Comp 590-184: Hardware Security and Side-Channels

Lecture 17: TEE Attacks

March 24, 2026

Andrew Kwong

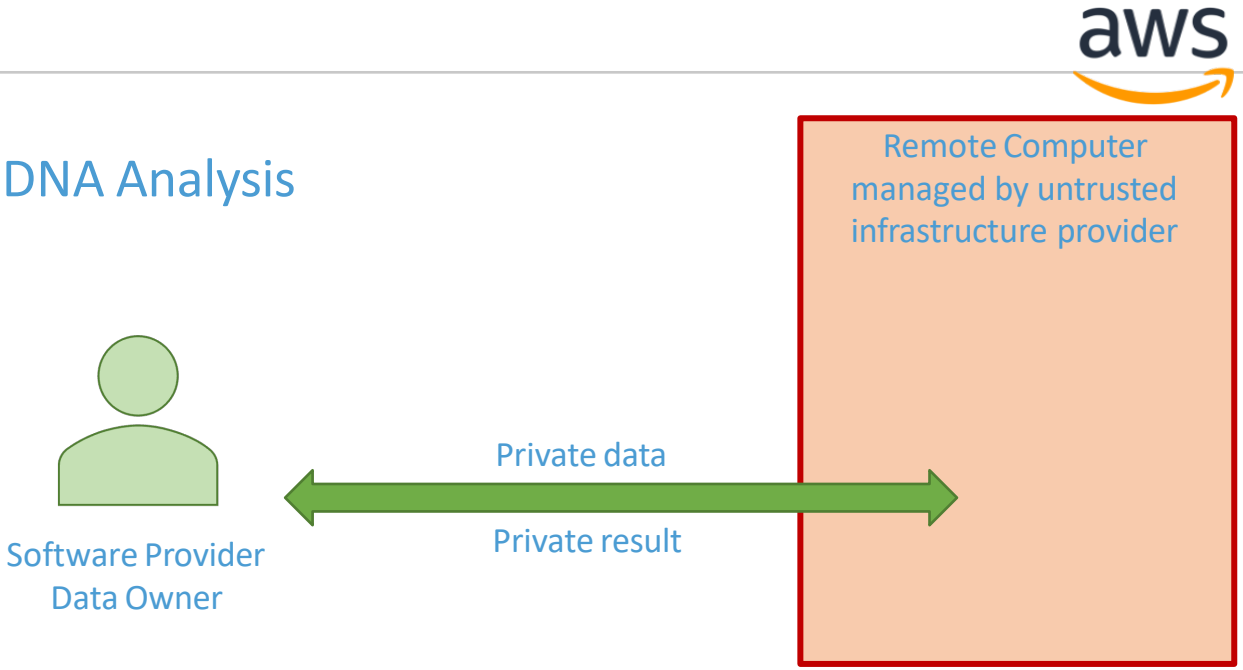
THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Outline

- How SGX protects memory
- Attacks against SGX

Secure Remote Computing

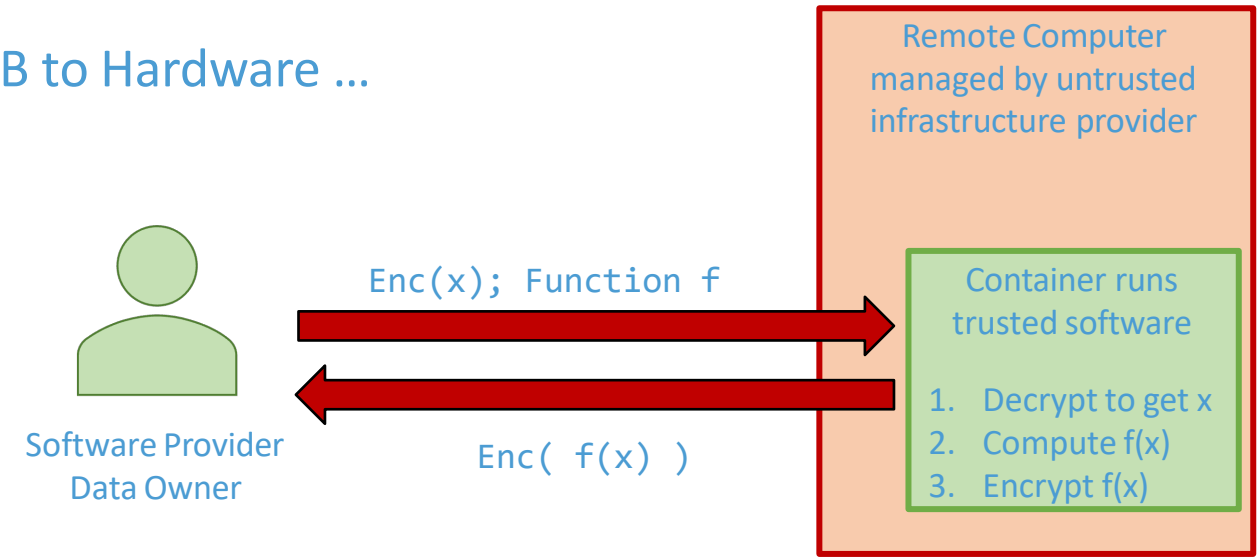
- Example: DNA Analysis



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

Hardware Solution

- Move TCB to Hardware …

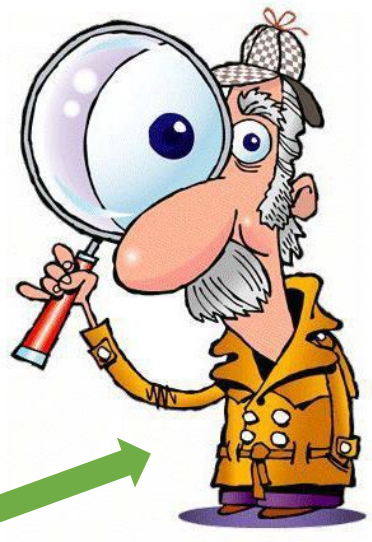


Software Guard Extensions (SGX) Security Model

Attestation

Remote Client

Software Guard Extensions (SGX) Security Model



Quote includes:

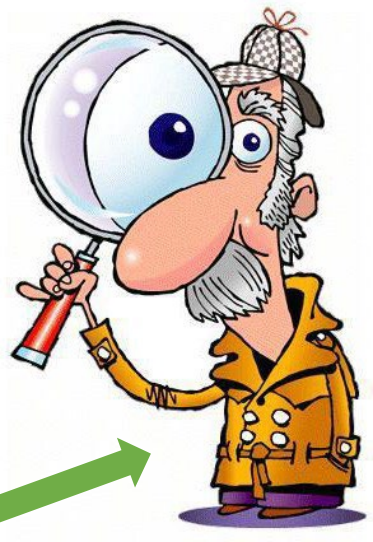
- “measurement”
- Data
- All signed by a private key

IAS

Remote Client

Enhanced Privacy ID

Software Guard Extensions (SGX) Security Model

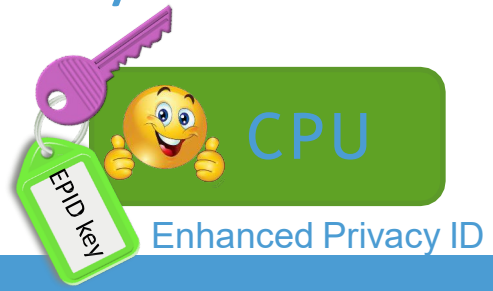


Quote includes:

