CASPER

CS773: Computer Architecture for Performance and Security

Lecture 6: 10K Feet View on the World of Secure Processors (Trusted Execution Environments)

https://www.cse.iitb.ac.in/~biswa/

Trust

Trusted Computing Base (TCB): Set of software and hardware units that are assumed to be secure.

Trusted Execution environment (TEE): A computing environment that facilitates creation/running of secure code/process (enclave as per Intel SGX)

Who provides TEE? Who is the boss here?

Root of Trust (Security monitor)

OS, what if the OS is malicious or hacked ☹

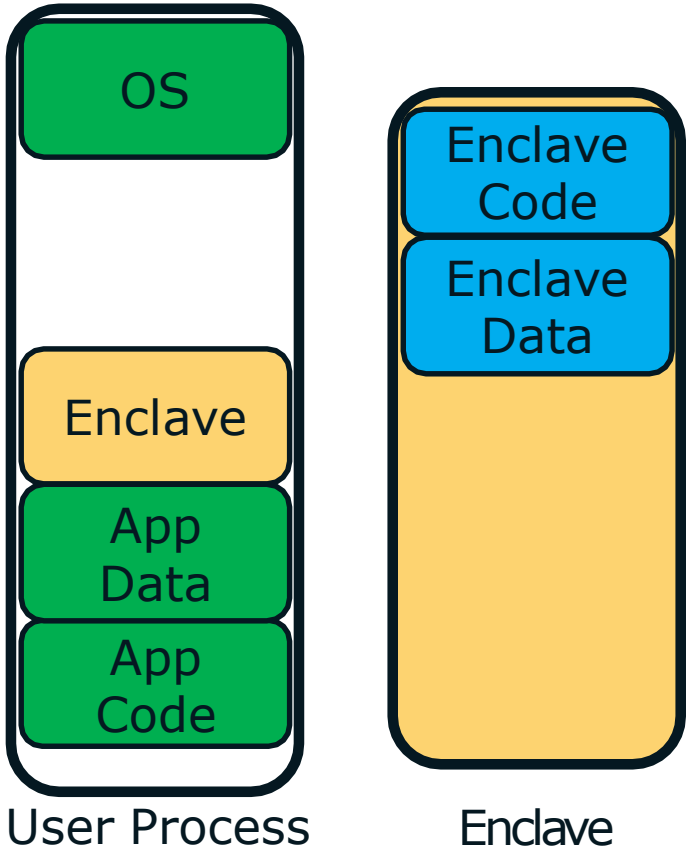
Root of trust: Fully trustworthy

So, we need a trusted platform module (TPM): can be software, hardware, firmware (code stored in ROM)

What is its job?

- Boot the system and verify BIOS is trustworthy and is not tampered. Compare a known hash with the hash generated by the BIOS
- It can be done for other entities like OS loader, ….. to build a chain of trust. The final hash is the hash of entire TCB.

Intel Software Guard Extensions (SGX)



