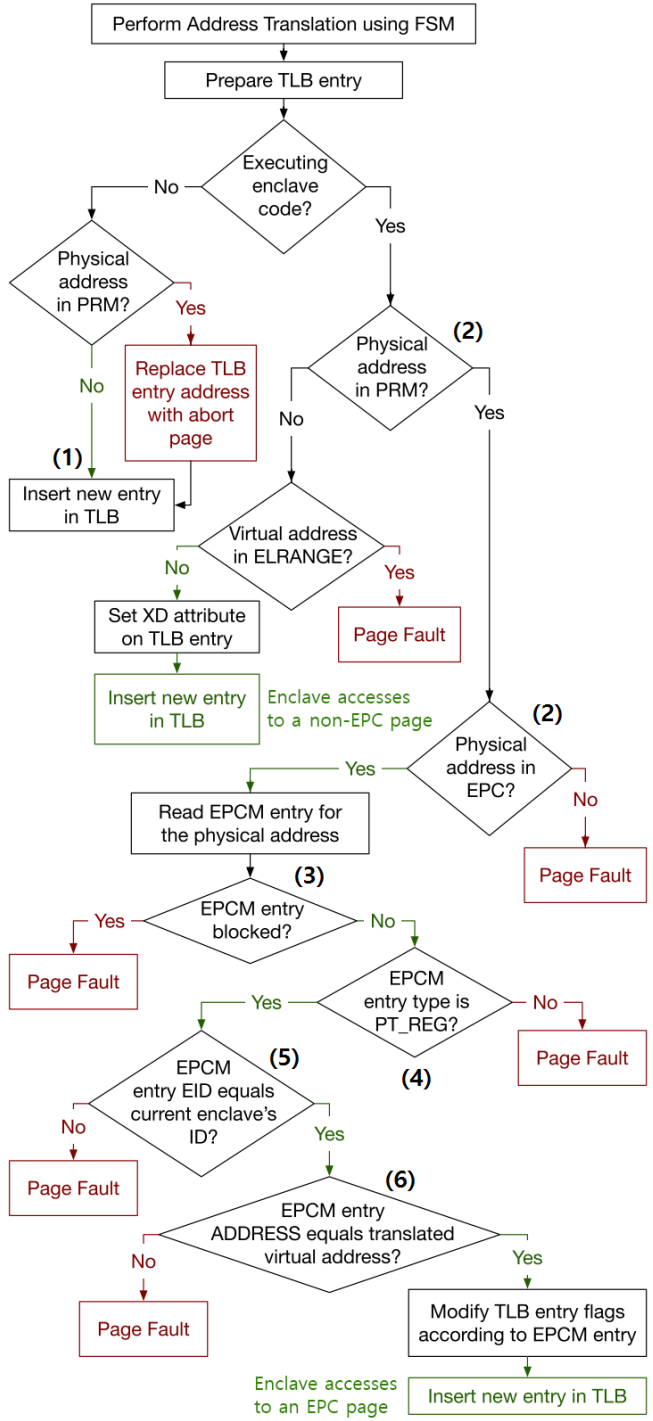
How to deal with all these attacks?

Enclave Page Mapping Information



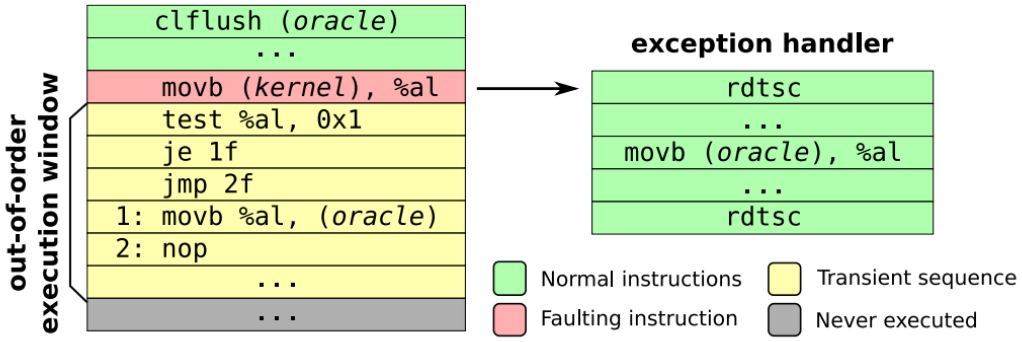
SGX Address Translation Attack Protection

- AMD
  - AMD-SEV uses a different mechanism
  - AMD-SEV-SNP adds a similar feature to have reversed page tables



Attacks on Intel SGX

- Page access side channels
  - Xu et al. “Controlled-channel attacks: Deterministic side channels for untrusted operating systems,” S&P’15
- L1FT/Foreshadow