- "measurement"
- Data
- All signed by private key

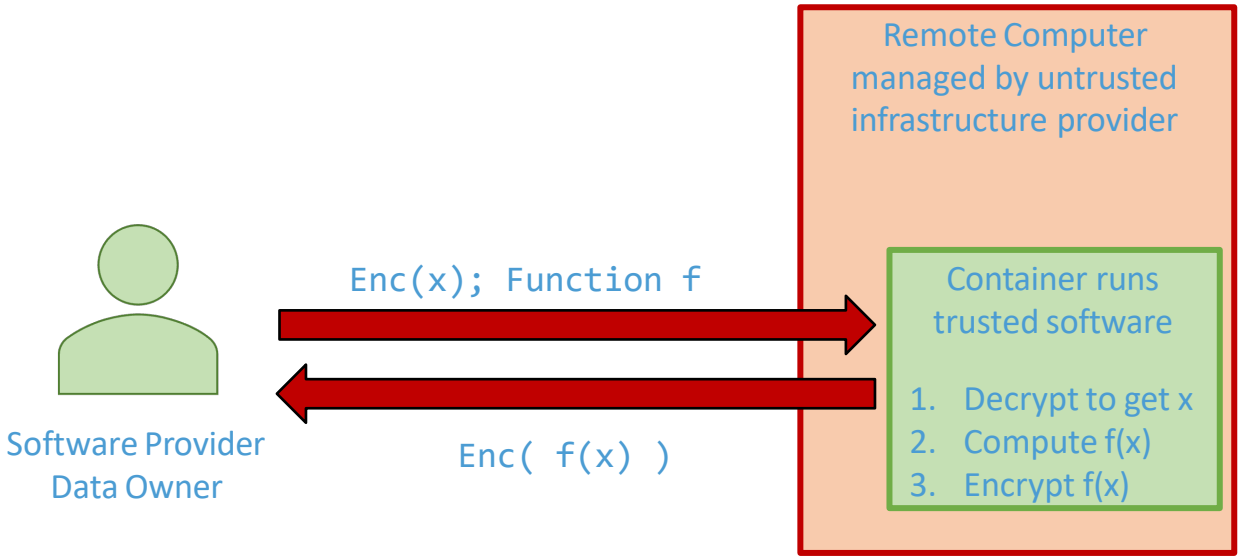
IAS

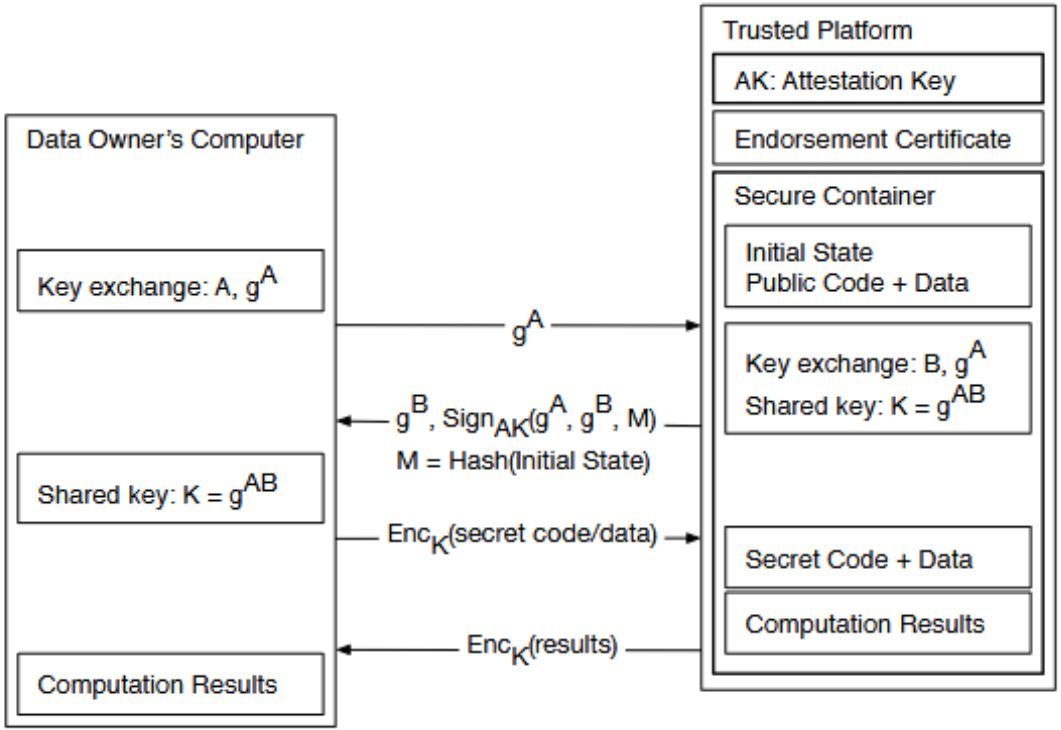
Remote Client



Enhanced Privacy ID

Secure Remote Computation Achieved!

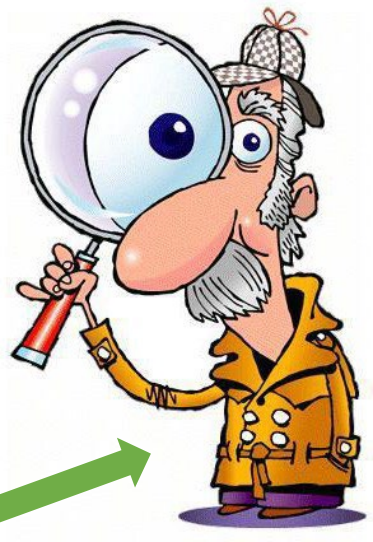



Trusted Platform
AK: Attestation Key
Endorsement Certificate
Secure Container
Initial State
Public Code + Data
Key exchange: B, g^A
Shared key: $K = g^{AB}$
Secret Code + Data
Computation Results
Data Owner's Computer
Key exchange: A, g^A
Shared key: $K = g^{AB}$
Computation Results
g^A
g^B, $Sign_{AK}(g^A, g^B, M)$
M = Hash(Initial State)
Enc_K(secret code/data)
Enc_K(results)

Original purpose of SGX

- DRM
- Software cracking:
  - Hackers modify binaries or extract product keys in order to redistribute software illegally
- Binary is unpacked and product keys are verified in an enclave
- Still used by blue ray
  - 4K Ultra HD Blu-ray discs still SGX for authorized playback on PCs.

Software Guard Extensions (SGX) Security Model

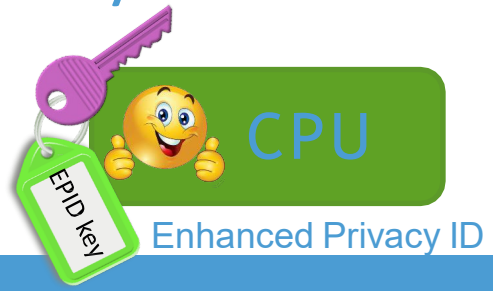


Quote includes:

- "measurement"
- Data
- All signed by private key

IAS

Remote Client



Enhanced Privacy ID

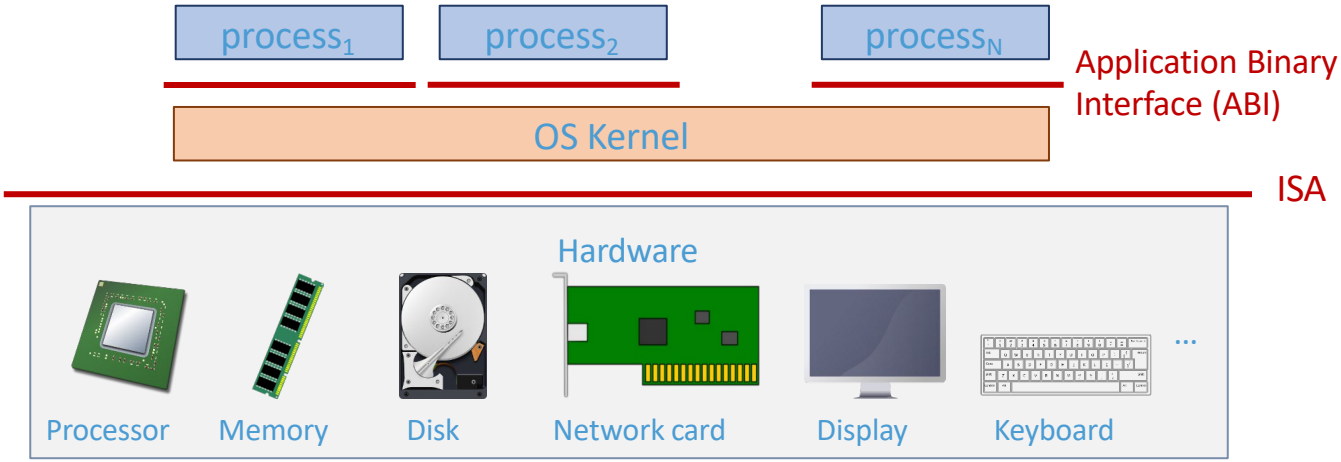
Software Guard Extensions (SGX) Security Model

Attestation

Remote Client

Privileged Software Attacks

Operating Systems



What Does Privileged SW Do?

```
./helloworld
```

- Operations at launch time:
  - Create a process (PID, status, etc.)
  - Create a virtual address space: allocate memory for stack, heap, code region, set up the page tables
  - Setup file descriptor for input and output
  - Load the binary into the code region, and linked libraries if needed
  - Transfer the control to user space




What can a privileged software attacker do?