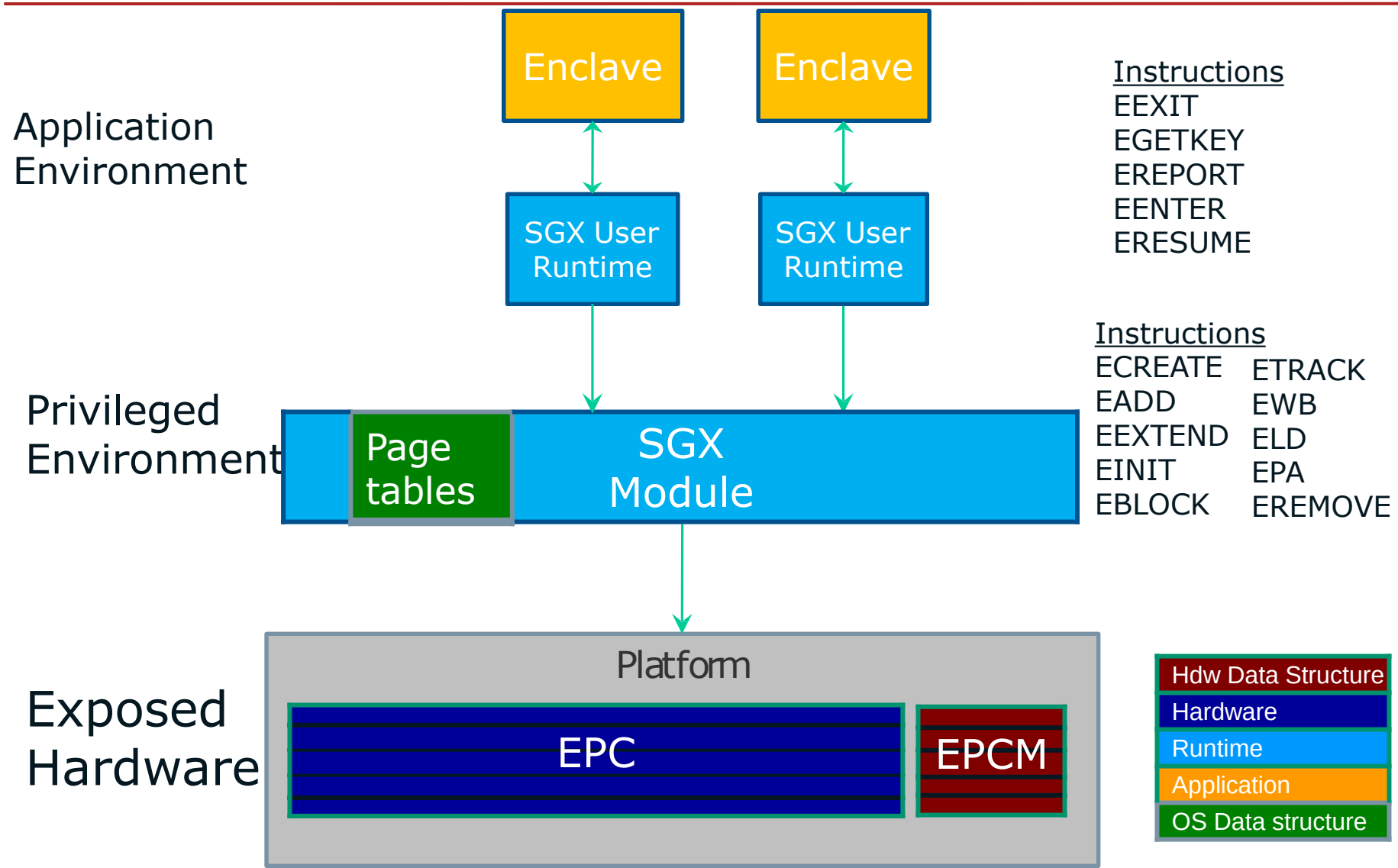
With its own code and data

Provide Confidentiality

Provide integrity

With controlled entry points

The Hw-Sw Picture



Data Sealing

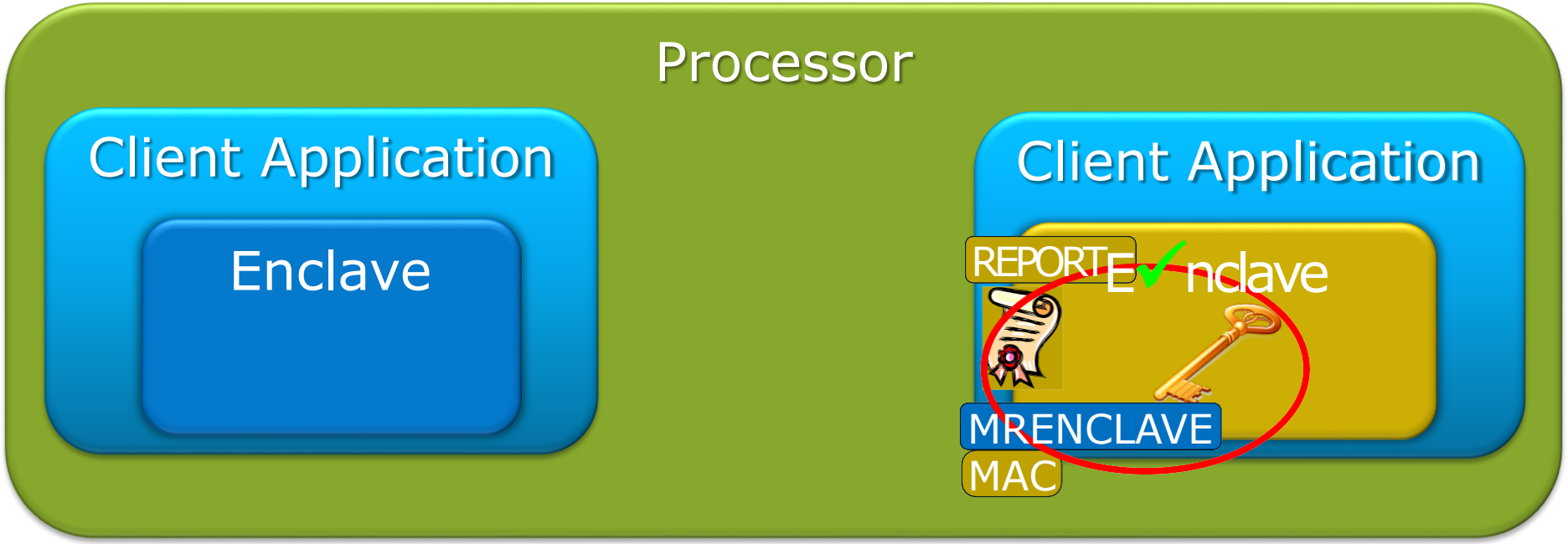
While accessing the untrusted memory, the data stored is encrypted using a key provided by the CPU