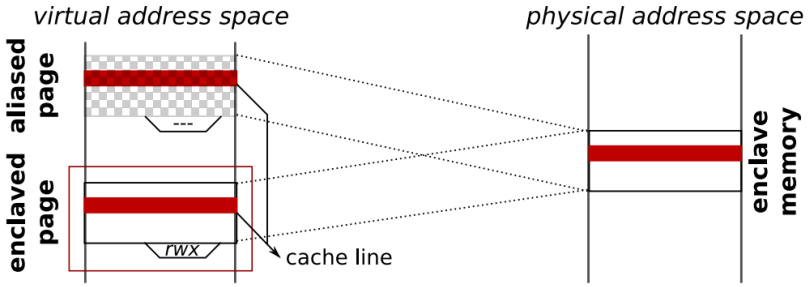
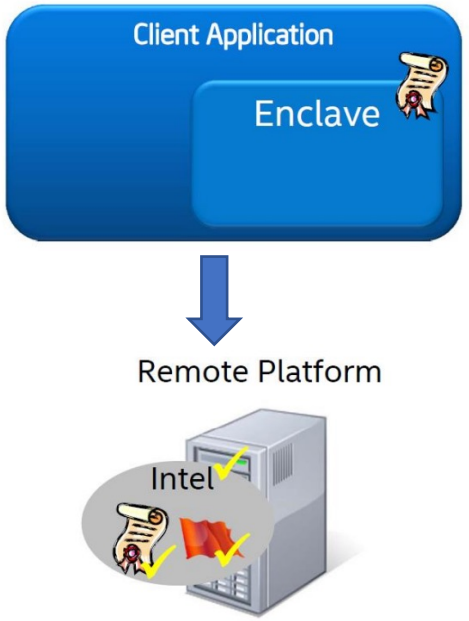


Figure 3: The physical enclave secret is mapped to an inaccessible virtual address for transient dereference.

