Privacy-Preserving Systems (a.k.a., Private Systems)

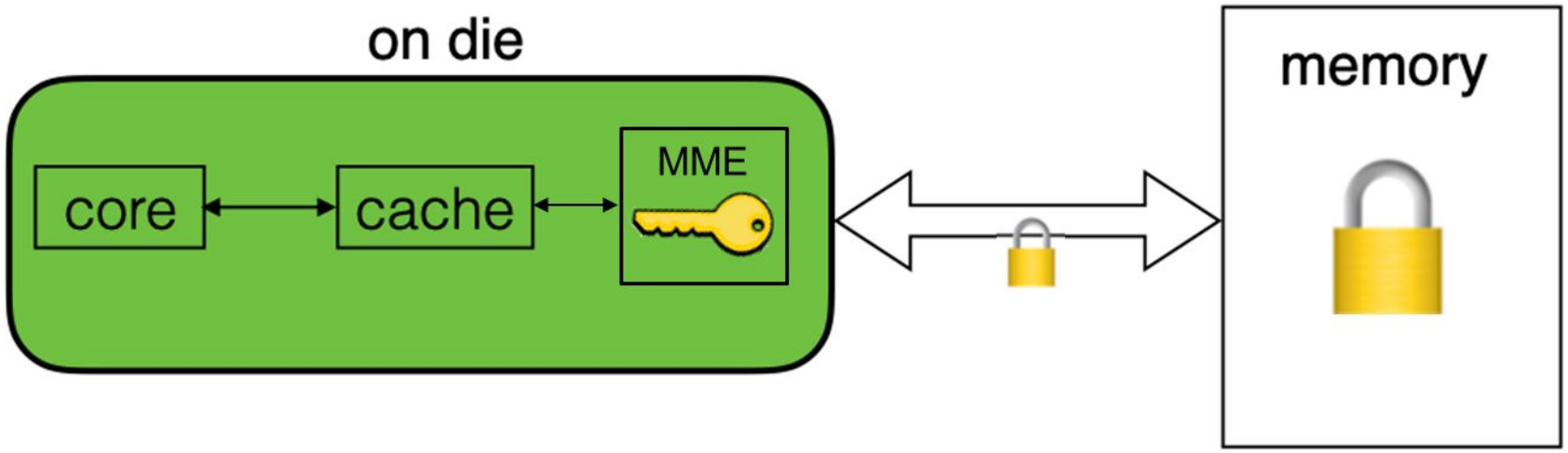
CU Graduate Seminar

Instructor: Roxana Geambasu

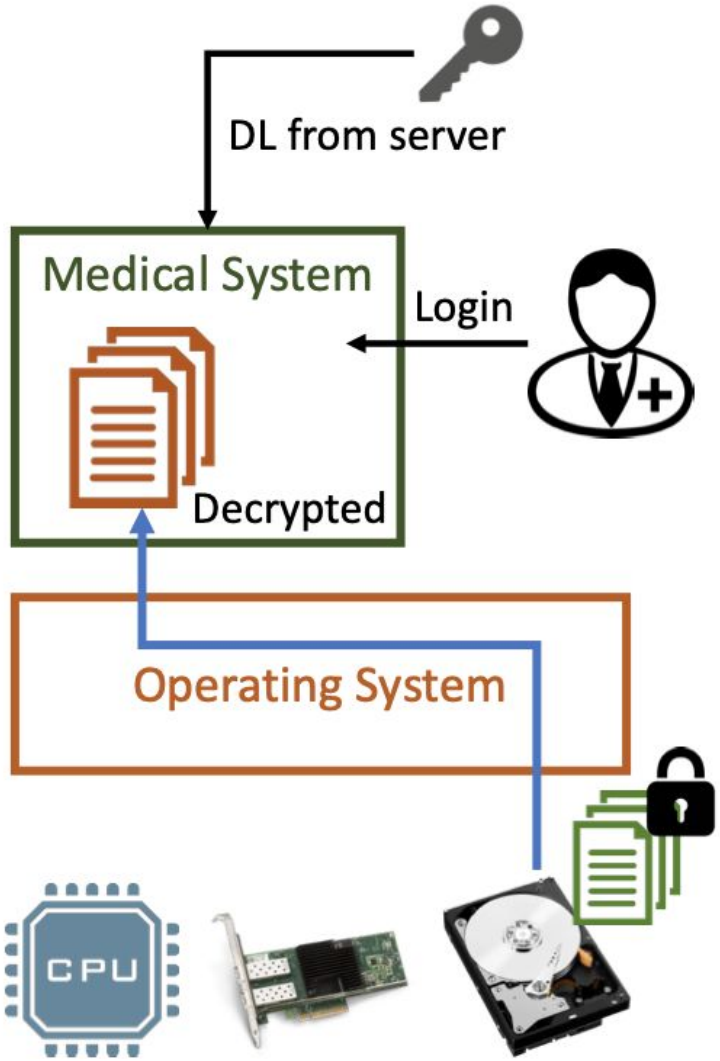
Hardware Enclaves

Hardware Enclaves (e.g., Intel SGX)

- Hardware-enforced isolated execution environment
- Data decrypted only on the processor
- Protect against an attacker who has root access or compromised OS
- Cloud offerings: Azure Confidential Computing, Google Asylo, …