Encrypted data blocks – Sealed data blocks, can be decrypted on the same system only (MRENCLAVE policy per enclave)

MRSIGNER policy: Data sealed by one enclave can be unsealed by another enclave on the same system

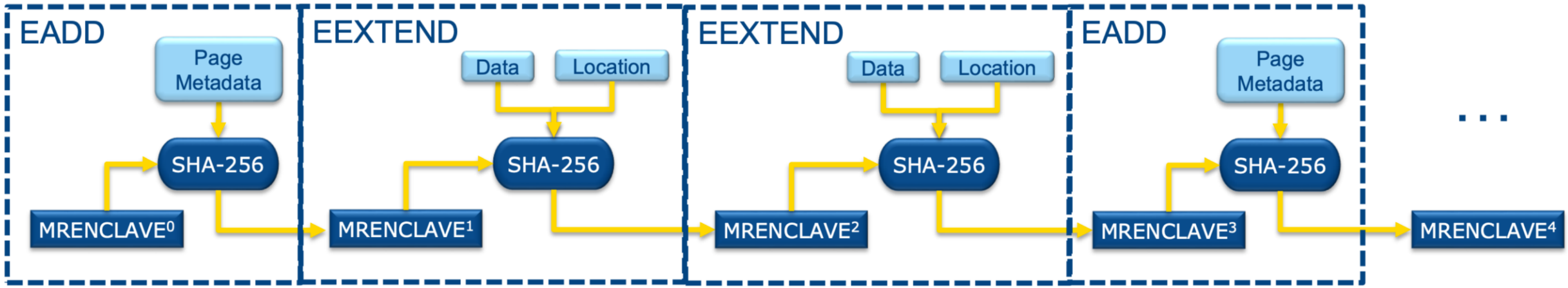
What if an outside world tries to access enclave data: Page abort ☺