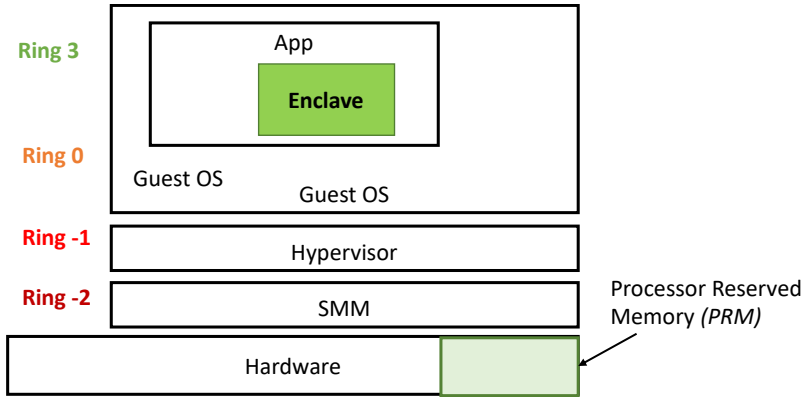
- Single-Step/Zero-Step

Intel SGX Security Mechanisms

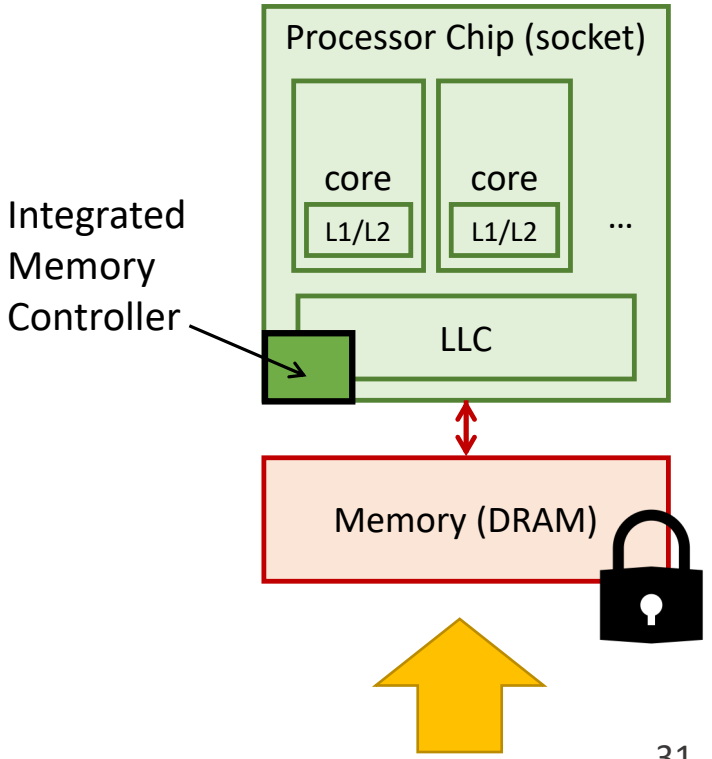
Attestation



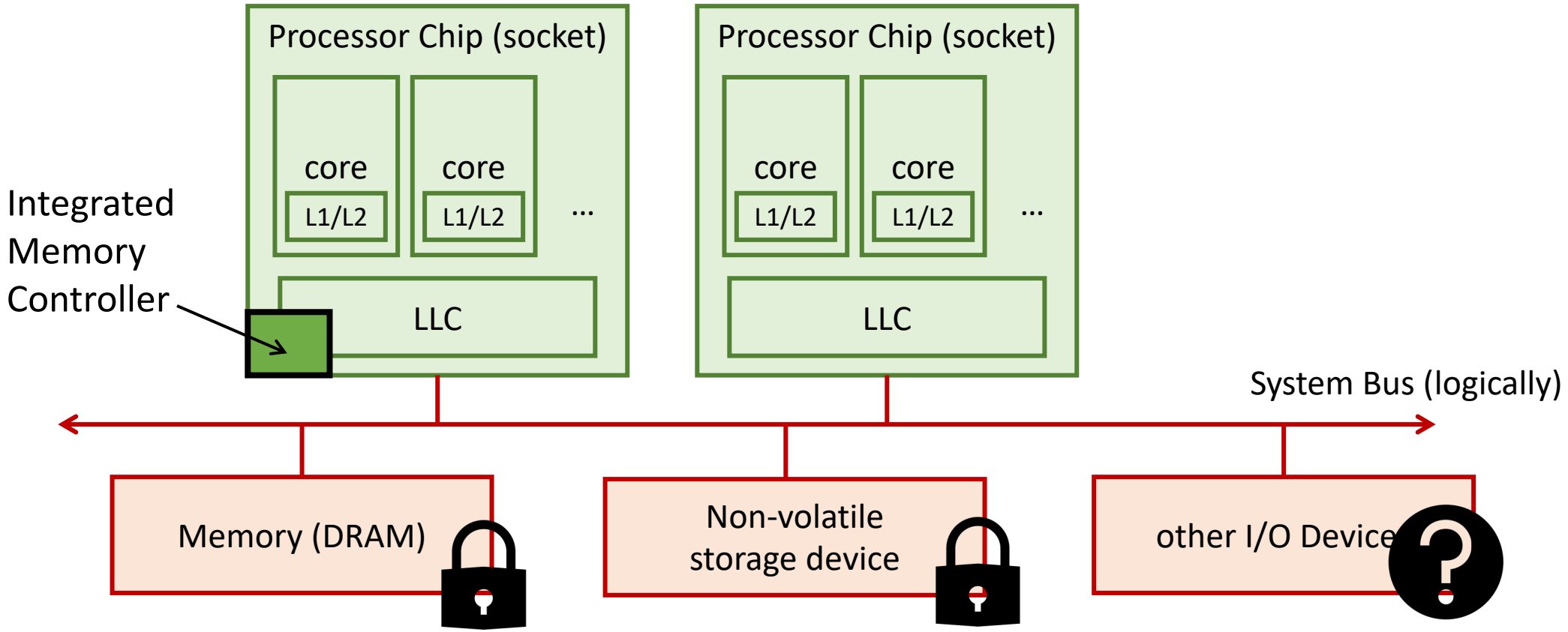
Isolation



DRAM Protection



Protect Memory



Memory Encryption Engine (MEE)

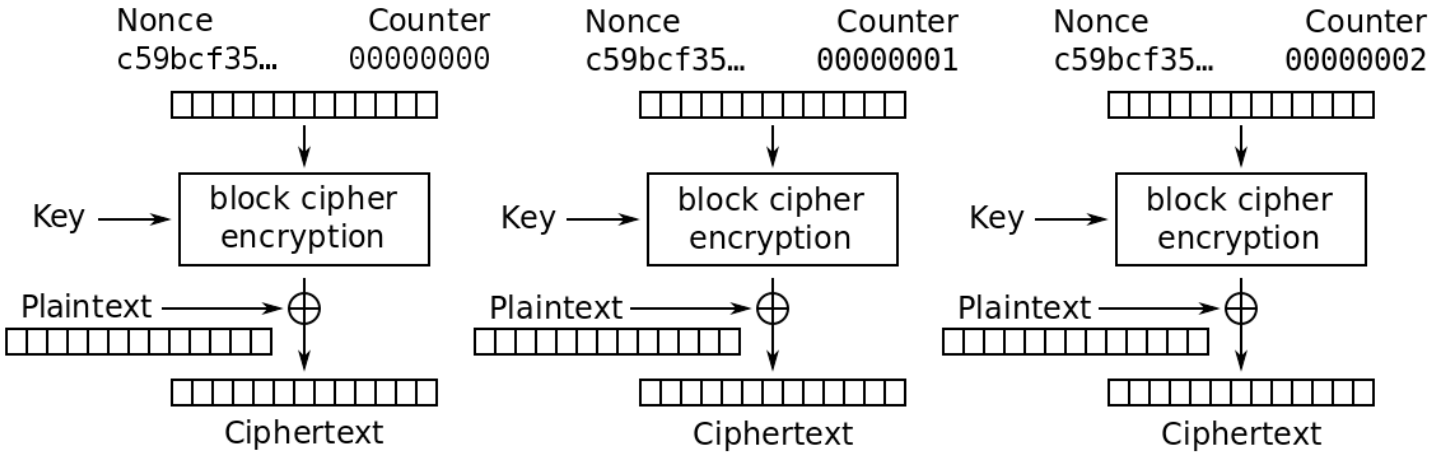
- Confidentiality:
  - DATA written to the DRAM cannot be distinguished from random data.

- Integrity + freshness:
  - DATA read back from DRAM to LLC is the same DATA that was most recently written from LLC to DRAM.

What attacks can be mitigated?
Rowhammer? Bus tapping? Side channels on address access?