- A non-comprehensive list
  - Modify the code to be executed
  - Monitor the whole execution process and data in register and in memory
  - Modify data in register and memory
  - Intercept IO, eavesdrop and tamper with the communication
  - ……

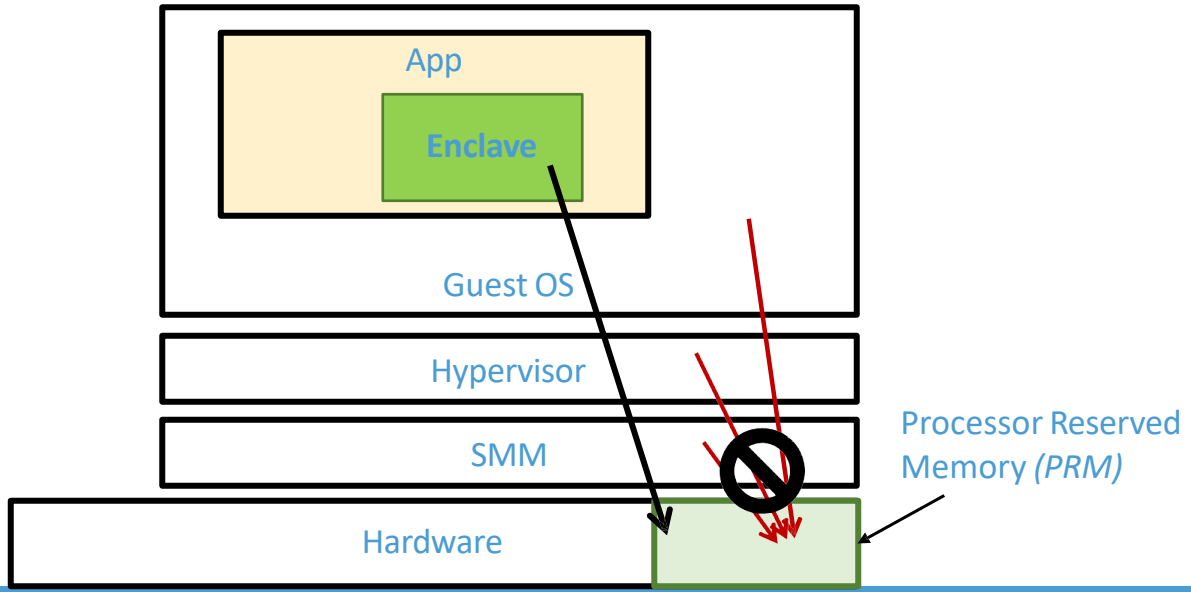
Interrupt Handling

- Switch from user space to kernel space
  - Remember the current PC
  - Jump to kernel code: perform a sequence of save operations
    - Save general purpose registers content into an object associated with the current thread
    - Save system registers, including page table root address (CR3 in X86)
  - Based on the interrupt type, decide what to do
- Switch back to user space
  - Restore all the registers: general-purpose + system registers
  - Jump back to the saved PC


Case Study: Memory Management in Intel SGX

Intel SGX Overview

- Enclave code/data map to PRM; Different enclaves access their own memory region

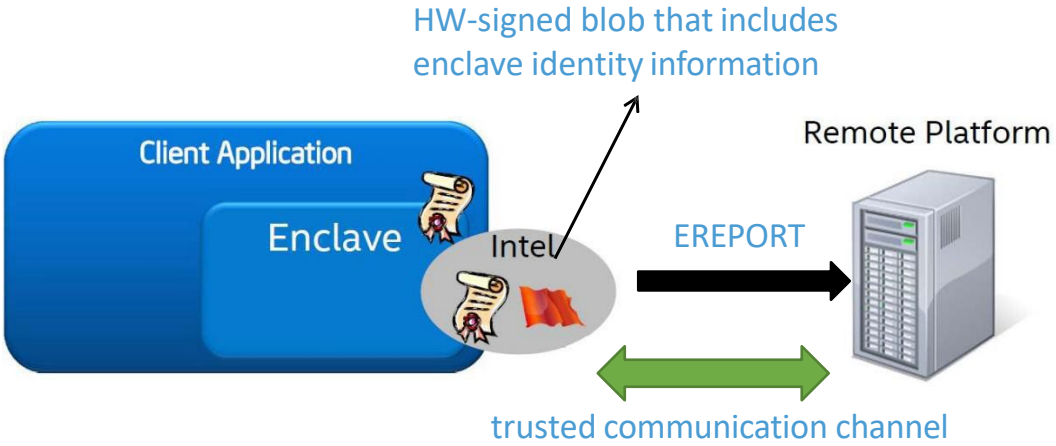


Security Tasks

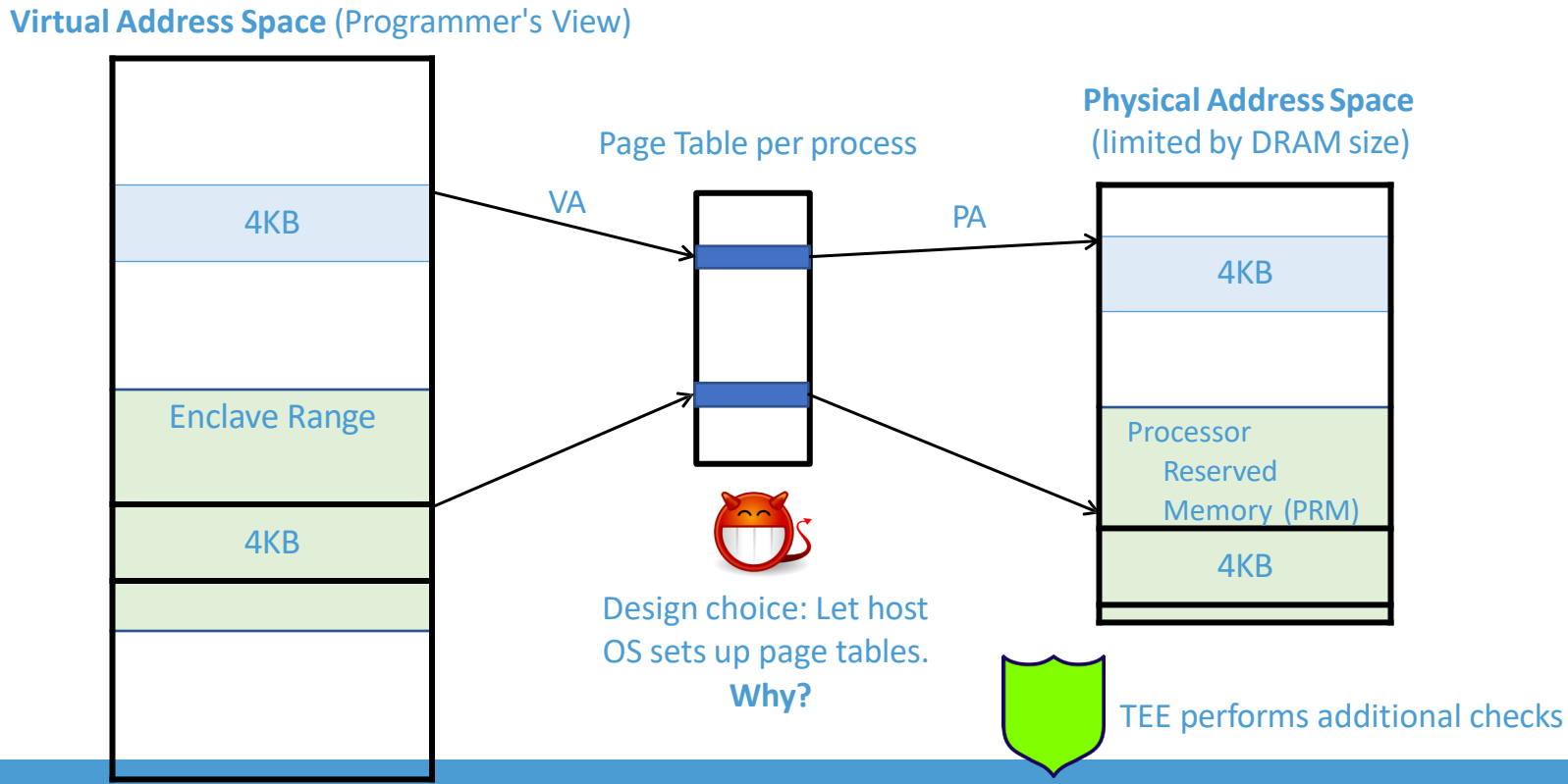
- How do we ensure the runtime execution follows our expectation (confidentiality and integrity of the execution)?
- How do we ensure the enclave code is the code that we want to execute? (code integrity during initialization)
- DRAM security? How to deal with Rowhammer and Coldboot attacks?