Local Attestation and Sealing

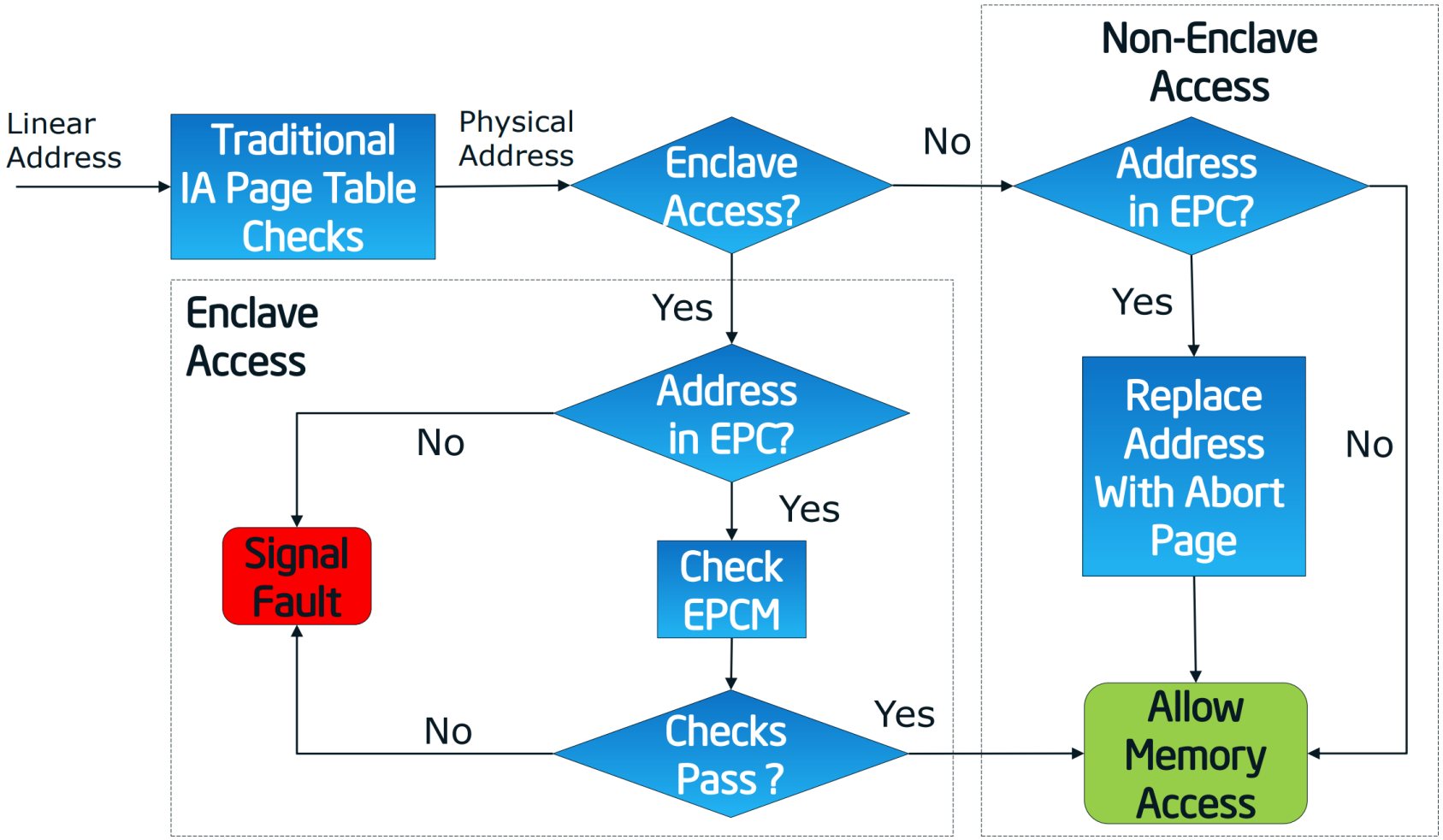


1. Verifying enclave sends its MRENCLAVE to reporting enclave
2. Reporting enclave creates a cryptographic REPORT that includes its MRENCLAVE
3. Verifying enclave obtains its REPORT key and verifies the authenticity of the REPORT