Confidentiality

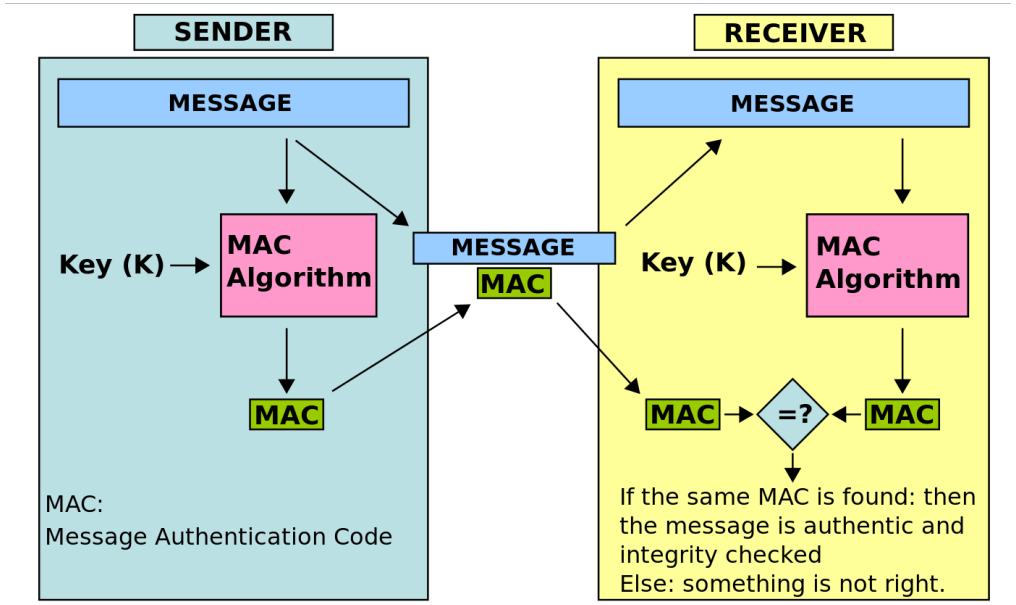
- AES 128-CTR mode



Counter (CTR) mode encryption

Message Authentication Code (MAC)

- Hash(plaintext)
- Keyed Hash
  - MAC = Hash(ciphertext || key)
- Freshness
  - MAC = Hash(ciphertext || key || nounce)