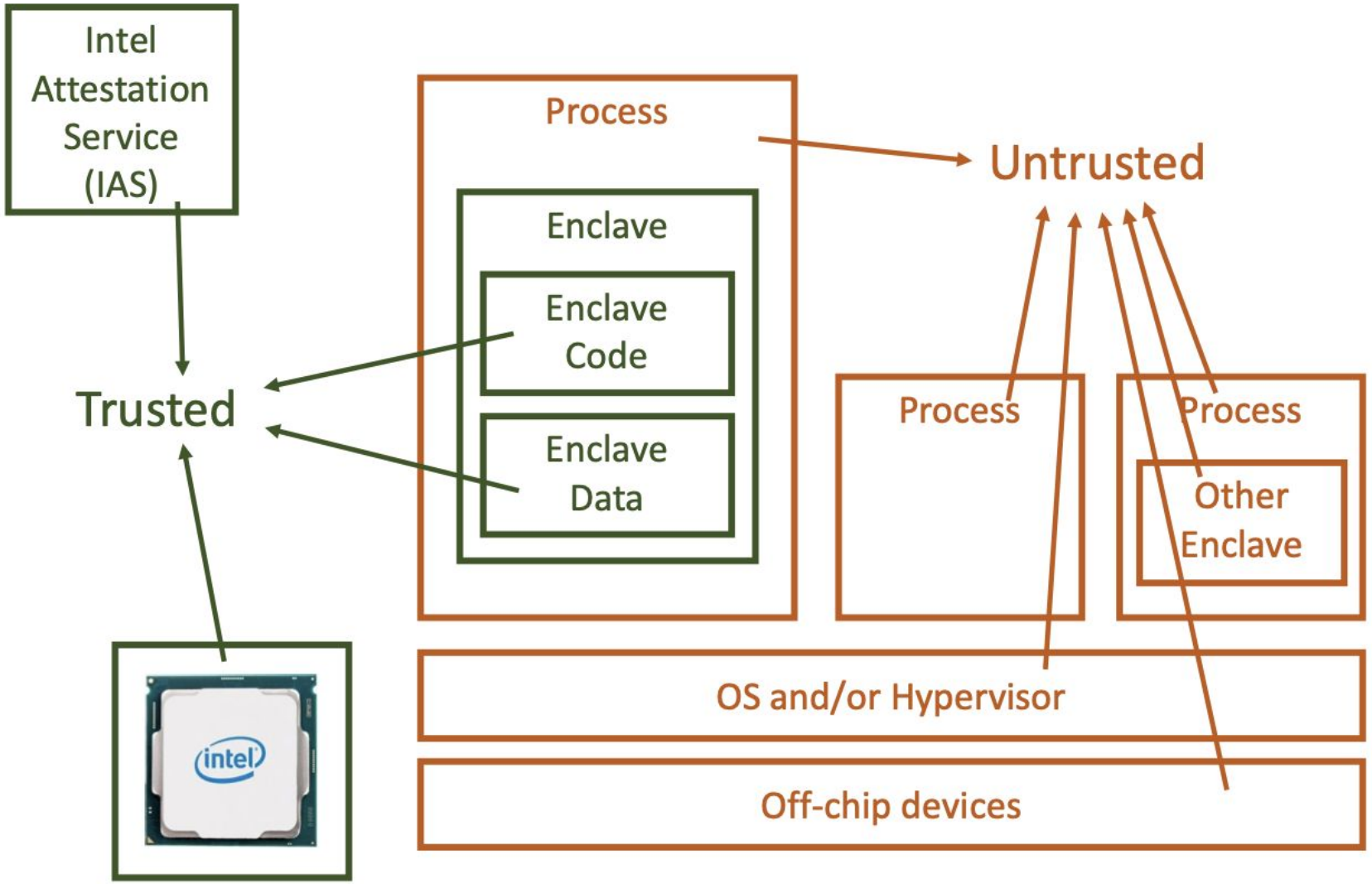


System Threats to Trusted Execution



- What can go wrong?
  - Side channels
    - out of scope for Intel SGX
  - Counterfeit software
  - Inject rootkits into OS
  - Privilege escalation
  - Install malicious kernel
  - Compromised HW devices
  - Cold-boot attacks