MRENCLAVE and the key

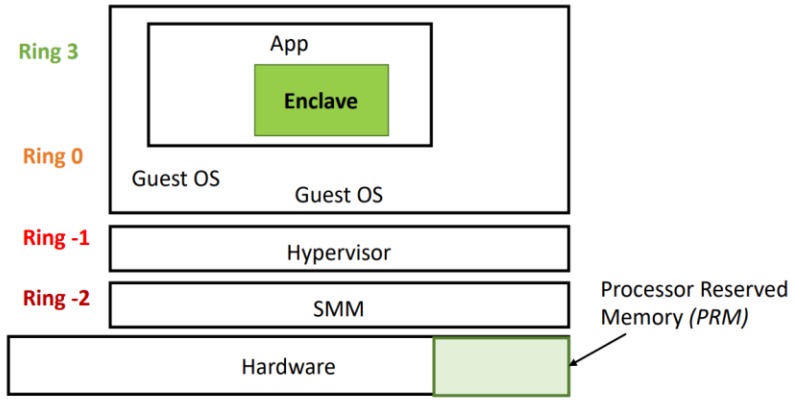


Access Flow

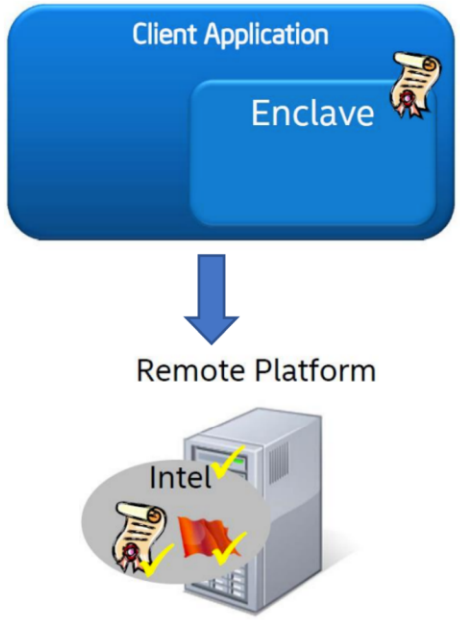

Linear Address
Traditional IA Page Table Checks
Physical Address
Enclave Access?
No
Non-Enclave Access
Address in EPC?
Yes
Replace Address With Abort Page
No
Enclave Access
Yes
Address in EPC?
No
Signal Fault
Yes
Check EPCM
Checks Pass ?
No
Yes
Allow Memory Access

