University of BRISTOL

Systems & Software Security

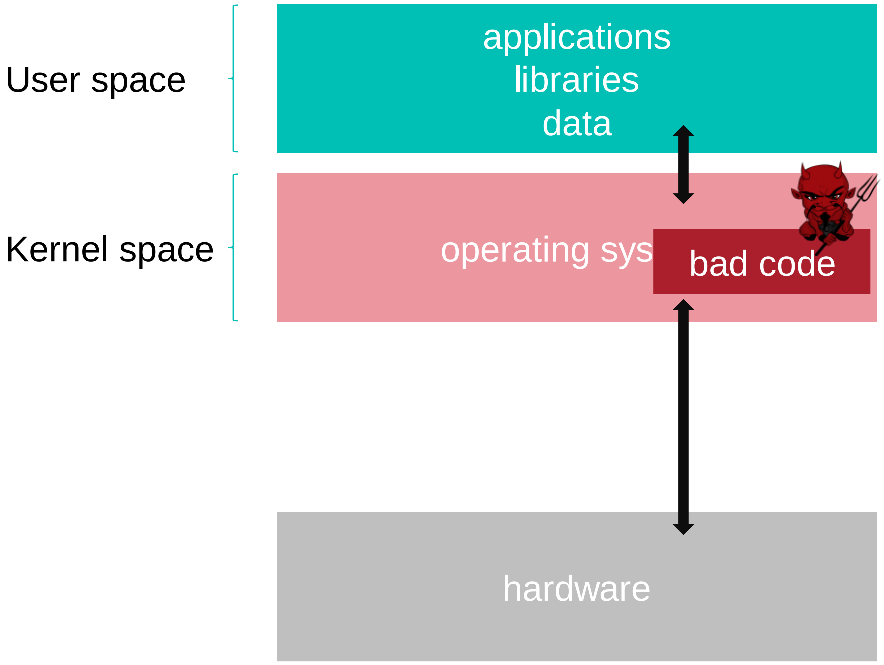
COMSM0050
2020/2021

University of BRISTOL

Intel SGX

bristol.ac.uk

Rootkit high-level understanding



Motivation

- An attacker can compromise
  - User space
  - Operating Systems
  - Even the hardware!
- What can we do?

Motivation

- An attacker can compromise
  - User space
  - Operating Systems
  - Even the hardware!
- What can we do?

Execute code in its own secure enclave!

SGX Hardware supported enclave

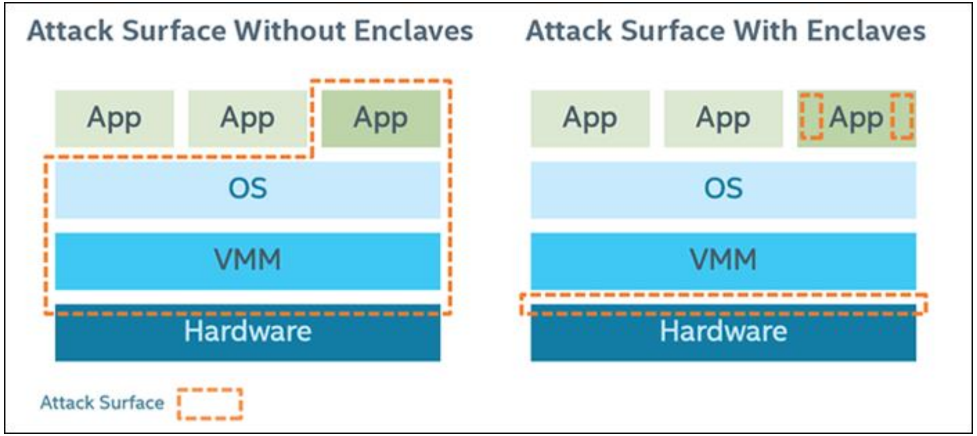
- WARNING: there is vulnerabilities in SGX

SGX Hardware supported enclave

- WARNING: there are vulnerabilities in SGX
- Idea: run an application within some isolation unit so it cannot be affected by the OS
  - don’t trust the OS or the VMM/hypervisor
  - only need to trust the hardware