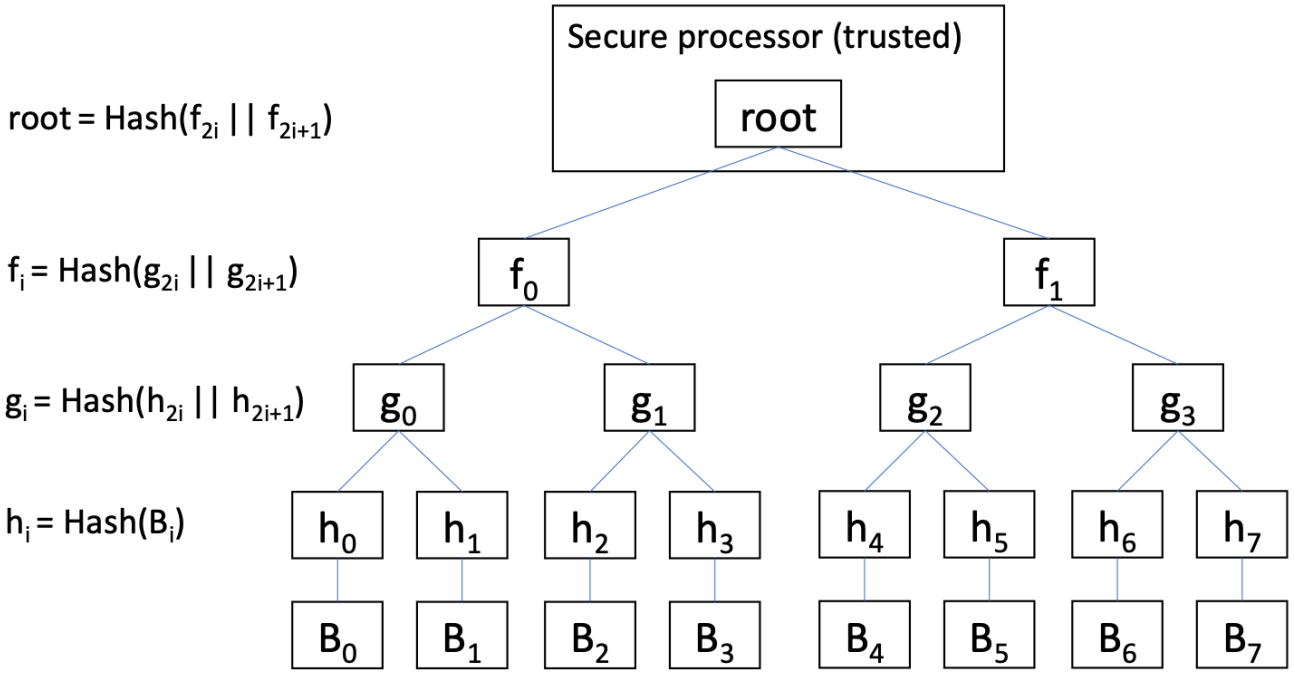


Integrity Storage Problem

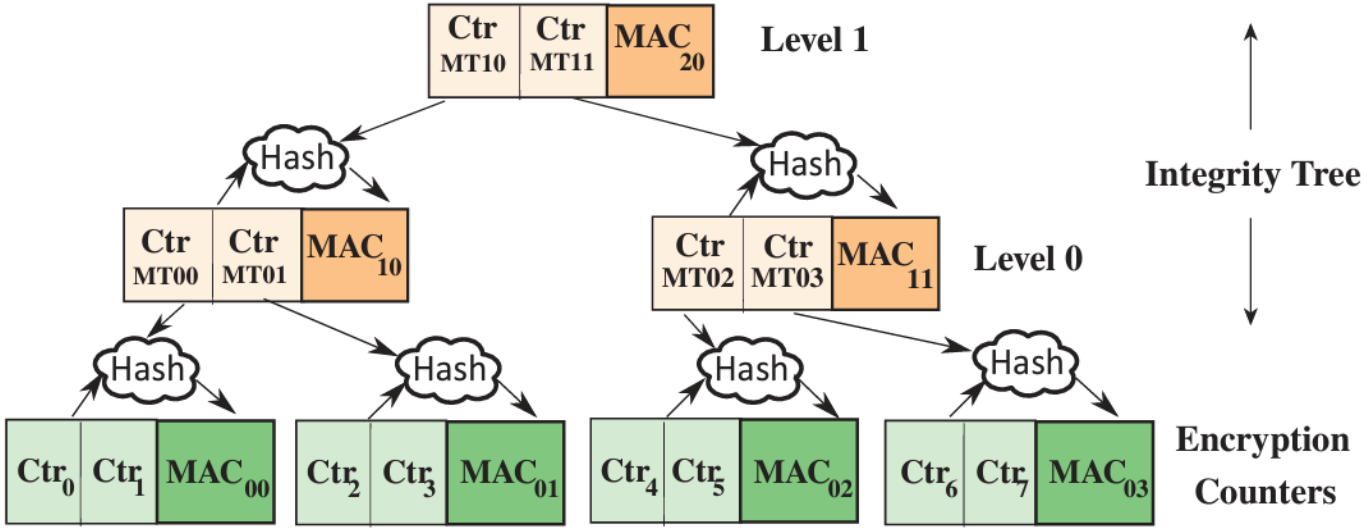
- For each cache line: {ciphertext + CTR + MAC}
  - MAC 56 bits
  - CTR 56 bits
- Can we store all the three components off-chip?
- Problem: if store CTR on-chip → high on-chip storage requirement

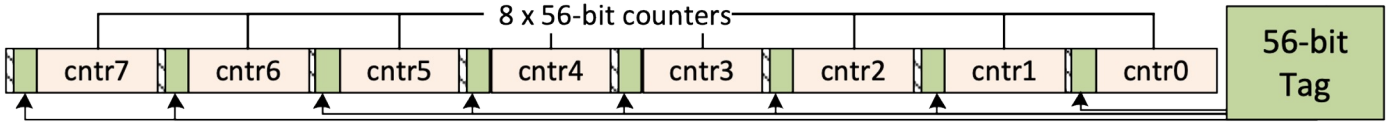
Operations on Merkle Tree

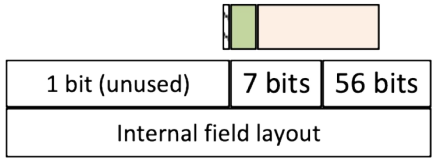
- Only need to store the root node on chip
- How to verify block B1?
- Write to block B3?