Intel SGX in Summary

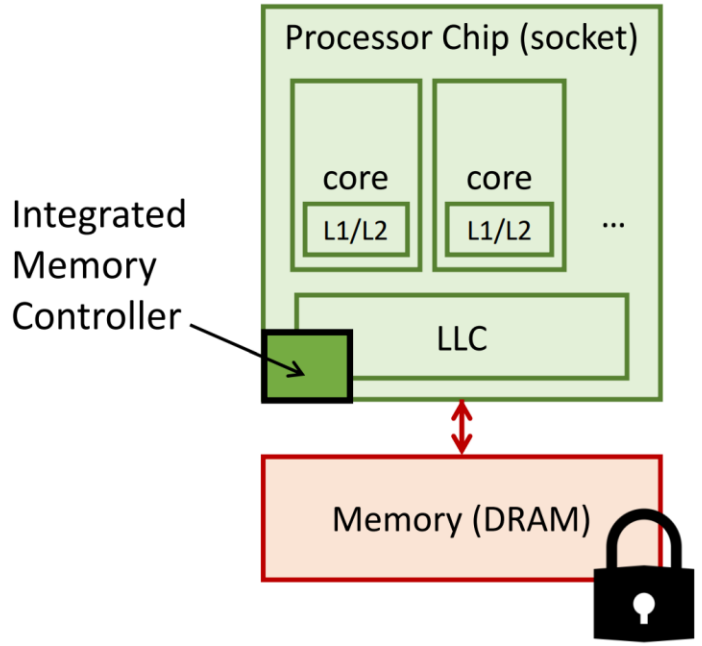
Isolation



Attestation



DRAM Protection



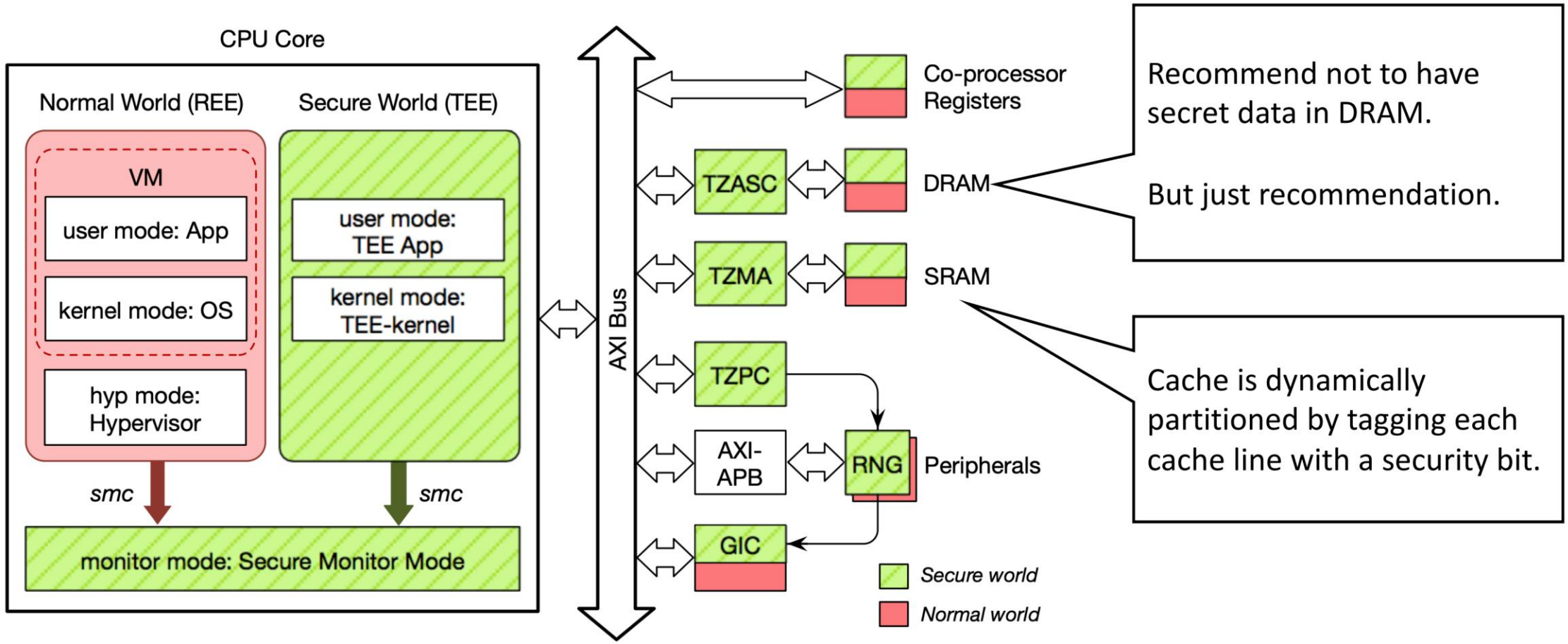
Intel SGX vs AMD SEV (Secure Encrypted Virtu..)

AMD SEV: Memory size limit: DRAM size
Intel SGX: Memory size limit: 128 to 256 MB