SGX Hardware supported enclave

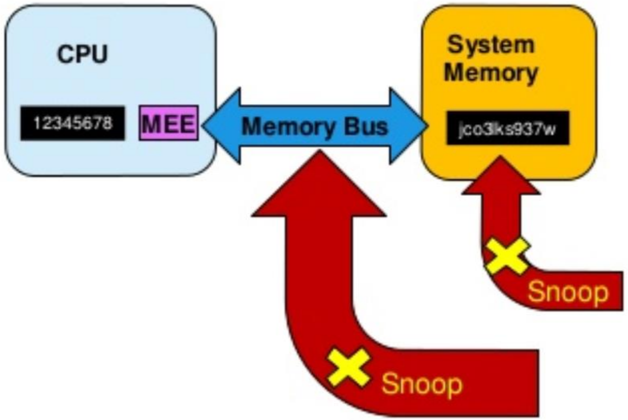
- WARNING: there is vulnerability in SGX
- Idea: run an application within some isolation unit so it cannot be affected by the OS
  - don’t trust the OS or the VMM/hypervisor
  - only need to trust the hardware
  - reduce attack surface



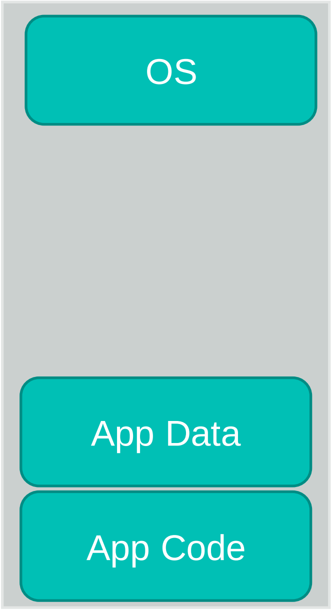
SGX preventing memory snooping attack

- Security boundary is CPU package
- Data unencrypted inside the CPU
- Data outside the CPU is encrypted
- External memory reads and bus snooping only see encrypted data