Threat Model for Hardware Enclaves

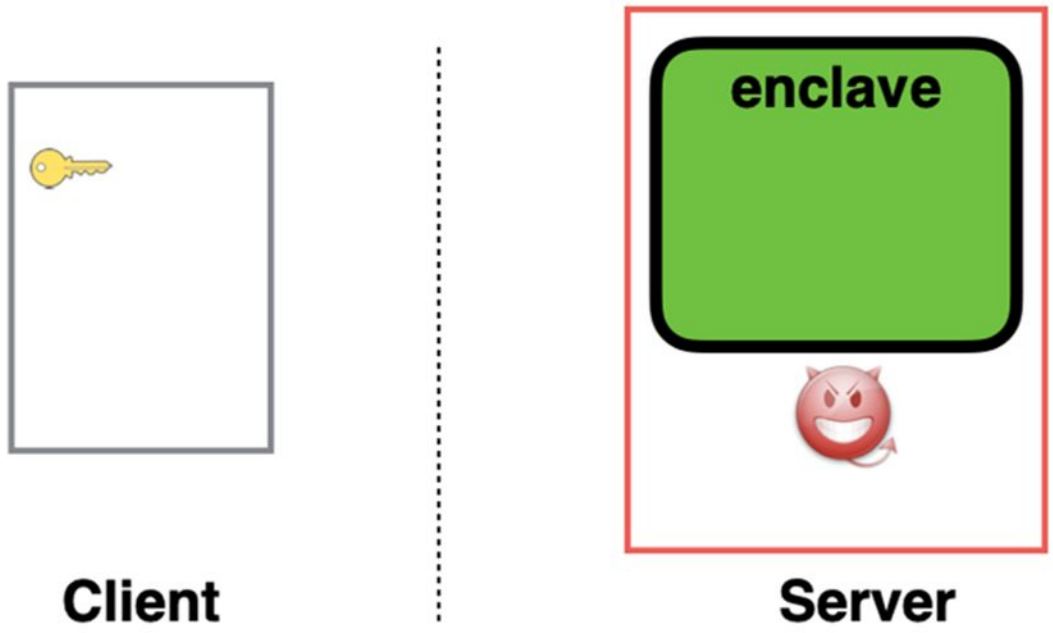


Elements of Secure Enclaves

- Secure boot: HW-verified measurement + first instruction
- On-chip program isolation
- Cryptographically protected external memory
- Execution integrity; no interference from attackers
- Remote attestation
- Secret sealing