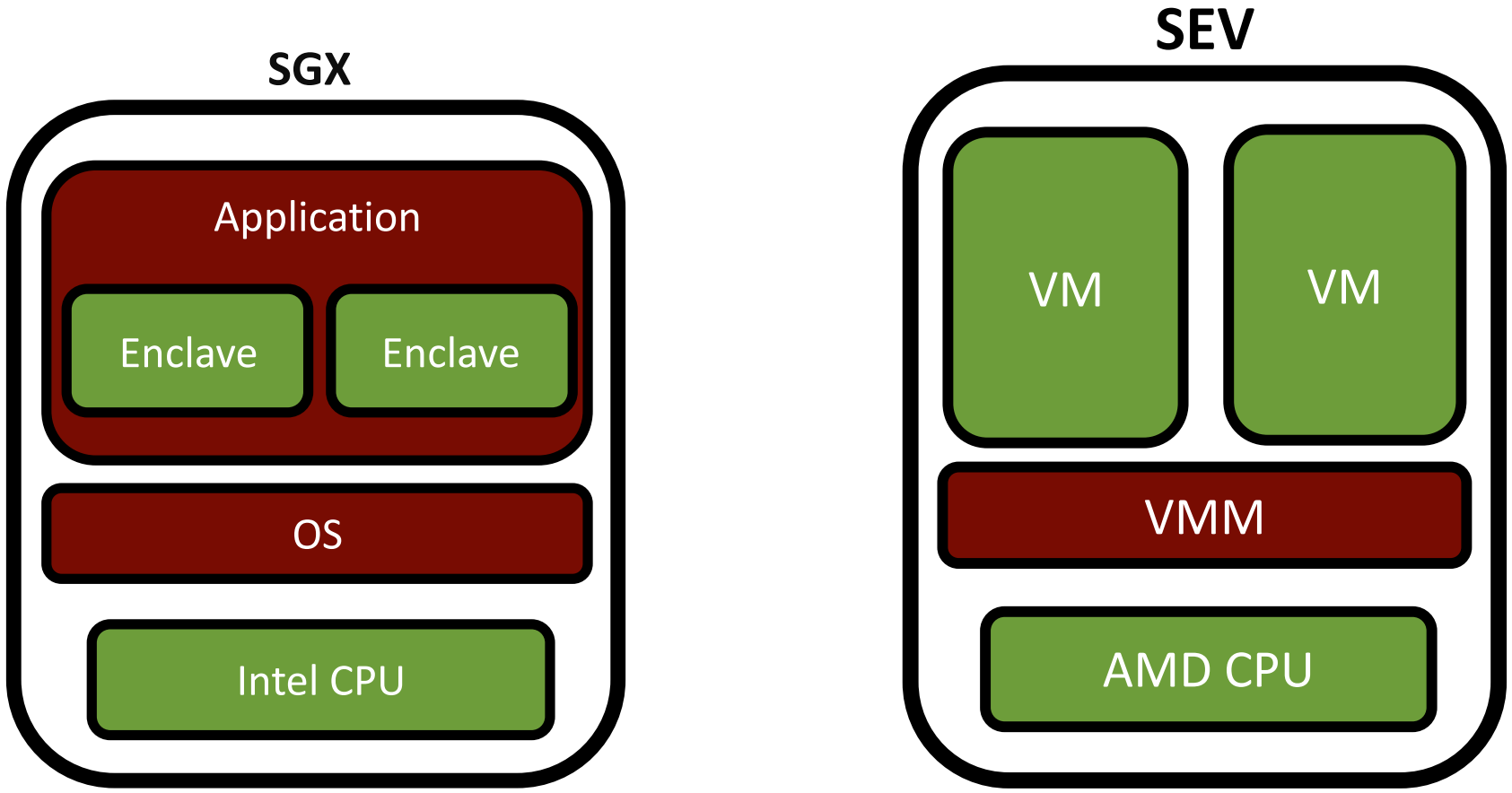
Counter Integrity Tree



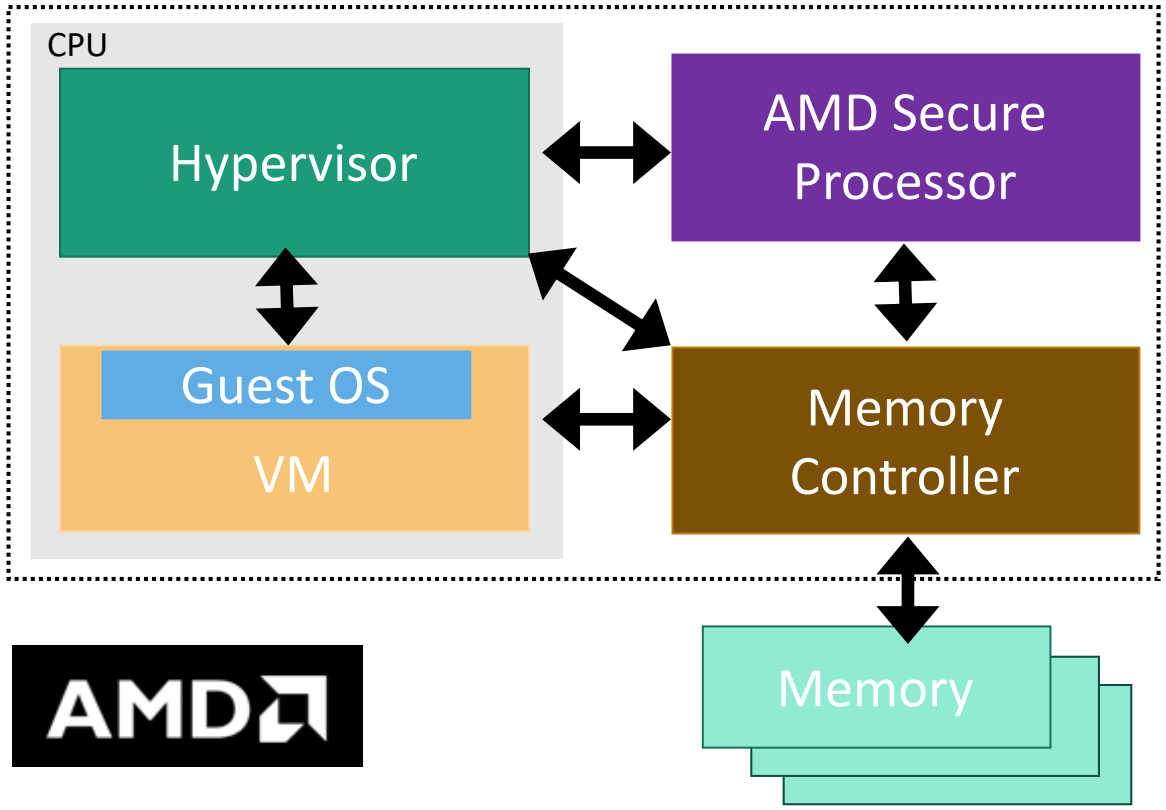




Intel SGX v.s. AMD SEV

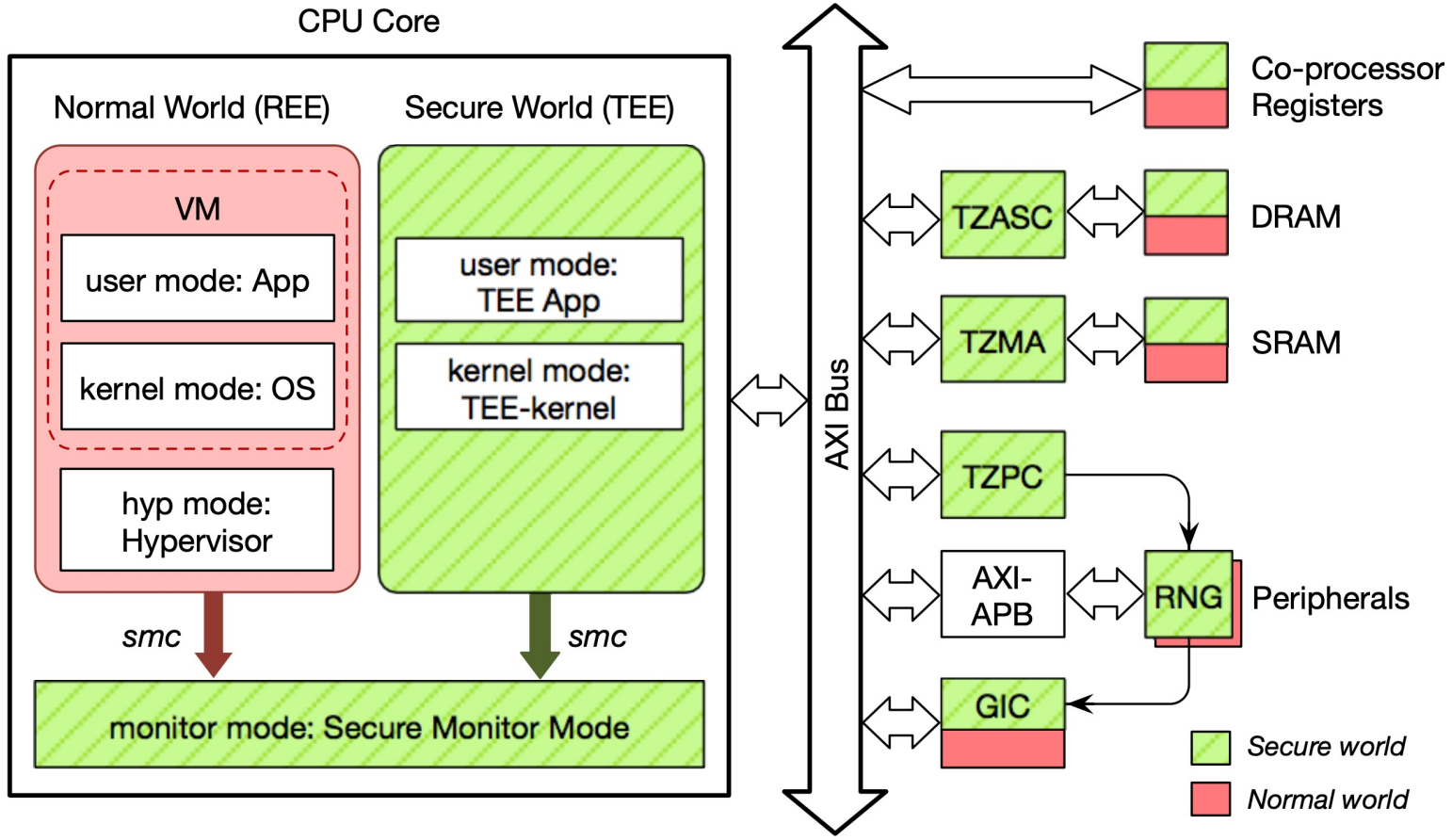


AMD SEV



- CPU
- AMD Secure Processor
  - Manages AES Keys
  - Handle SEV API
- Memory Controller
  - Memory Encryption Engine(MEE)
  - AES encryption/decryption