Intel attestation: Remote attestation
AMD attestation: Secure co-processor

Intel SGX: suited for small secure code
AMD SEV: Large enterprise apps

Arm Trustzone



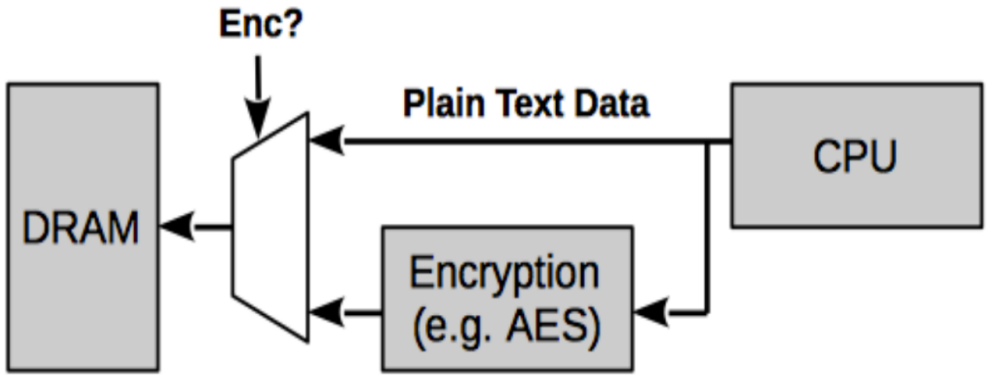
RISC-V based open TEE

Home Blog Docs Forum Subscribe

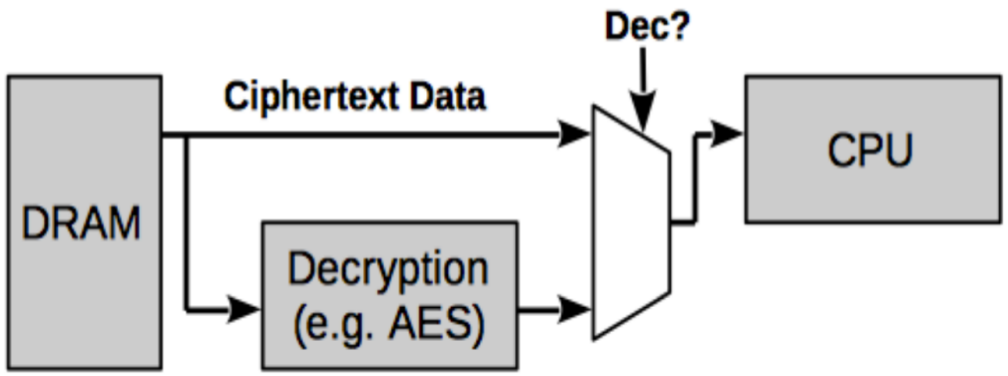
Keystone

An Open Framework for Architecting Trusted Execution Environments

Interaction with Memory



(a) Memory Write



(b) Memory Read

How Secure is SGX?

Malware Guard Extension: abusing Intel SGX to conceal cache attacks

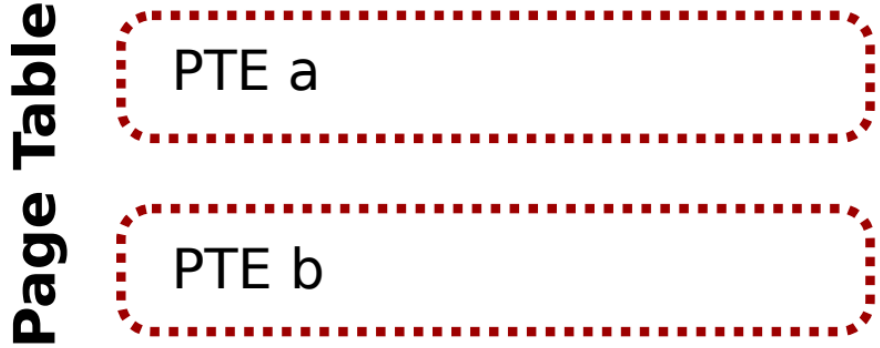
Software Grand Exposure: SGX Cache Attacks Are Practical

CacheZoom: How SGX amplifies the power of cache attacks

Telling Your Secrets Without Page Faults: Stealthy Page Table-Based Attacks on Enclaved Execution

Page Table Side Channel

```
void inc_secret( void )
{
    if (secret)
        *a += 1;
    else
        *b += 1;
}
```



Foreshadow (Spectre like) Attack

LILY HAY NEWMAN SECURITY 08.14.18 01:00 PM

SPECTRE-LIKE FLAW UNDERMINES INTEL PROCESSORS' MOST SECURE ELEMENT

I'M SURE THIS WON'T BE THE LAST SUCH PROBLEM —

Intel's SGX blown wide open by, you guessed it, a speculative execution attack

Speculative execution attacks truly are the gift that keeps on giving.

https://wired.com and https://arstechnica.com

https://foreshadowattack.eu/

Thanks