* MEE: SGX Memory Encryption Engine

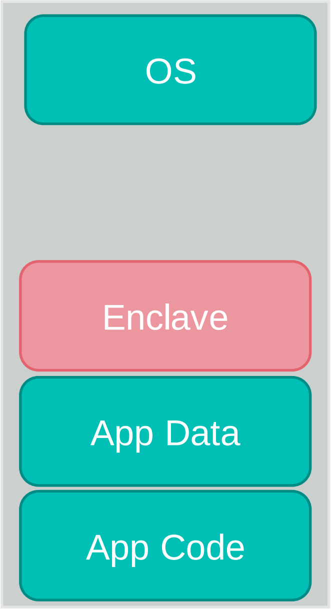


SGX Programming environment



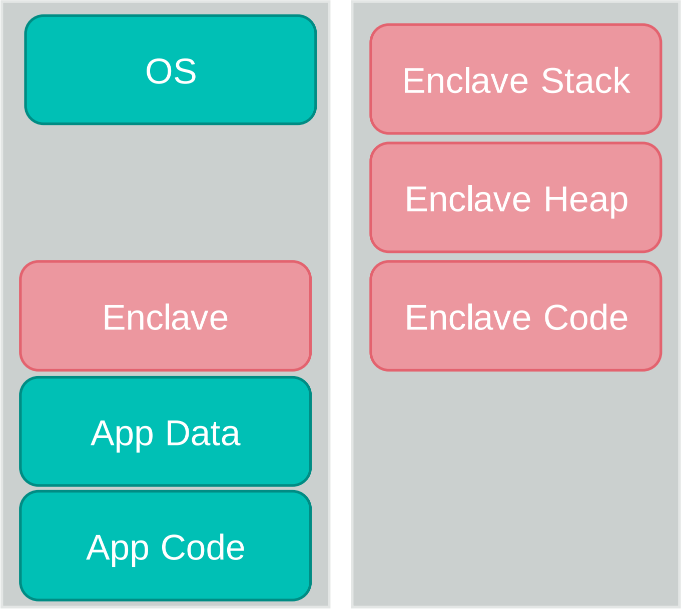
User Process

SGX Programming environment



User Process

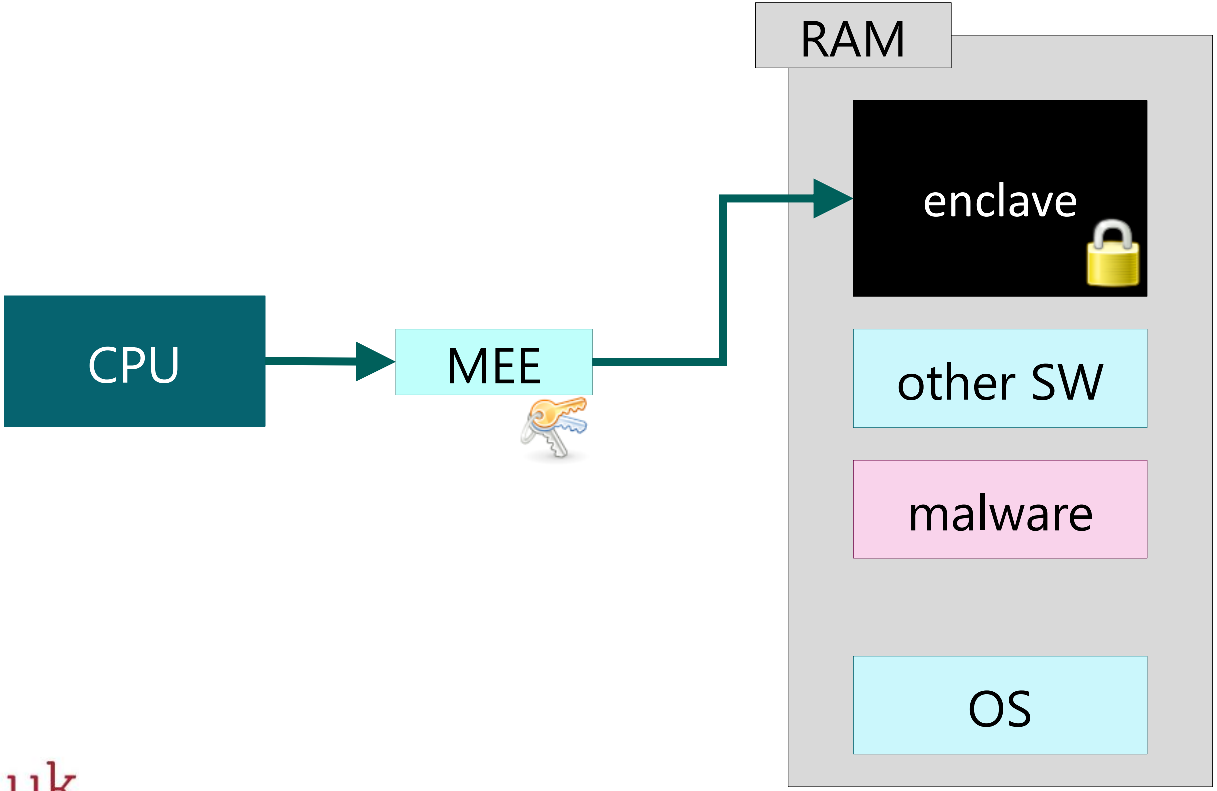
SGX Programming environment



User Process

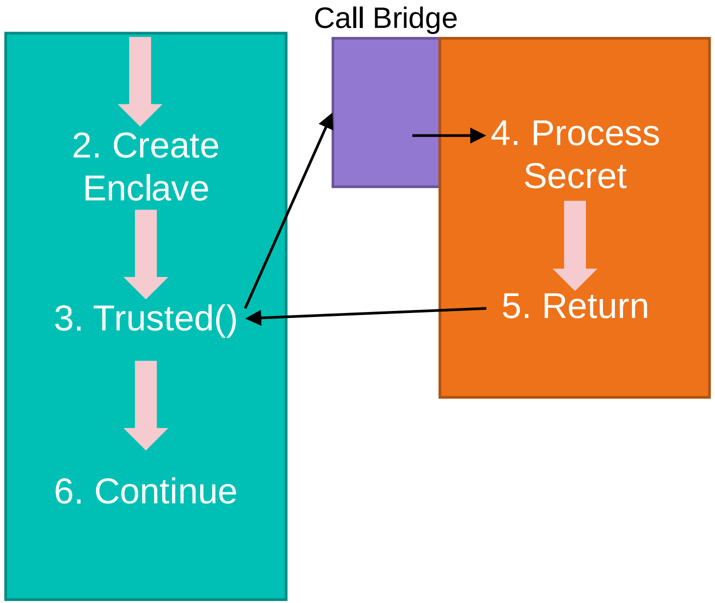
- Enclave has its own code and data
  - Provide confidentiality
  - Provide integrity
- Controlled entry point
  - Can enter enclave code only at specific point
  - Enclave execution takes over

Memory protection



SGX Application Flow

1. Define and partition application into trusted and untrusted part
2. App create enclave
3. Trusted function is called
4. Code in enclave process some secret
5. Trusted function returns
6. App continue as normal


Call Bridge
2. Create Enclave
3. Trusted()
6. Continue
4. Process Secret
5. Return