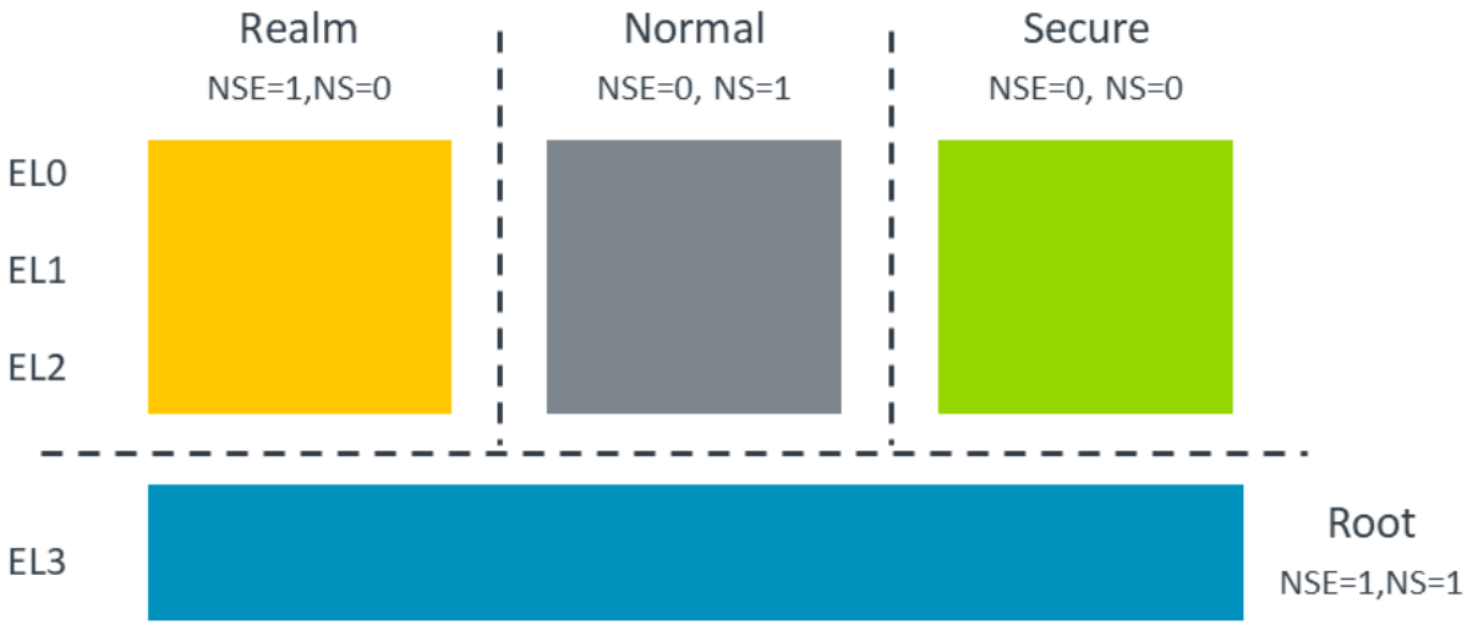
Arm TrustZone



from Hua et al. vTZ: Virtualizing ARM TrustZone. Usenix'17

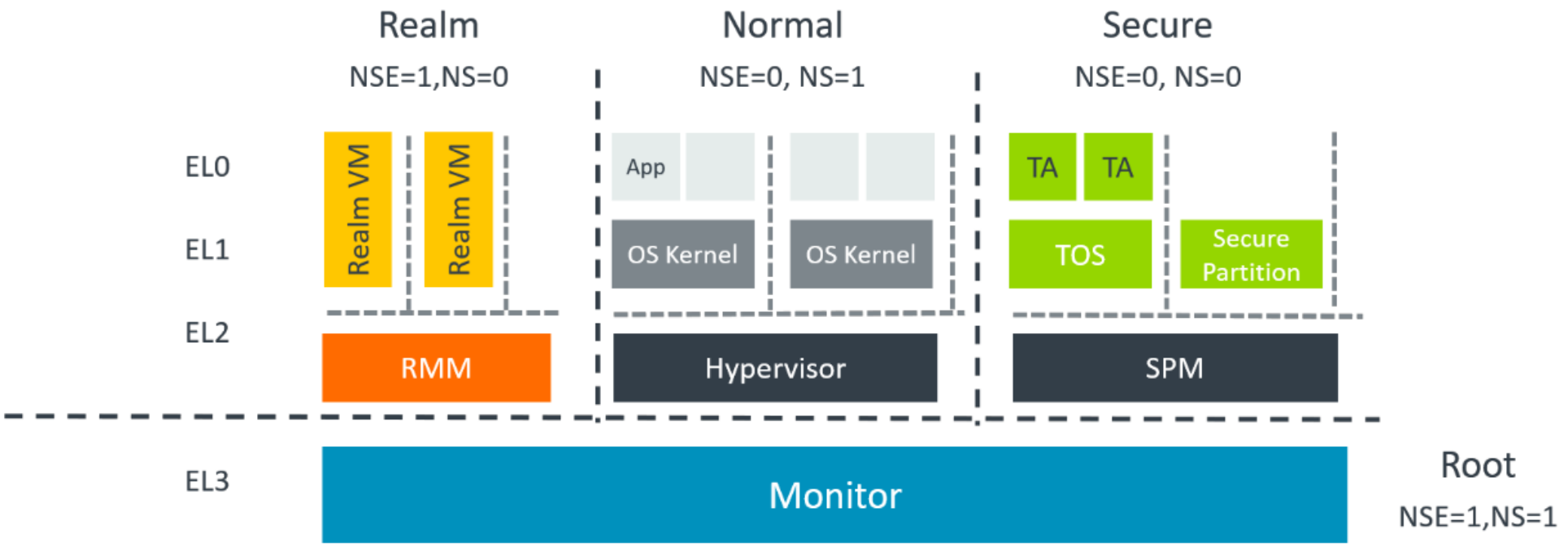
ARM CCA

- ARM Confidential Computing Architecture



Introducing Arm Confidential Compute Architecture, Issue 2, 2022

ARM CCA


Realm
NSE=1,NS=0
Normal
NSE=0, NS=1
Secure
NSE=0, NS=0
EL0
EL1
EL2
EL3
Realm VM
Realm VM
App
OS Kernel
OS Kernel
TA
TA
TOS
Secure Partition
RMM
Hypervisor
SPM
Monitor
Root
NSE=1,NS=1

Summary

- What is trusted execution environment/confidential computation?
- Main security mechanisms
- Multiple commercialized design
  - Intel SGX, AMD SEV, ARM CCA
  - Keystone, Sanctum, Penglai, etc