Enclave Attestation and Sealing

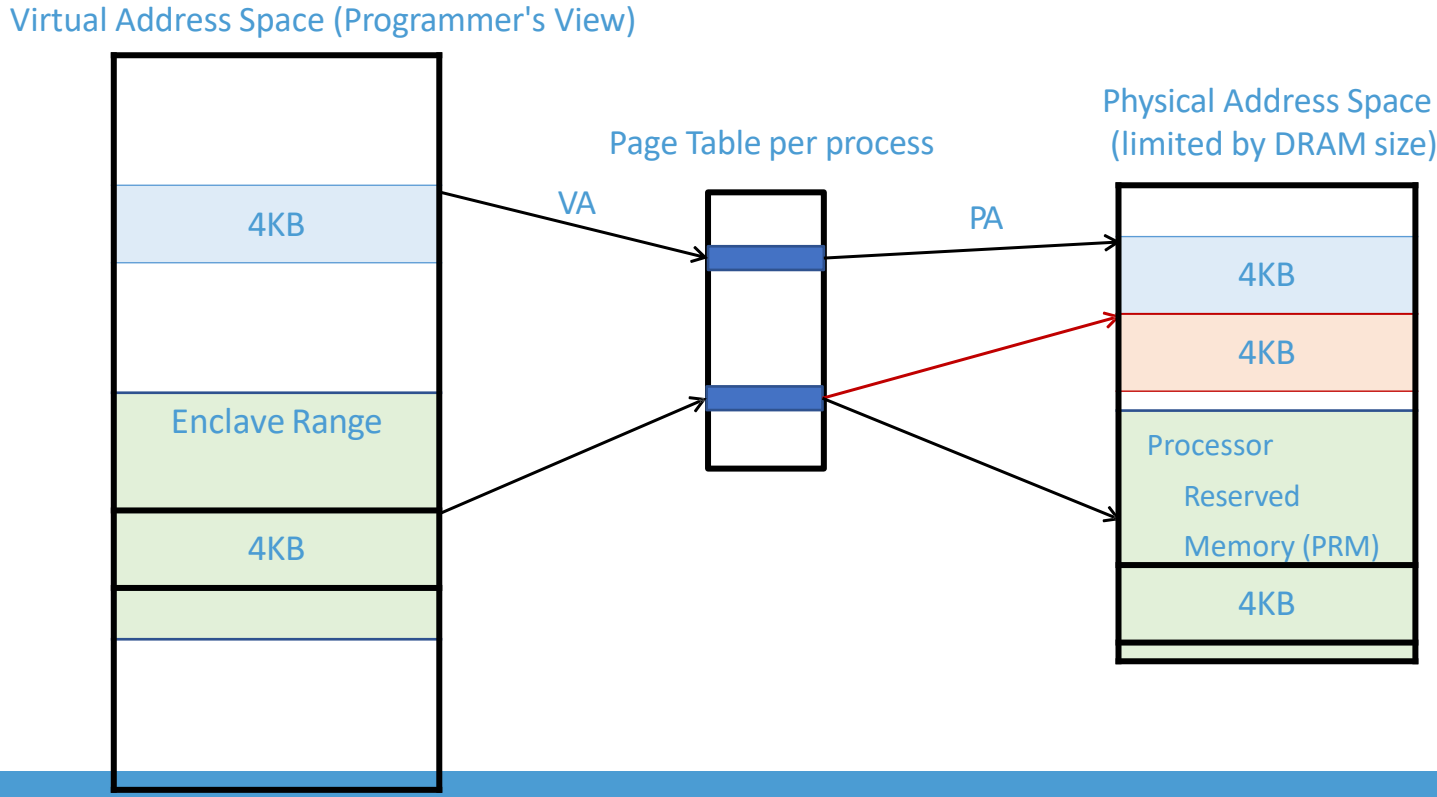
- HW based attestation provides evidence that “this is the right application executing on an authentic platform” (approach similar to secure boot attestation)