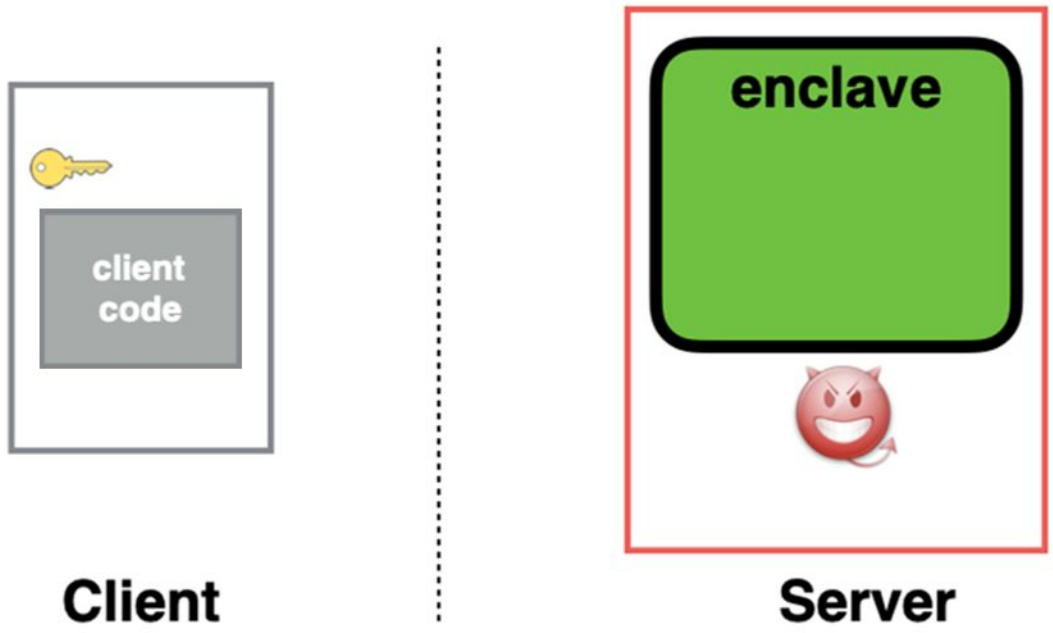
Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.



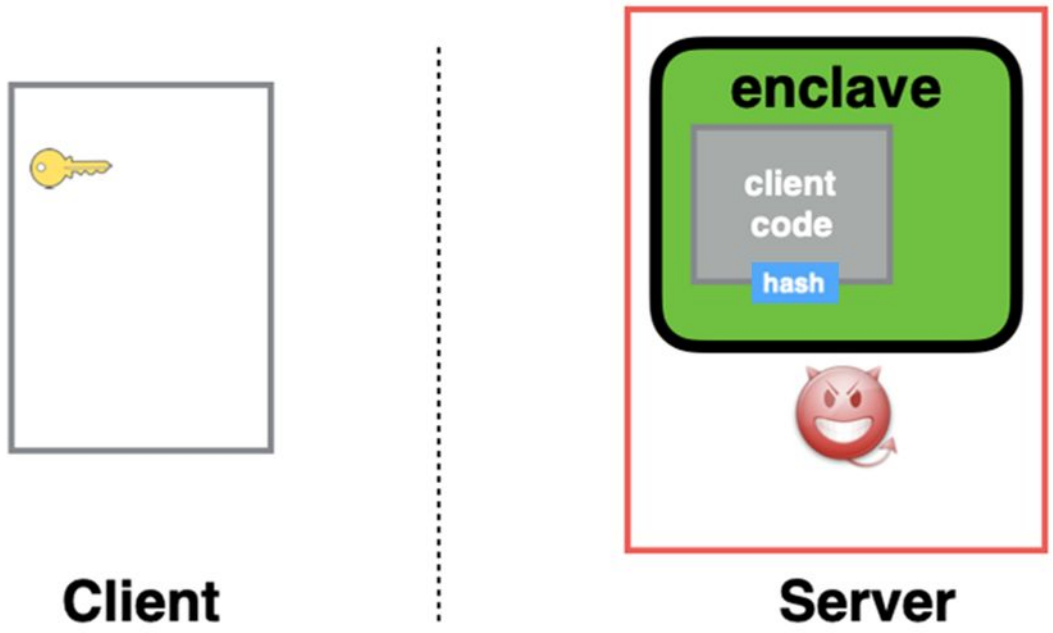
Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.