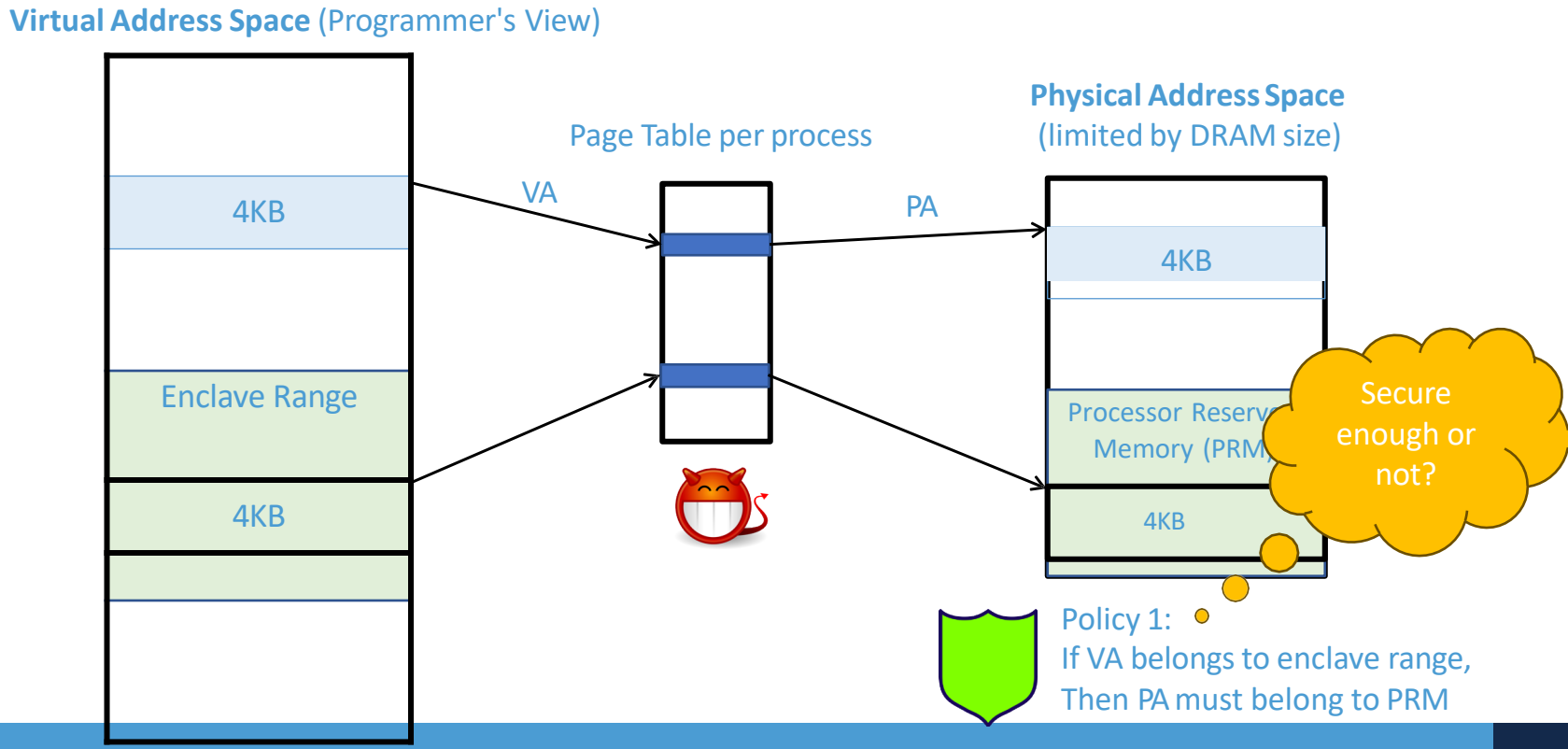
Intel SGX Address Translation Overview



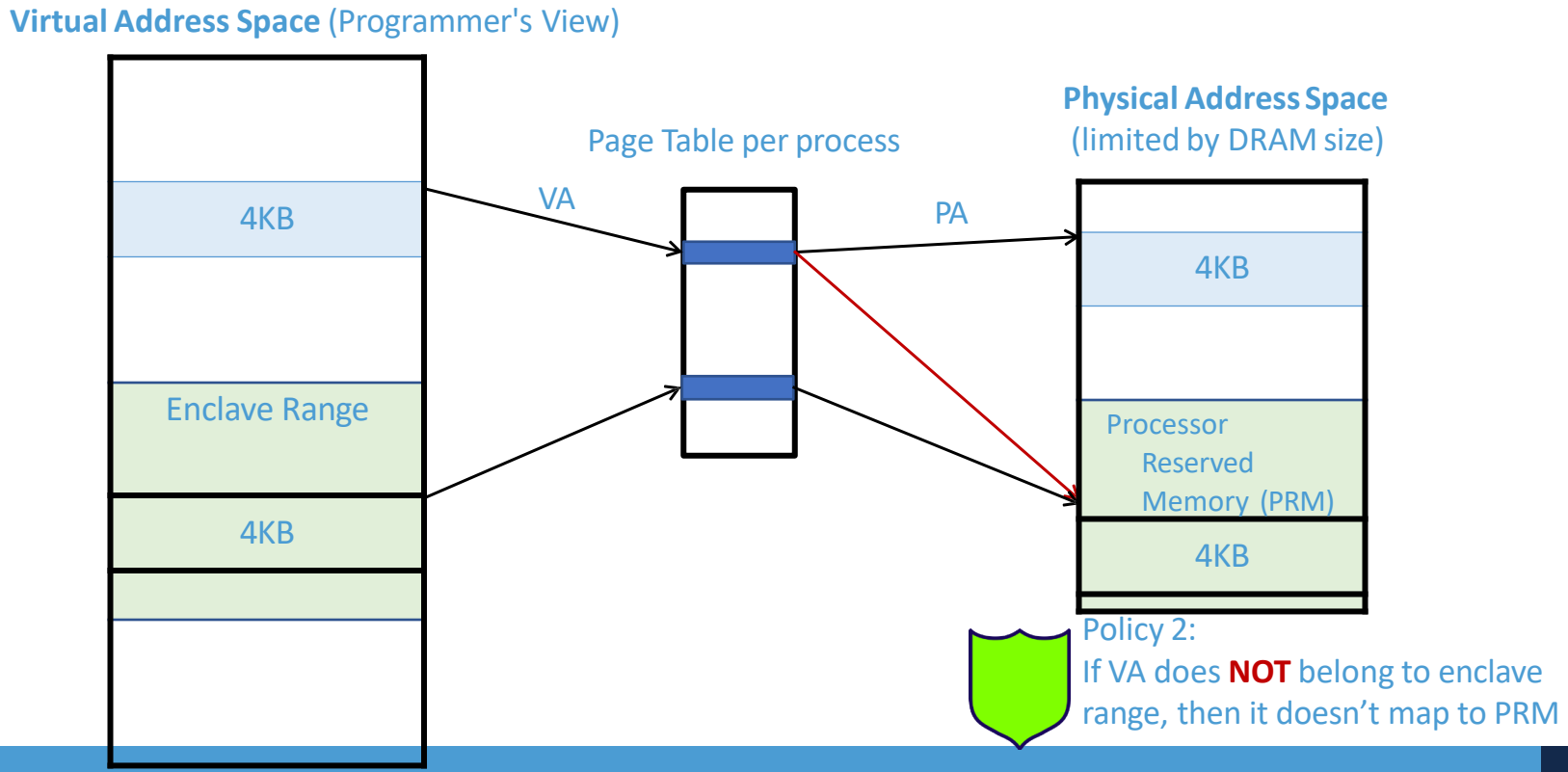
Malicious Address Translation #1



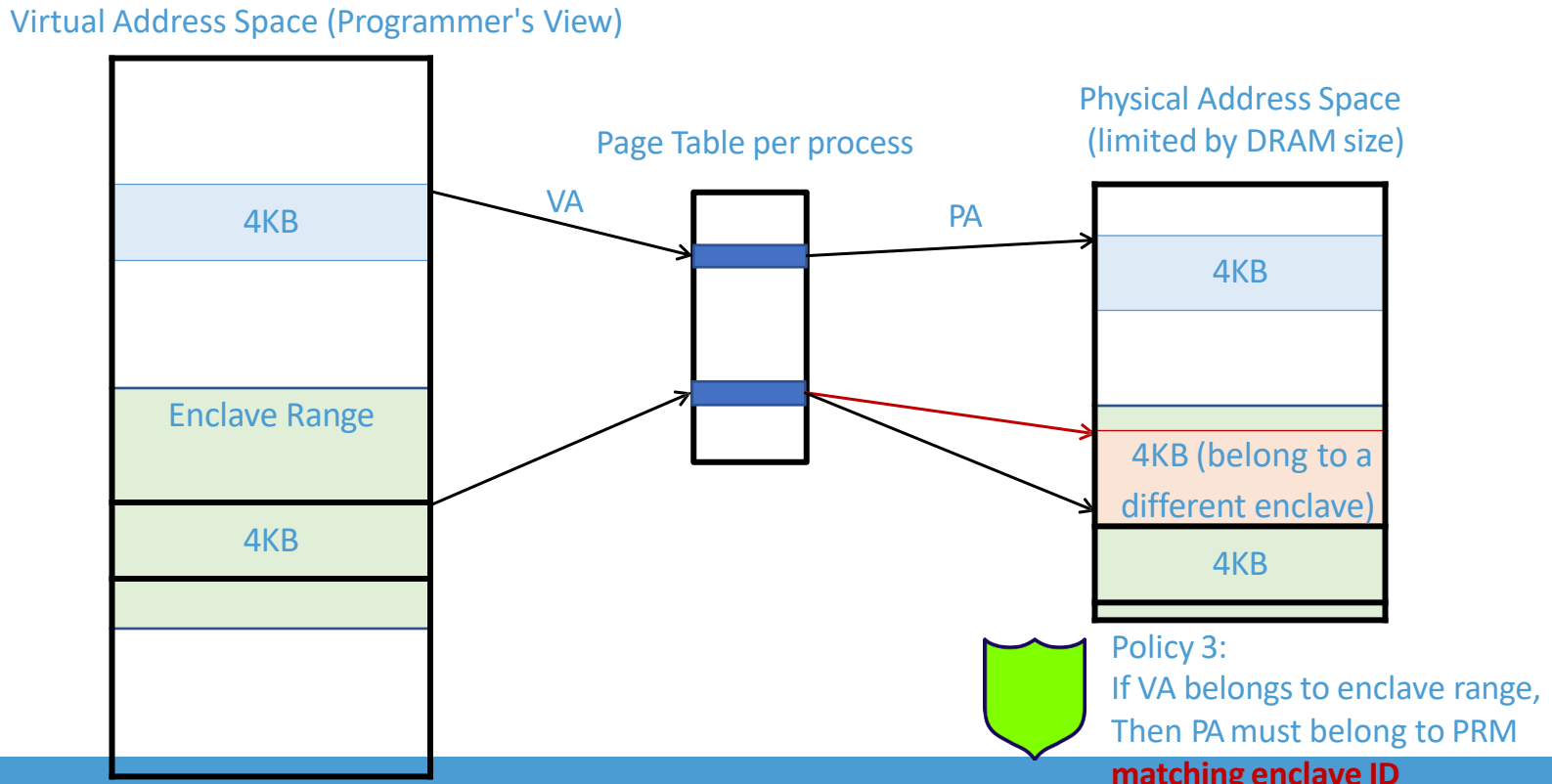
Intel SGX Address Translation Overview



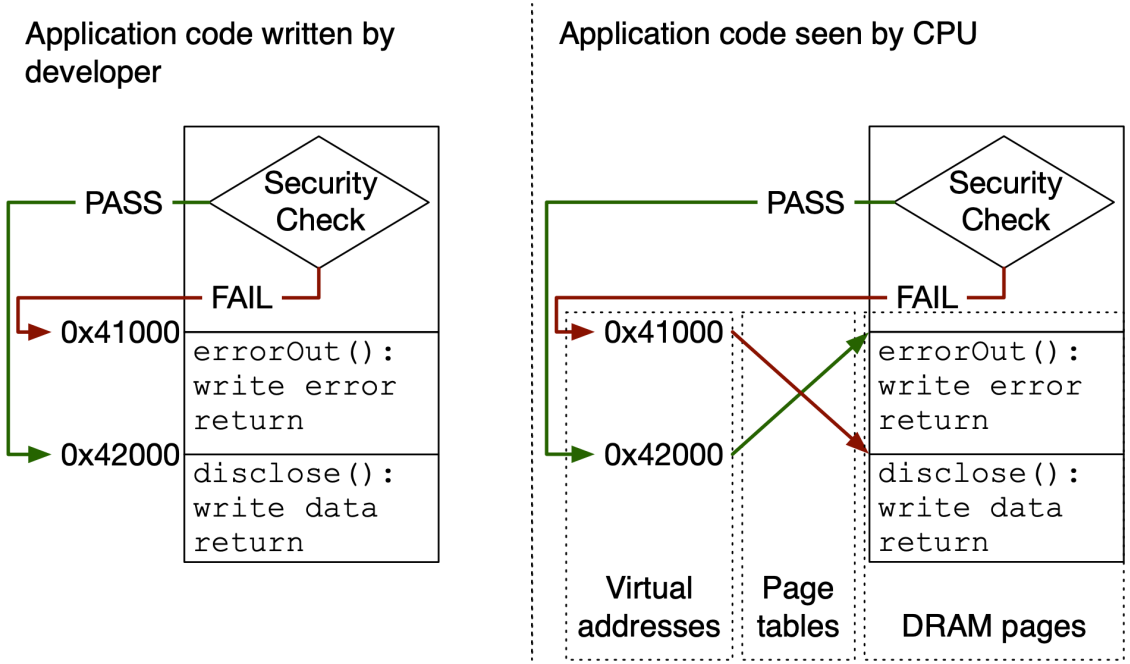
Malicious Translation #2



Malicious Translation #3



Malicious Translation #4



Solution: Inverted Page Table

- For each page in the PRM, remember the mapping from

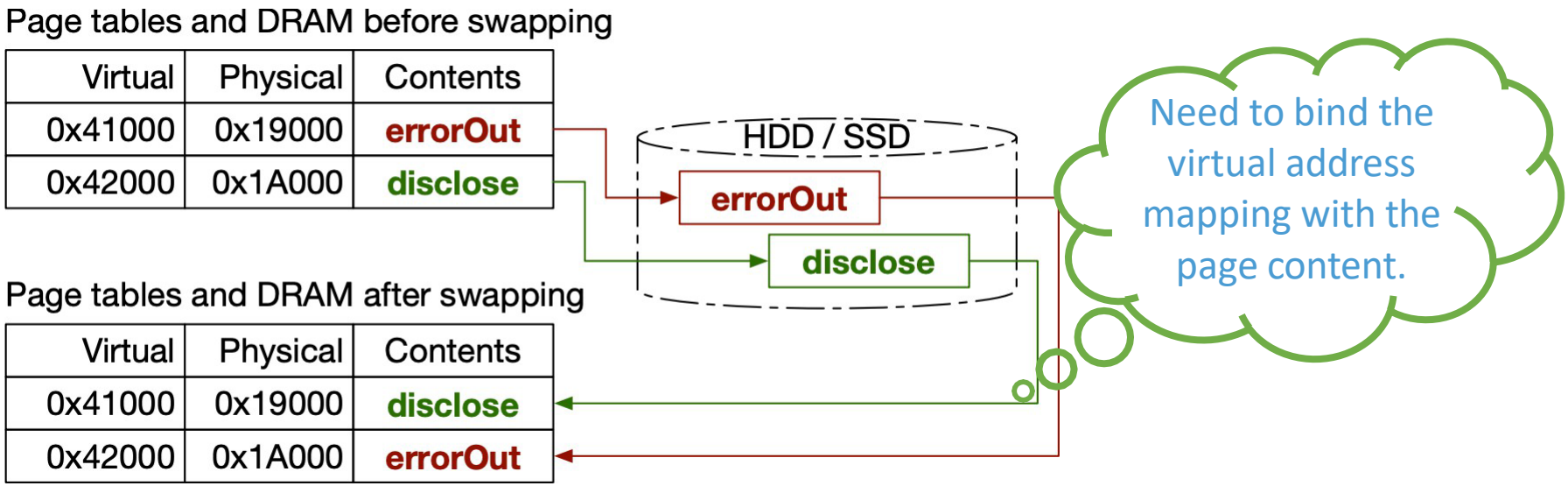
  <PPN> ➔ <VPN, Enclave ID>

  Keep the reversed page table in PRM, so privilege software cannot modify

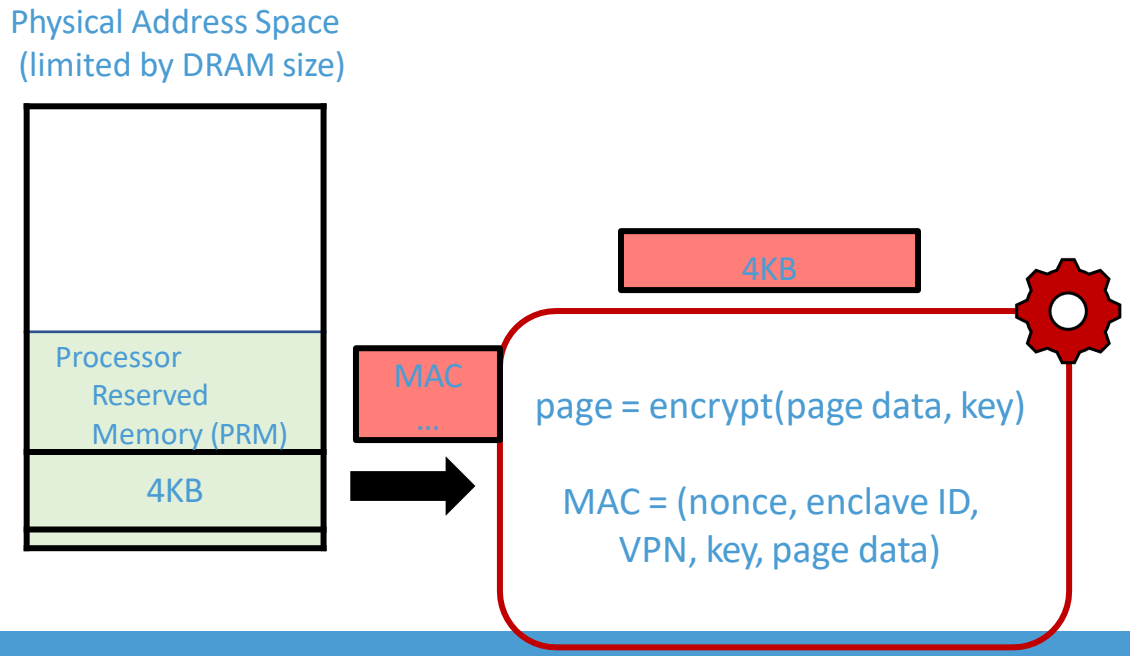
- When to perform the check? (Review address translation process)
  - After each address translation

Malicious Address Translation #5

A memory mapping attack that does not require modifying the page tables.