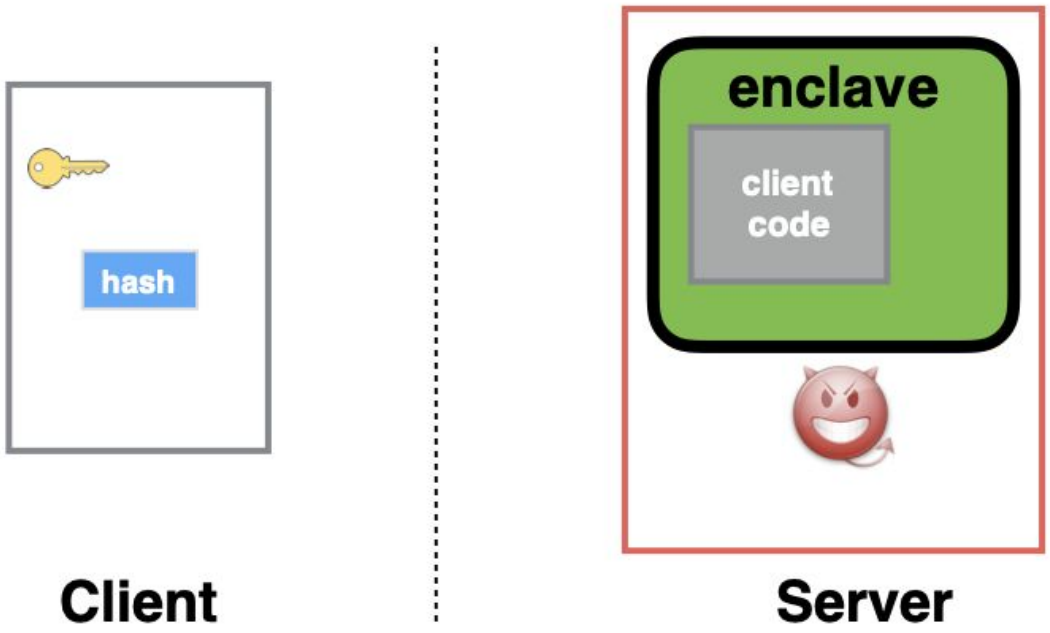
Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.



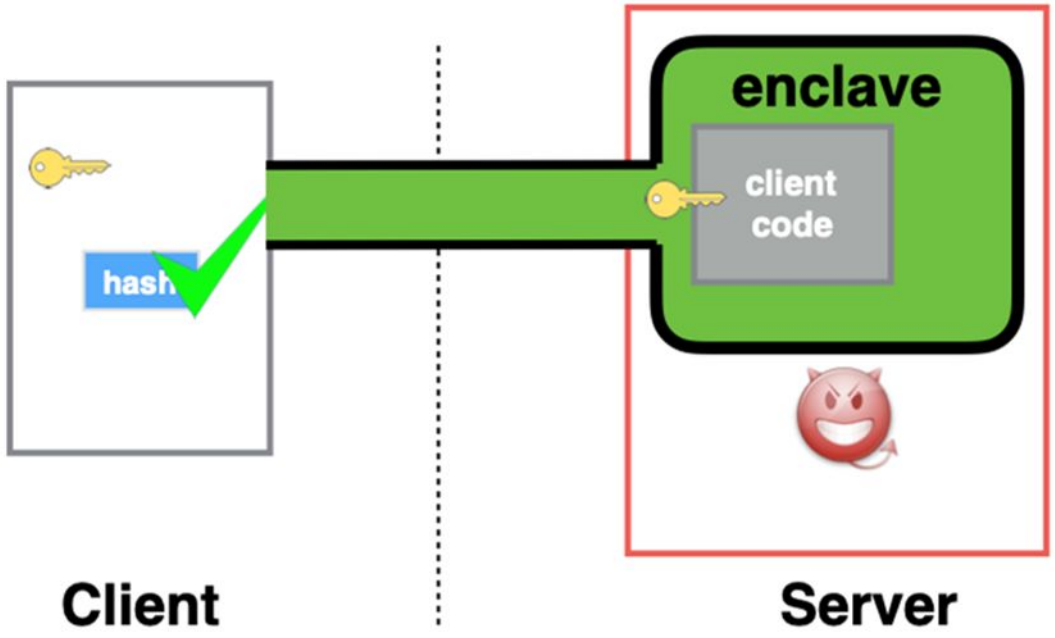
Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.