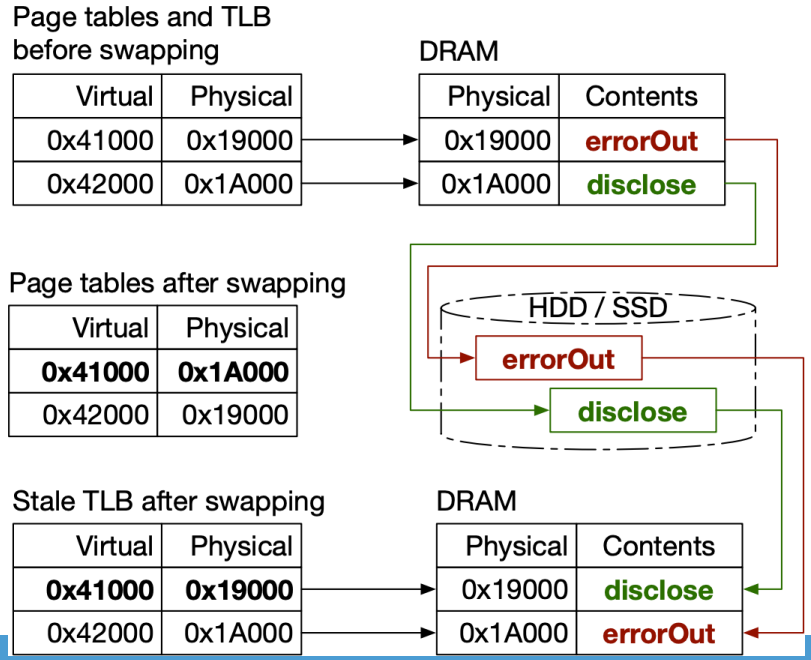


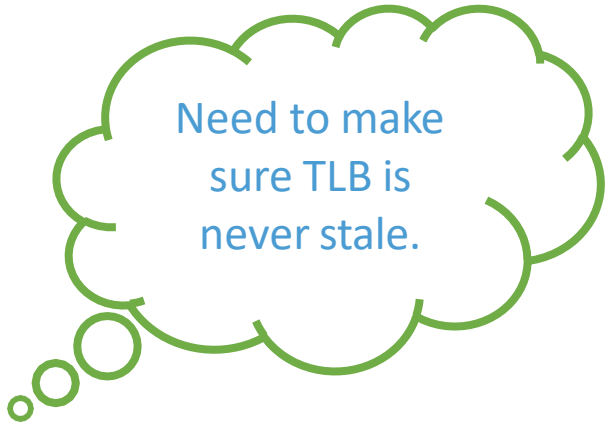
Solution: Page Encryption and Authentication



Malicious Address Translation #6

A memory mapping attack that exploits stale TLB entries.





Solution: Keep TLB up-to-date

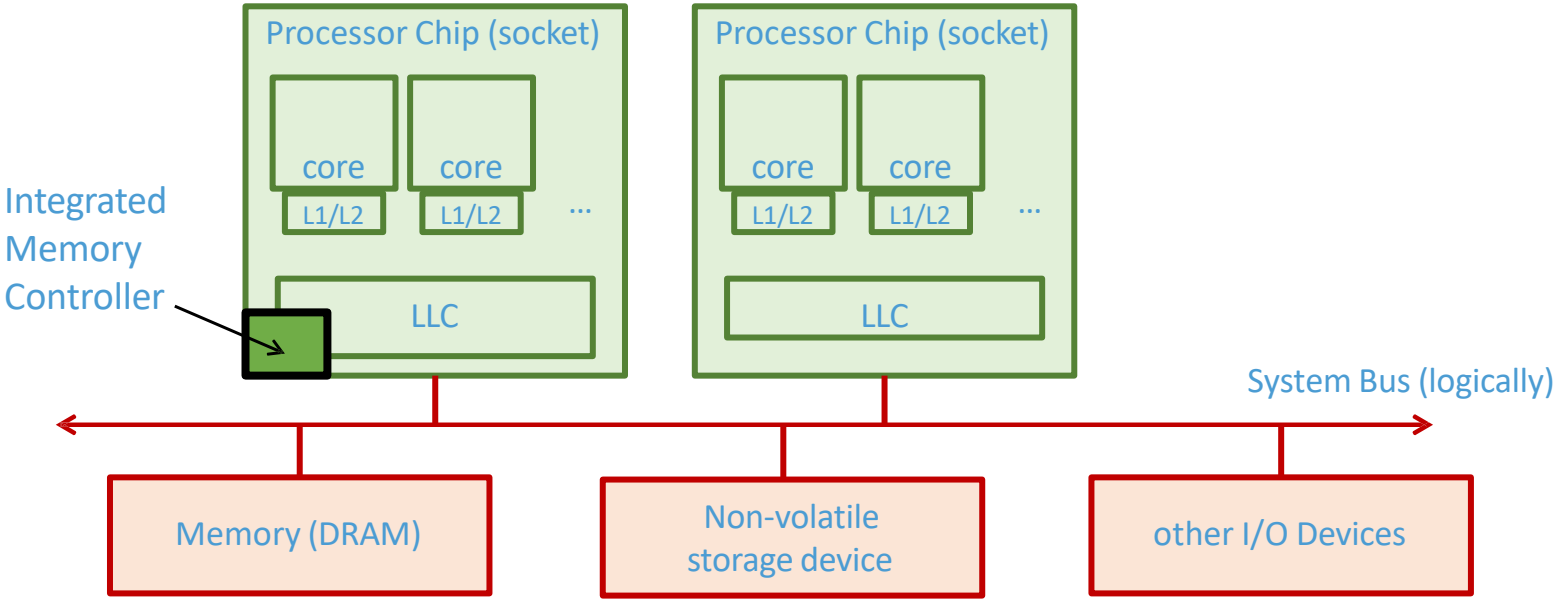
- Keep an extra state in the inverted page table
  - <PPN> ➔ <VPN, Enclave ID>
  - <PPN, state> ➔ <VPN, Enclave ID>
  - Mark “blocked”
  - Unset only until all the VPNs (can mapped by multiple enclaves) exist and flush TLBs
- If the TLB has stale data, post address translation check will see the physical address is “blocked”

Summary: SGX Memory Management

- #1: Maintain an inverted page table and check after every address translation
  - Physical page in PRM -> (enclave ID, virtual page number)
- #2: Encrypt/decrypt upon page swap to non-PRM region
  - (nonce, enclave ID, virtual page number, key, page content) ➔ MAC
- #3: Keep TLB state up-to-date
  - Upon page swap, block the page in the inverted page table and unblock only after all the corresponding TLB entries are flushed