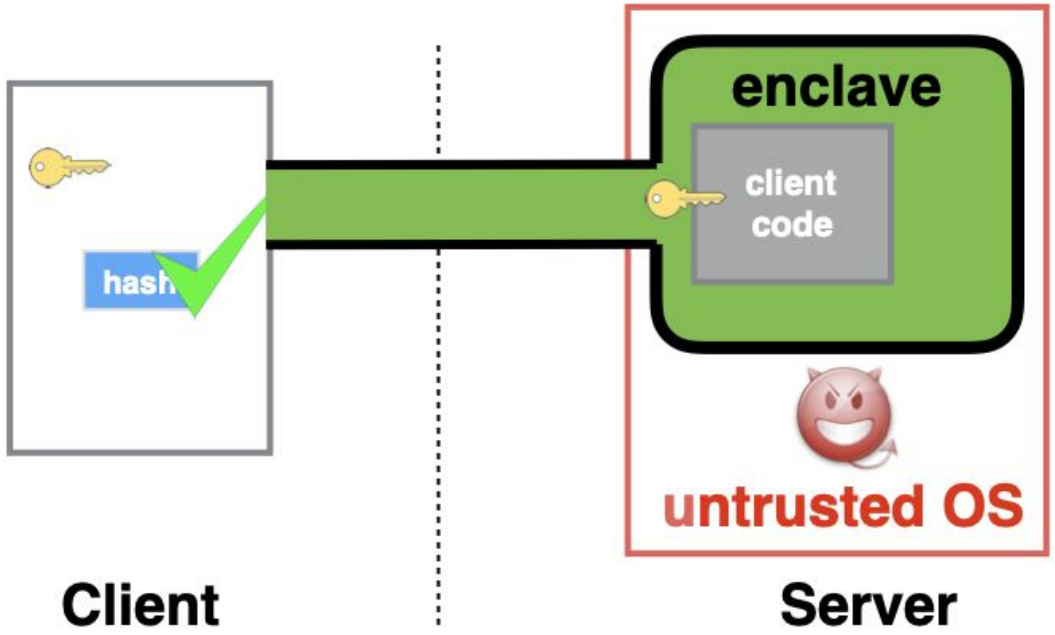
Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.

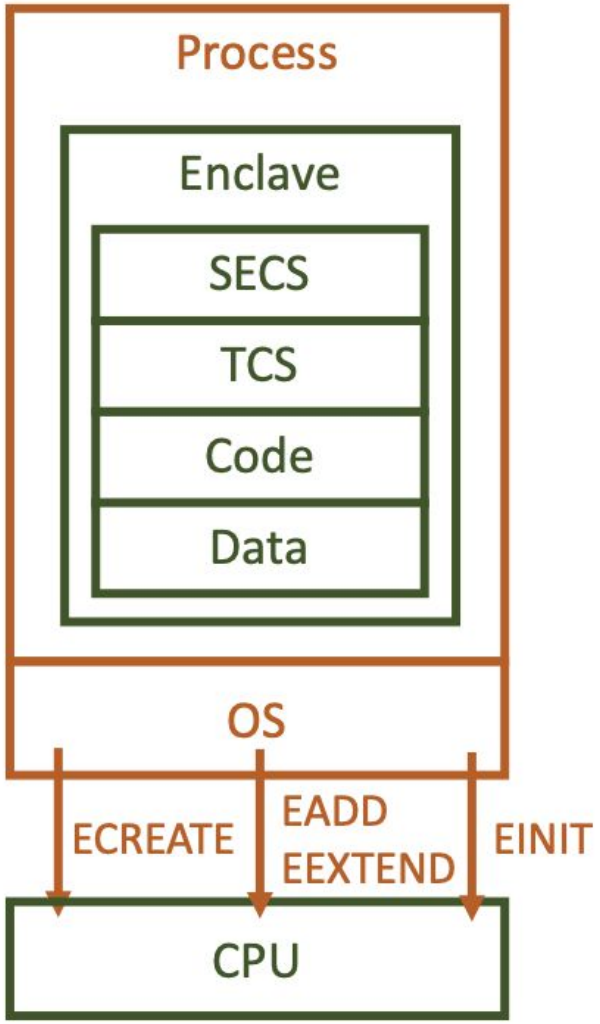


Remote Attestation

Enables verifying which code runs in the enclave and performing key exchange. With this, you can bootstrap end-to-end encryption between your clients and the authenticated (trusted) code of your application.

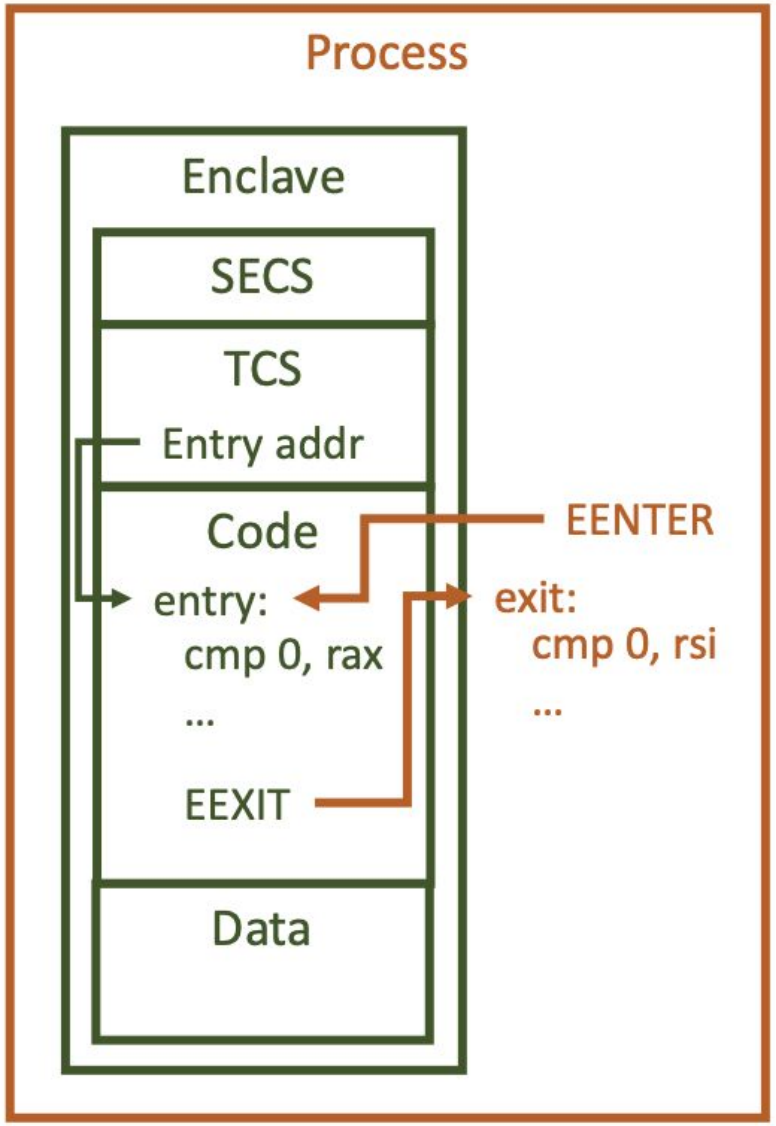


Enclave Creation with Intel SGX



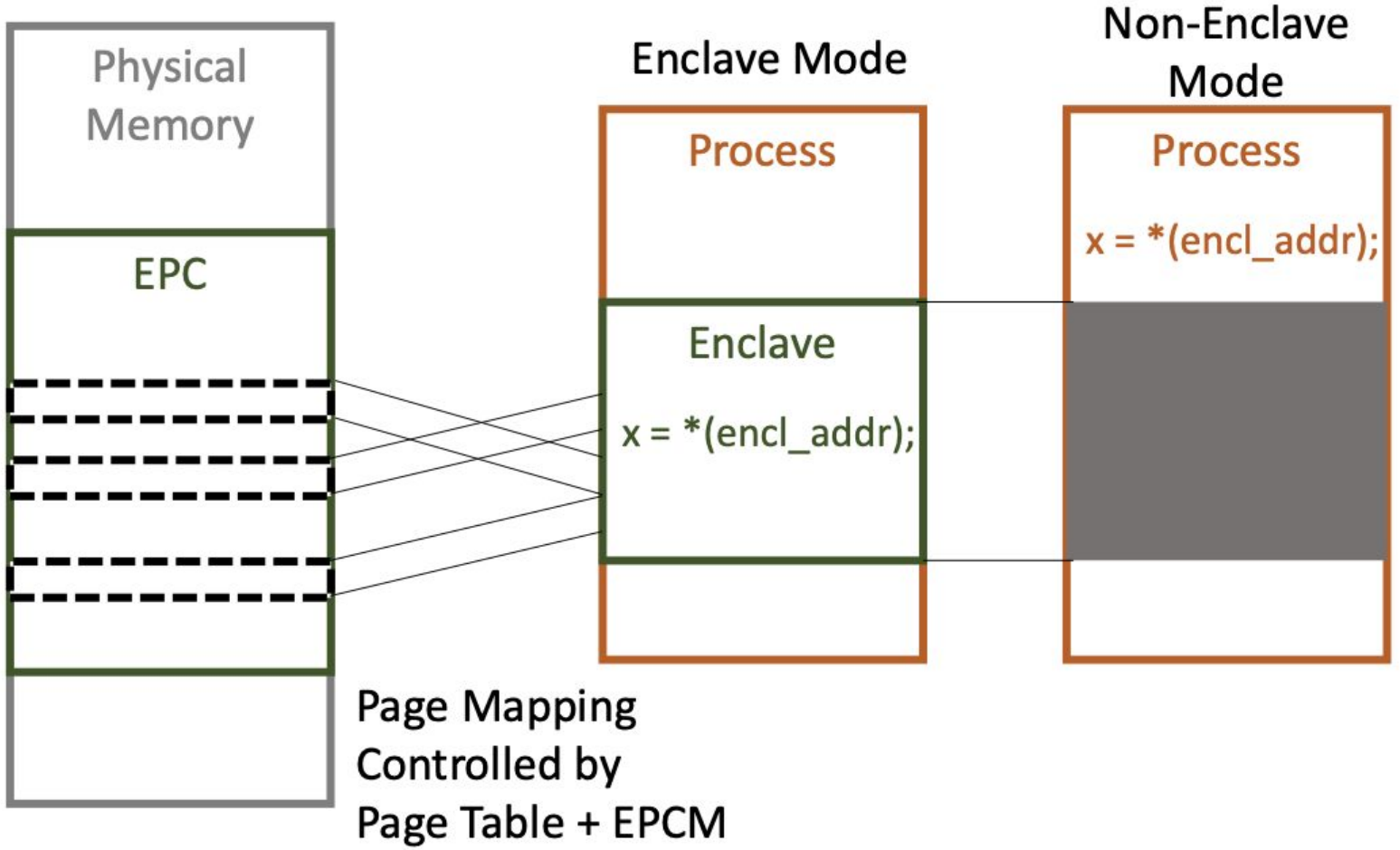
- ECREATE(SECS):
  create an enclave range
- EADD(SECS, addr, prot),
  EEXTEND(SECS, addr):
  add a page to enclave and measure the content
- EINIT(SECS, license):
  check & initialize an enclave

Enclave Enter & Exit



- EENTER(SECS, TCS):
  enter at a static enclave addr
- EEXIT(addr):
  exit enclave to any addr
- Enclave can accept parameters after the entry
- Attackers cannot interfere control flow unpredictably

Enclave Isolation



Abort page semantic:

EPC pages contains all 0s for execution outside the enclave

Existing Systems

Hardware enclaves are a very real technology that is available in multiple clouds, e.g.:

- Amazon: AWS EC2 Nitro Enclaves
- Microsoft: Azure SGX Enclaves
- Google: GCP Asylo

The End