Additional Security Threats

- DRAM attacks: Rowhammer, Coldboot attacks



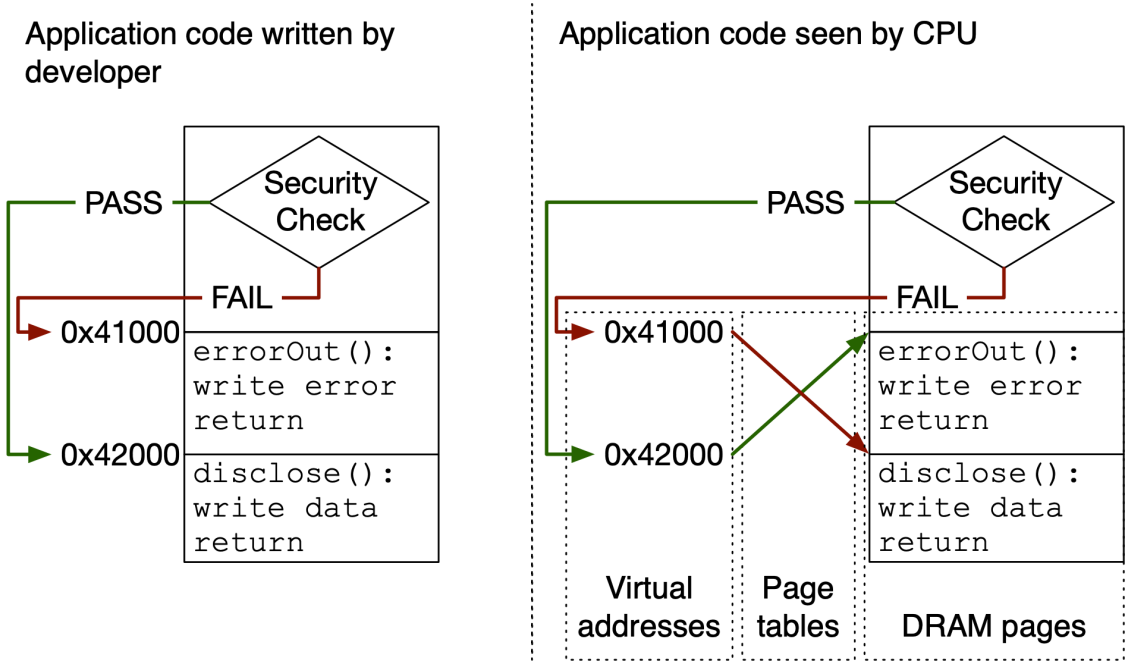
- What about side-channel attacks?

Software Guard Extensions (SGX) Security Model

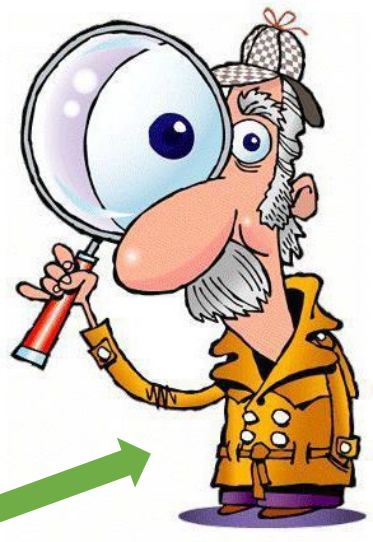
Attestation

Remote Client

Controlled Channel attack



Software Guard Extensions (SGX) Security Model

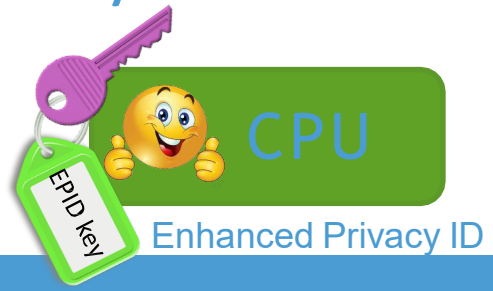


Quote includes:

- "measurement"
- Data
- All signed by private key

IAS

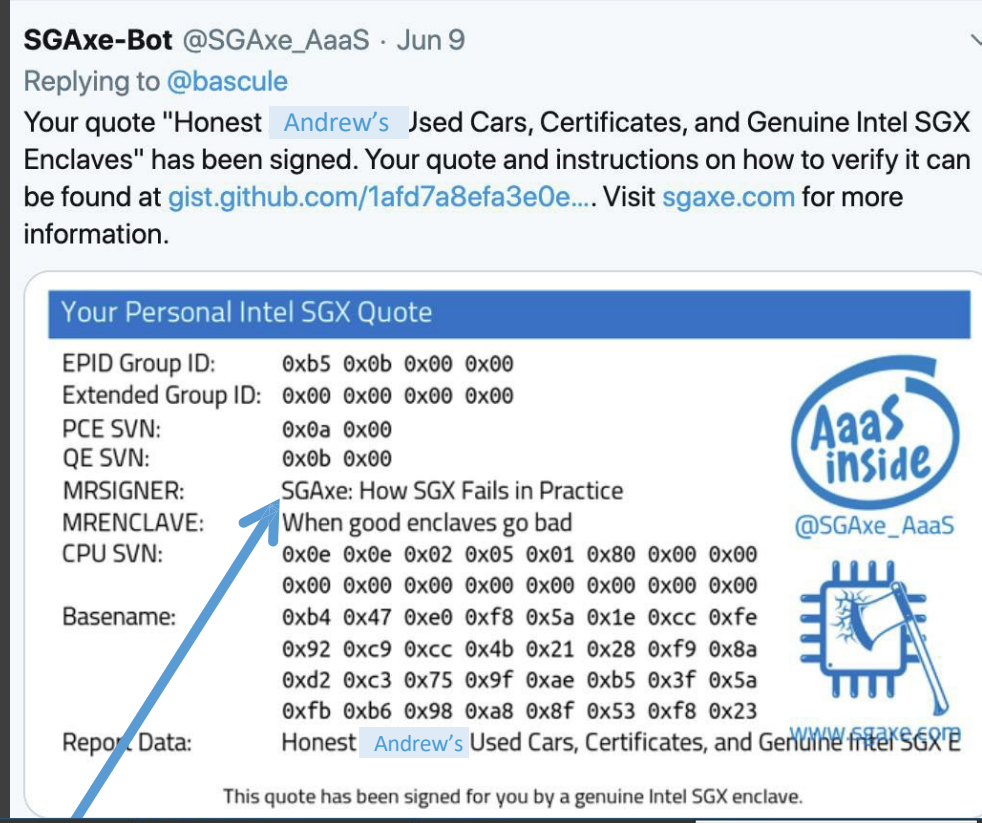
Remote Client

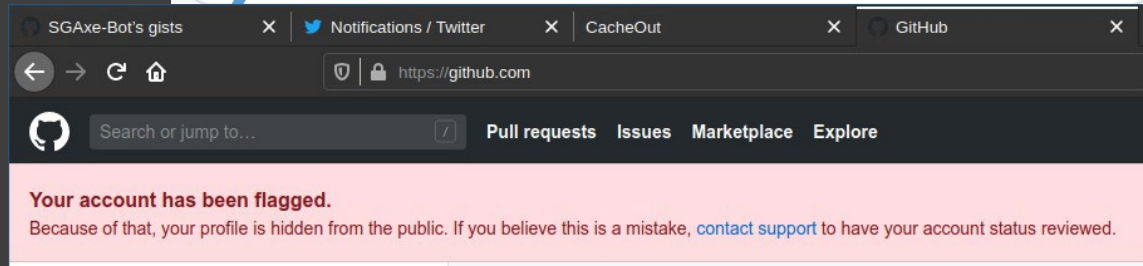


Enhanced Privacy ID

AaaS (Attestation as a Service)

- @SGAxe_AaaS
  Will attest to anything tweeted at it
- Signed 100+ quotes within 2 hours
  - Blocked by Github
- After the public release of the paper, key was still trusted for a whole month
- Can't update TCB quickly because SGX users need to install BIOS updates
- Hardcoded MRSIGNER prevents abuse





Foreshadow

- Uses Meltdown to directly read from the cache within the enclave
  - Contains decrypted PRM data


FORESHADOW


However, FORESHADOW
can read the actual
enclave memory

Summary

- What can privileged software attackers do?
- How SGX defends against these
- Side-channel attacks on TEEs
- Read more:
  - Intel SGX Explained; by Costan et al
  - SoK: Understanding Designs Choices and Pitfalls of Trusted Execution Environments; by Li et al

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL