Trusted Execution Environment – Concept, Major Security Problem & Examples

Eom, Hyeonsang (엄현상)
Department of Computer Science & Engineering
Seoul National University (SNU)

2022.5.24
서울대학교 우리은행 교육과정 핀테크 산업 응용 3차시 강의

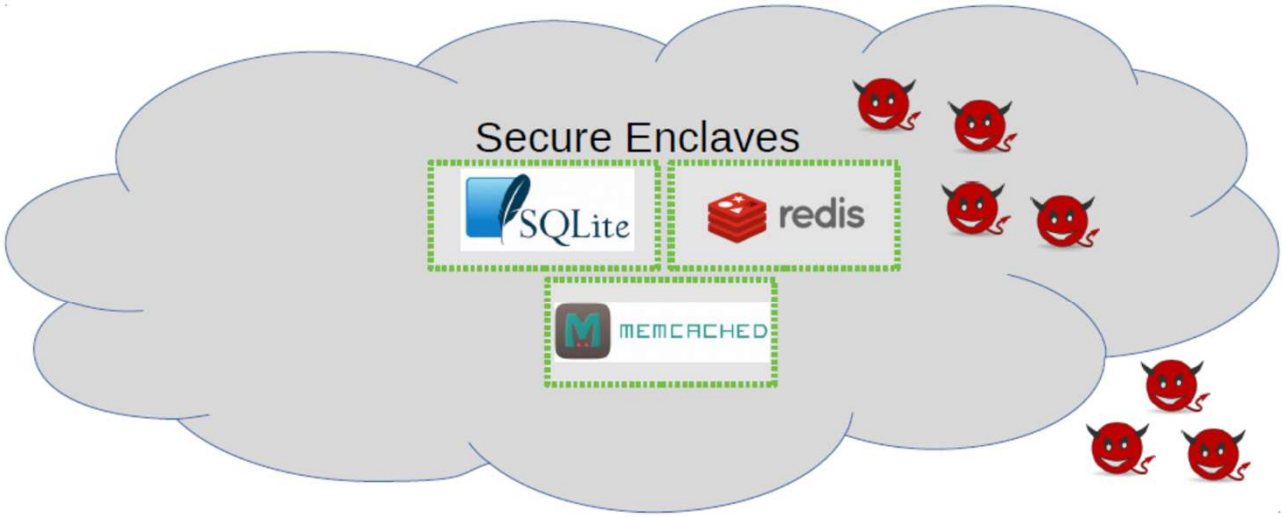
Index

- Risk Factor in the Public Cloud
- Trusted Execution Enviornment
- Enclave
- SGX
- Problems (Side-channel Attack)
- SCONE & Opaque

Risk Factor in the Public Cloud

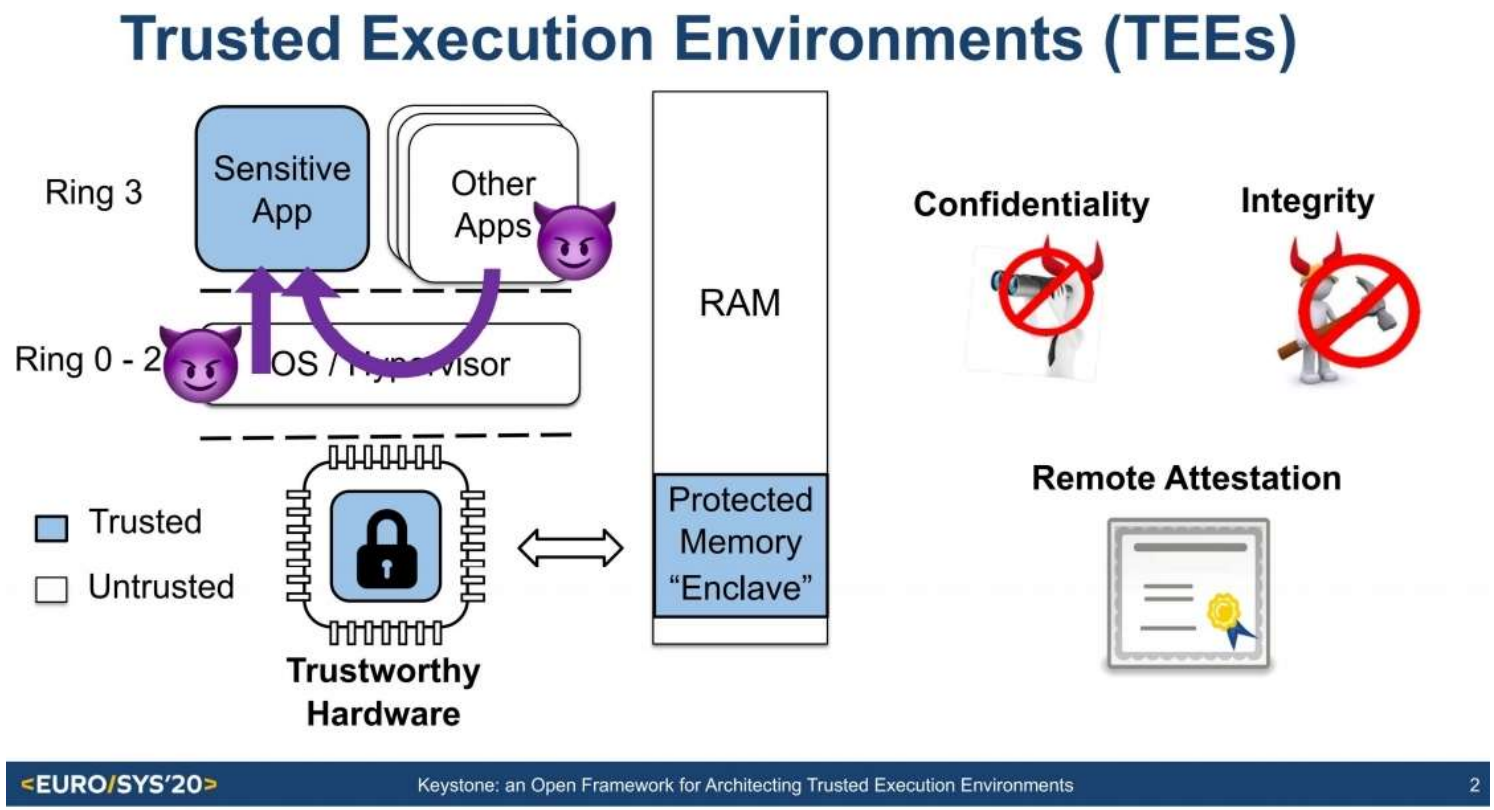
- Public cloud

Risk Factor in the Public Cloud (Cont'd)



- Cloud is dark and full of terrors
  - But, hardware enclaves can help

Trusted Execution Environment



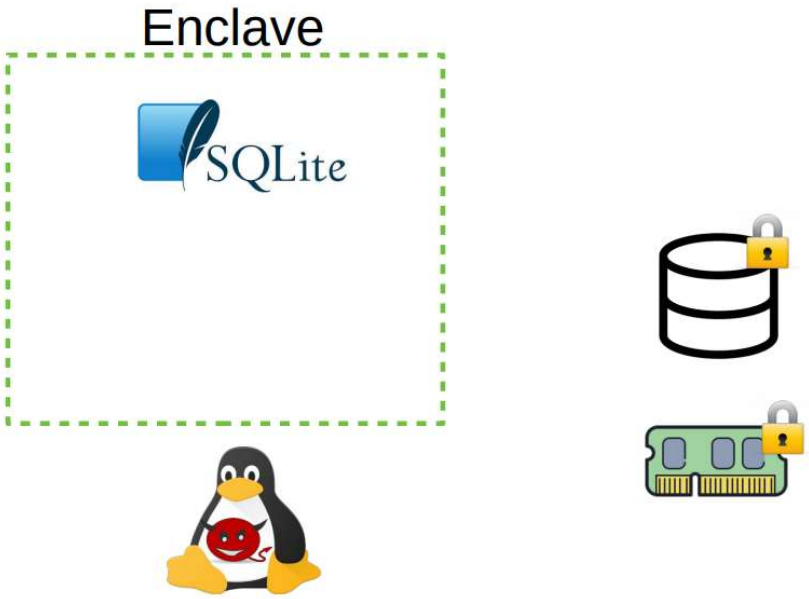
[*Keystone*]

Enclave

- Secure enclave
  - A hardware component
  - Protected by locked-down hardware in the CPU that safeguards data being processed from attack and attempted access outside the TEE (Trusted Execution Environment)
  - Making it difficult for attackers to unscramble private data without legitimate approval even with the physical access to the infrastructure

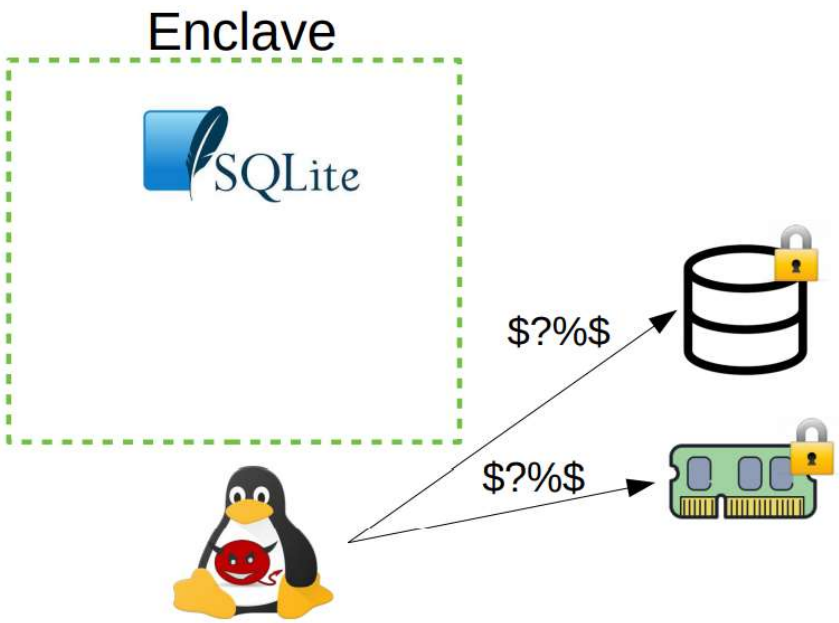
Enclave (Cont'd)

- Enclaves shield application from privileged adversaries



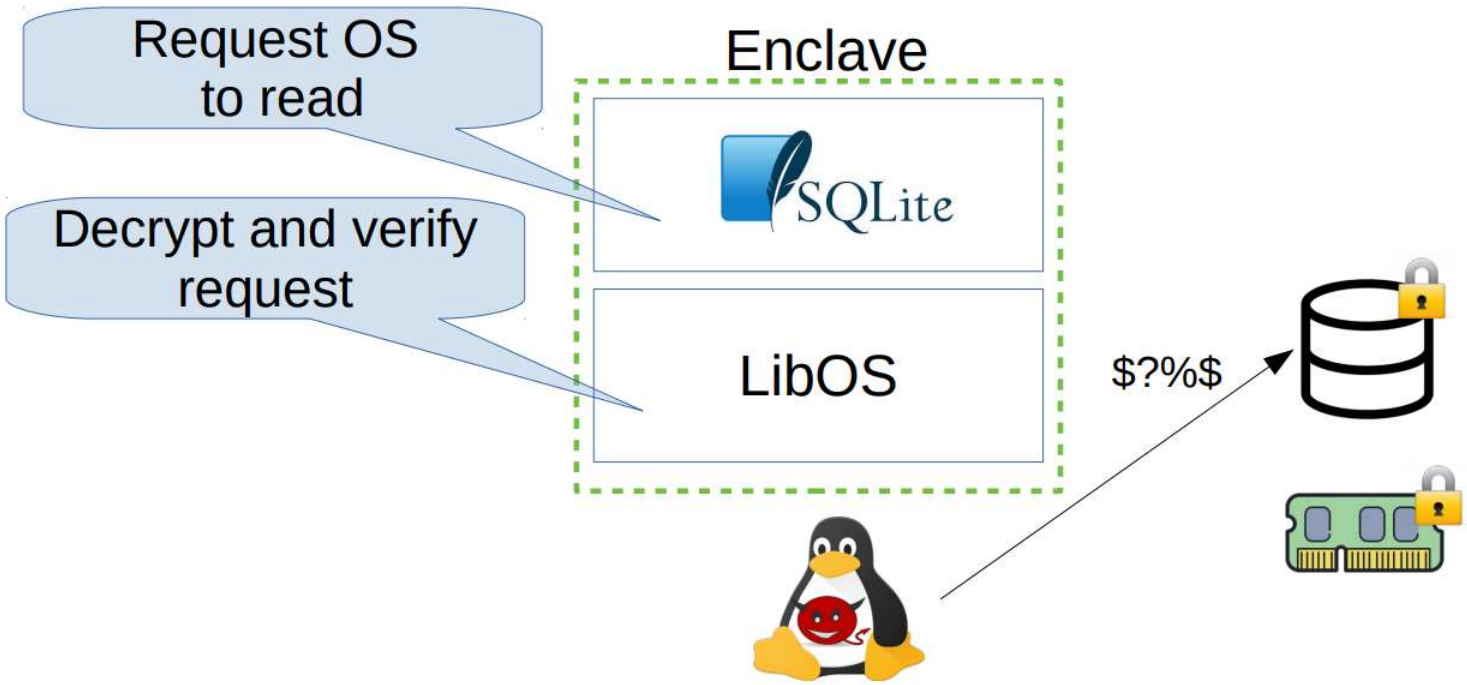
Enclave (Cont'd)

- Enclaves shield application from privileged adversaries



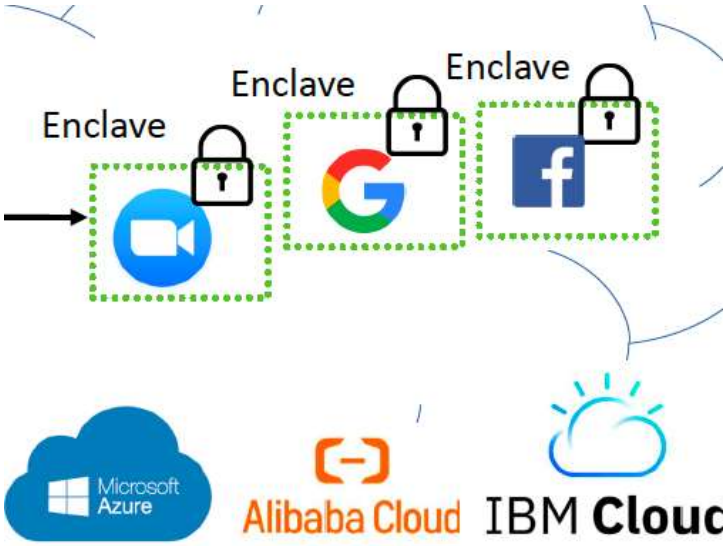
Enclave (Cont'd)

- Run unmodified applications inside enclaves by using a LIB OS

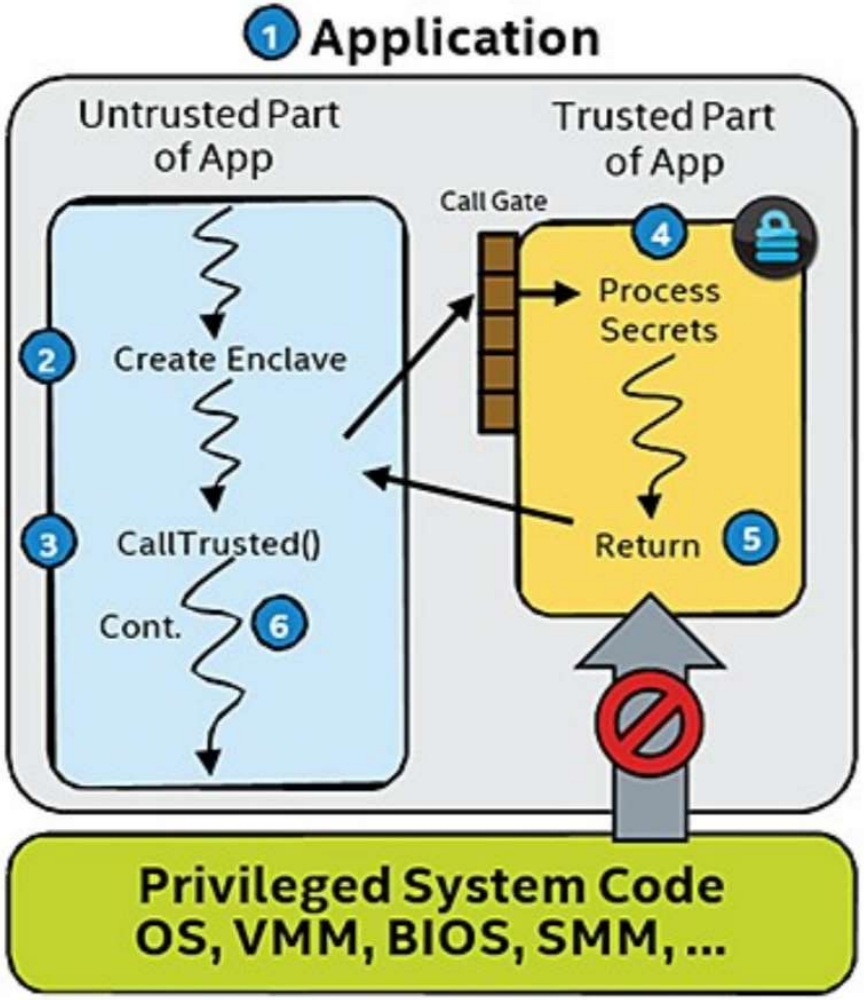


Intel SGX (Software Guard Extensions)

- Isolated user-mode environment
- Commodity CPUs
- Small trusted computing base
  - CPU
  - Enclave's code and data
    - Confidentiality
    - Integrity



Intel SGX (Software Guard Extensions) (Cont'd)



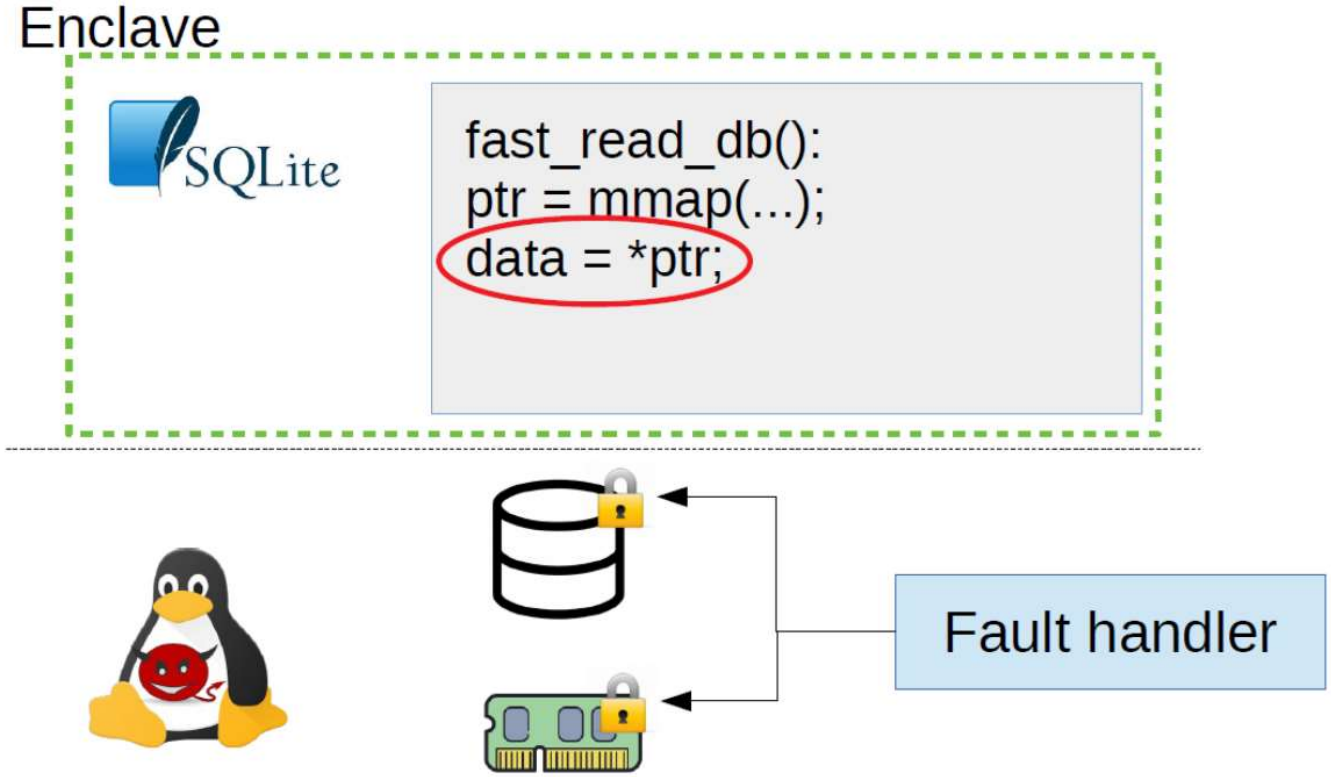
- App is built with trusted and untrusted parts
- App runs and creates the enclave, which is placed in trusted memory
- Trusted function is called, and execution is transitioned to the enclave
- Enclave sees all process data in the clear; external access to the enclave is denied
- Function returns; enclave data remains in trusted memory
- Normal execution resumes

Question

Can we execute any x86 application inside **enclaves**?

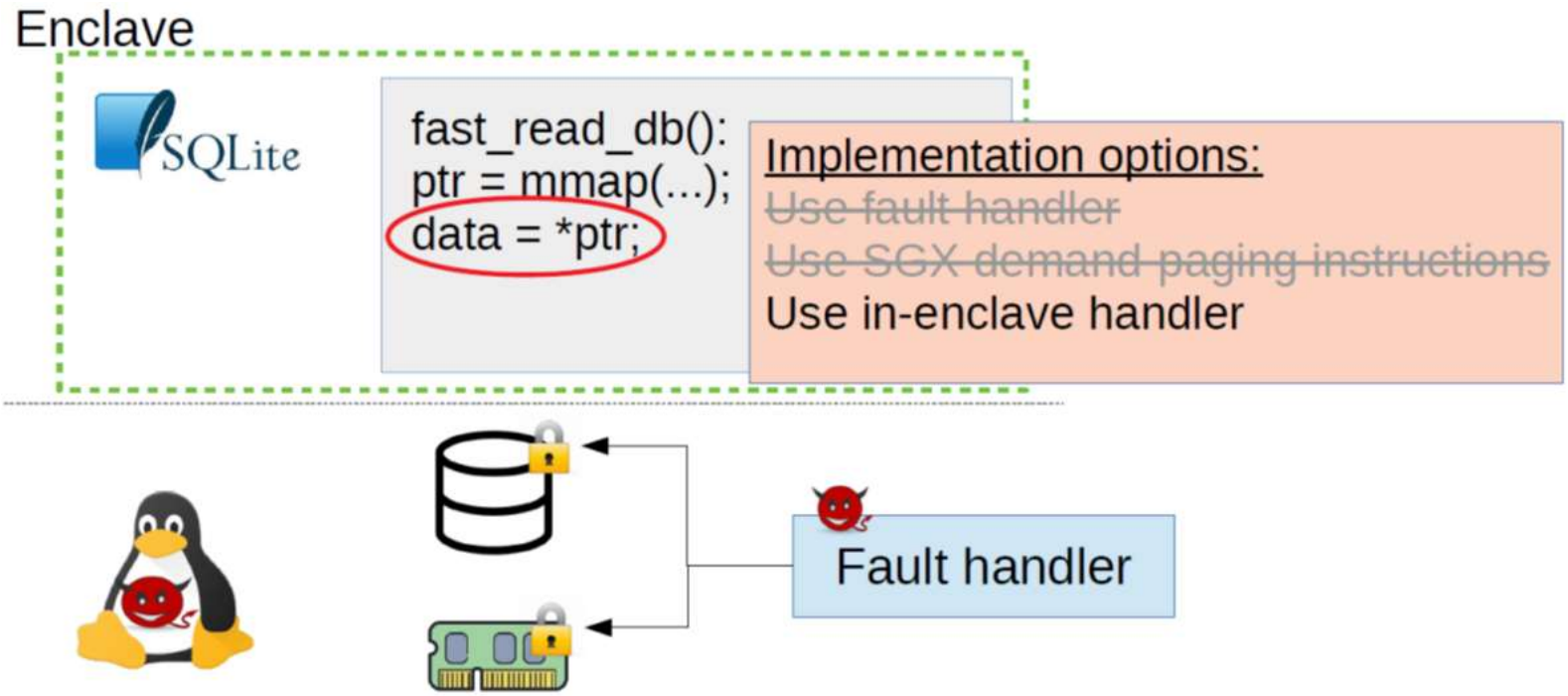
Problems (Side-channel attack)

- Memory-mapped files in SGX



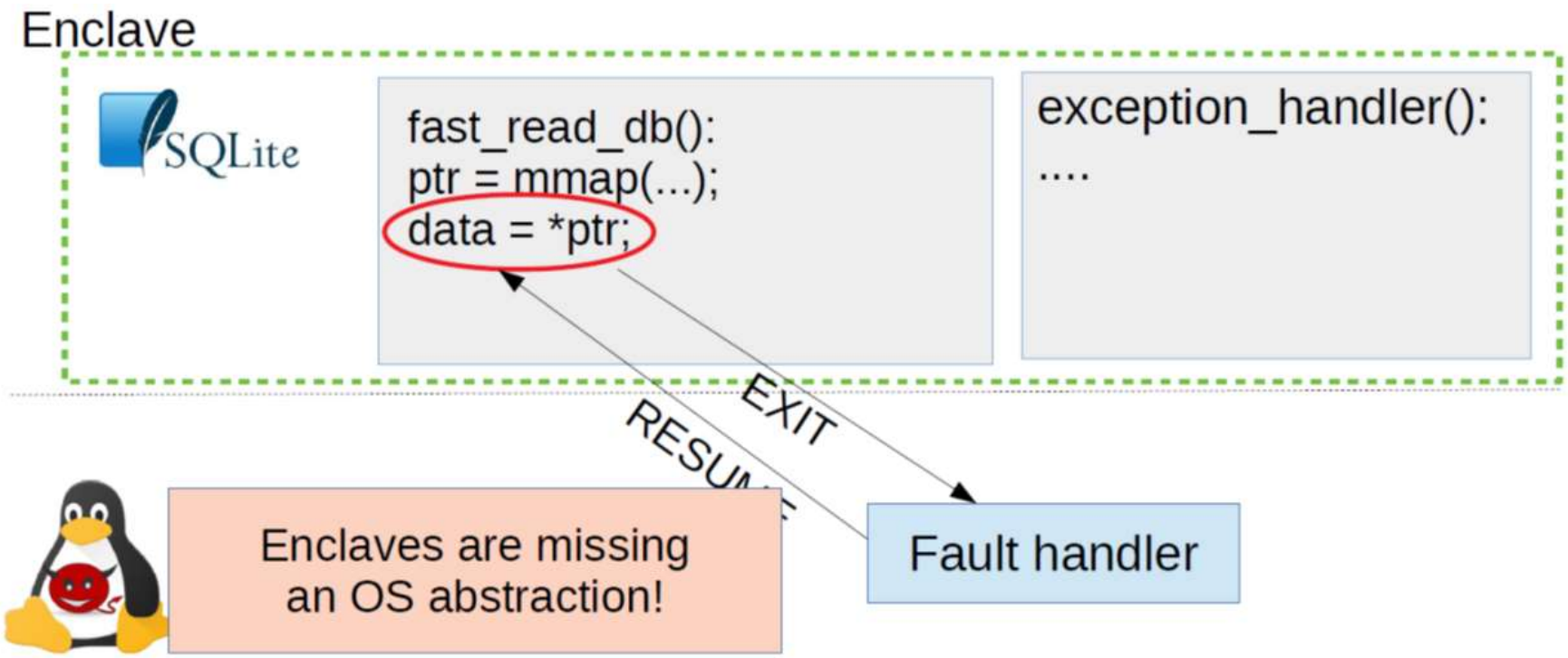
Problems (Side-channel attack) (Cont'd)

- Memory-mapped files in SGX



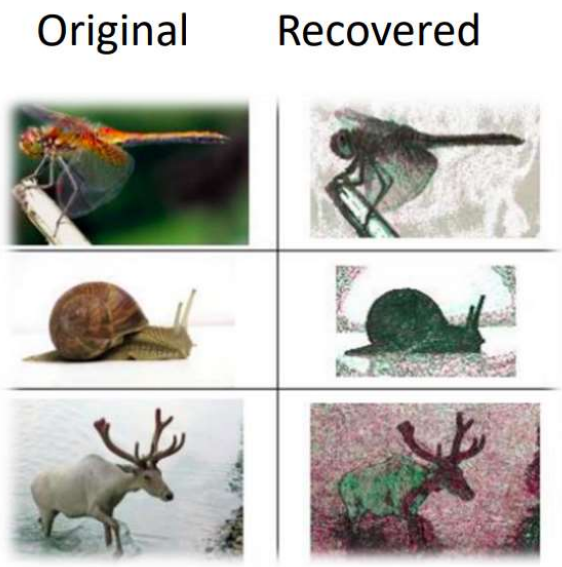
Problems (Side-channel attack) (Cont'd)

- Insecure: in-enclave handler



Problems (Side-channel attack) (Cont'd)

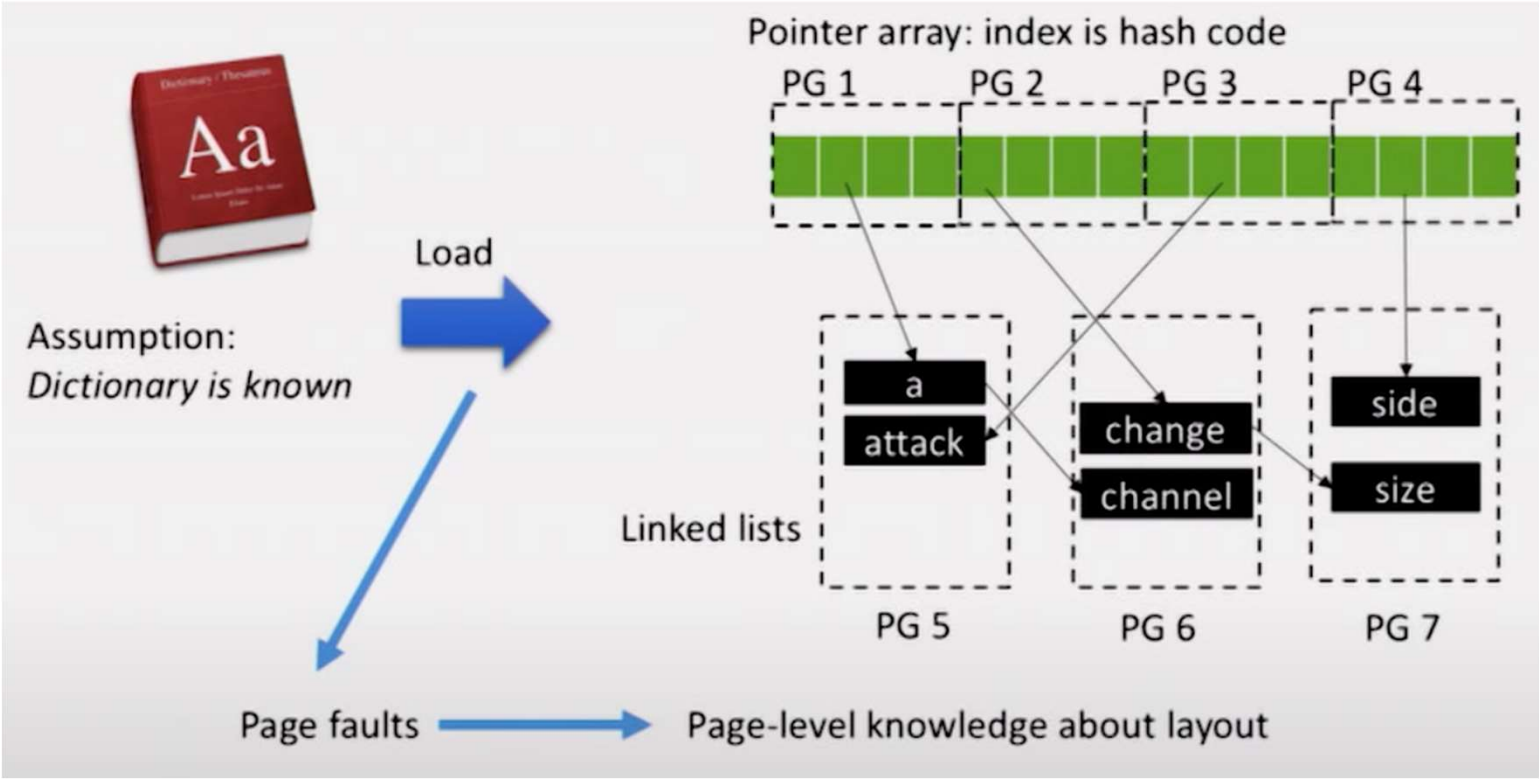
- OS-level attacker
  - Induces page faults
  - Tracks faulted address
  - Infer secrets content that depends on page address pattern
    - Control-dependent accesses
    - Data dependent accesses



Xu, Y., Cui, W. and Peinado, M., 2015. **Controlled-Channel Attacks:** Deterministic Side Channels for Untrusted Operating Systems.

Problems (Side-channel attack) (Cont'd)

- Example : Hunspell – hash table



Problems (Side-channel attack) (Cont'd)

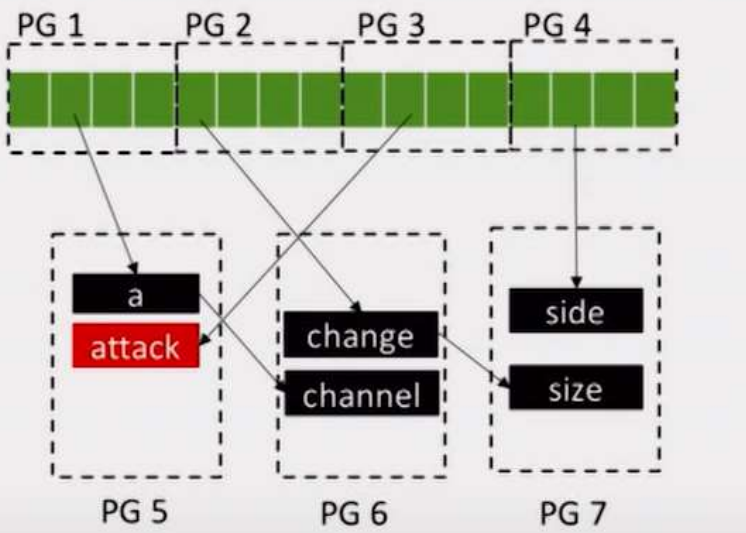
- Example : Hunspell – hash table

Input: side channel attack

```
while (word) {
  n = hash(word);
  listnode = table[n];

  while (listnode) {
    if (equal(listnode, word))
      break;
    listnode = listnode->next;
  }

  if (listnode) success(); else failure();
  word = get_next();
}
```



Page faults:

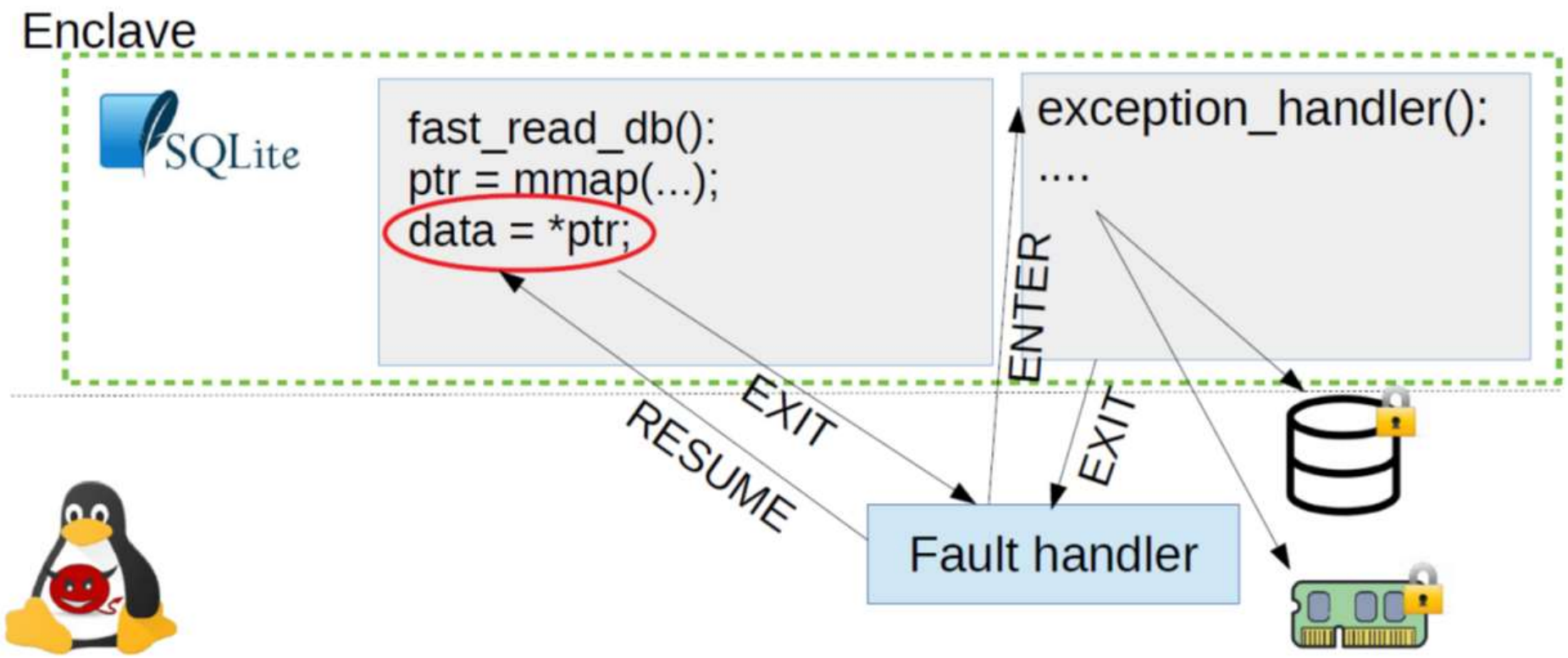
4 7 1 5 6 3 5

Problems (Side-channel attack) (Cont'd)

- Hunspell – hash table
  - ~96% accuracy for novel, "The Wizard of Oz"

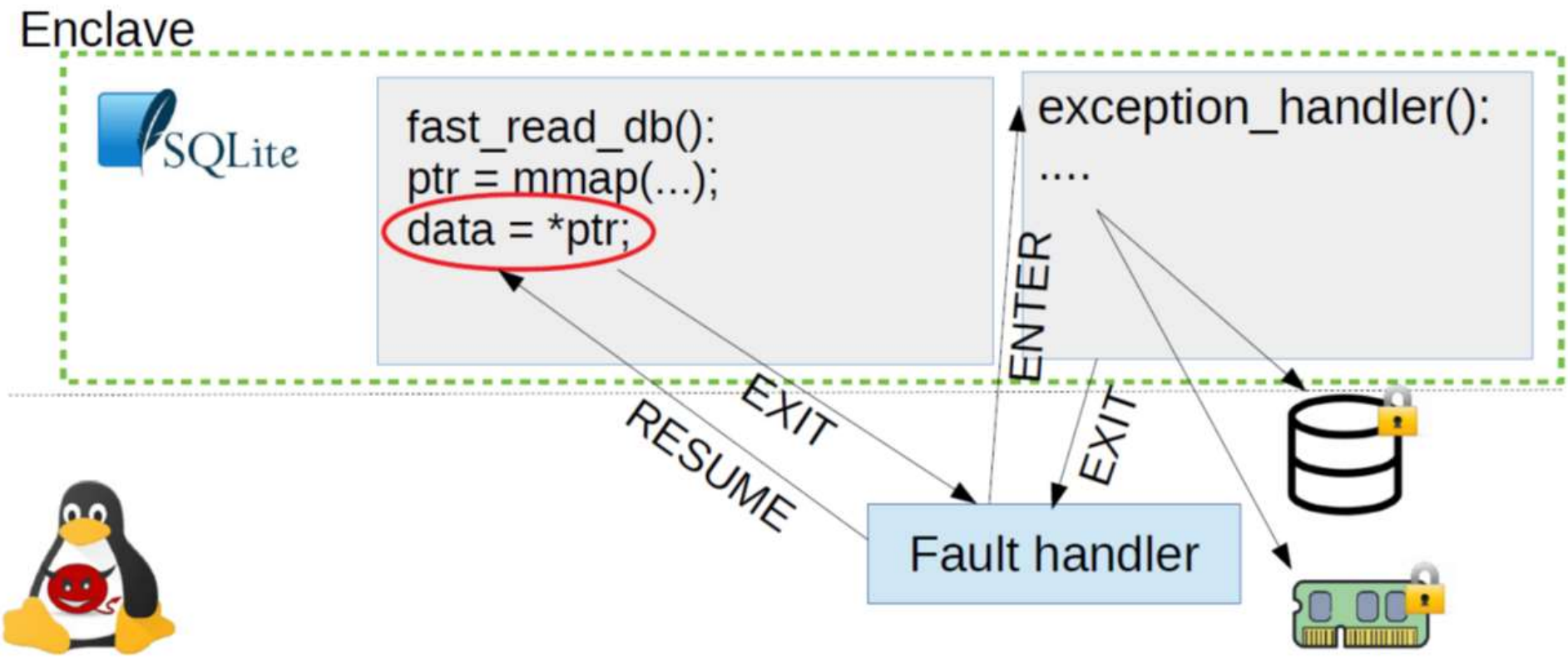
Problems (Performance)

- Inefficient: in-enclave handler



Problems (Performance) (Cont'd)

- Inefficient: in-enclave handler



SCONE

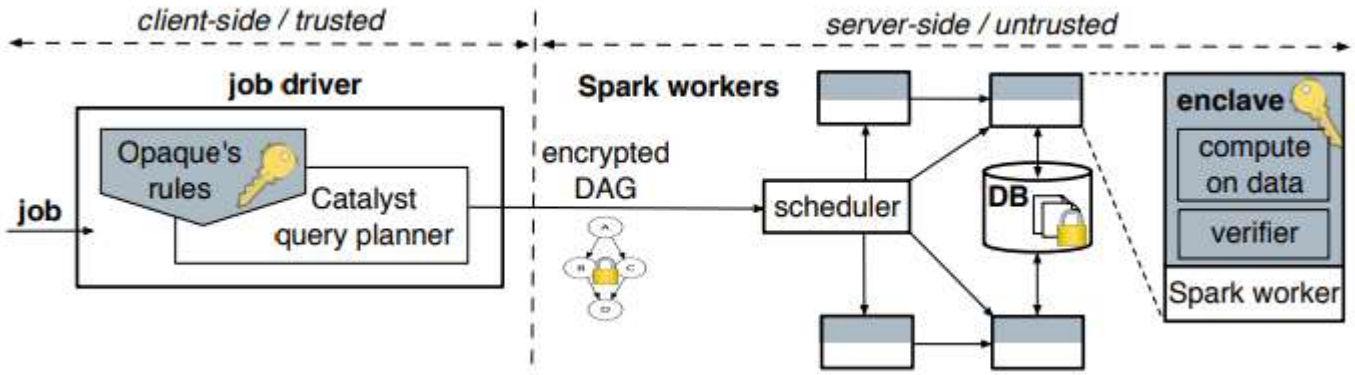
- SCONE
  - Uses Intel SGX to protect a container process
  - Intel SGX protects the process from not only malicious programs but also malicious OS

- Problem
  - Intel SGX might not be good enough
    - Possible access pattern side-channel attack

[SCONE]

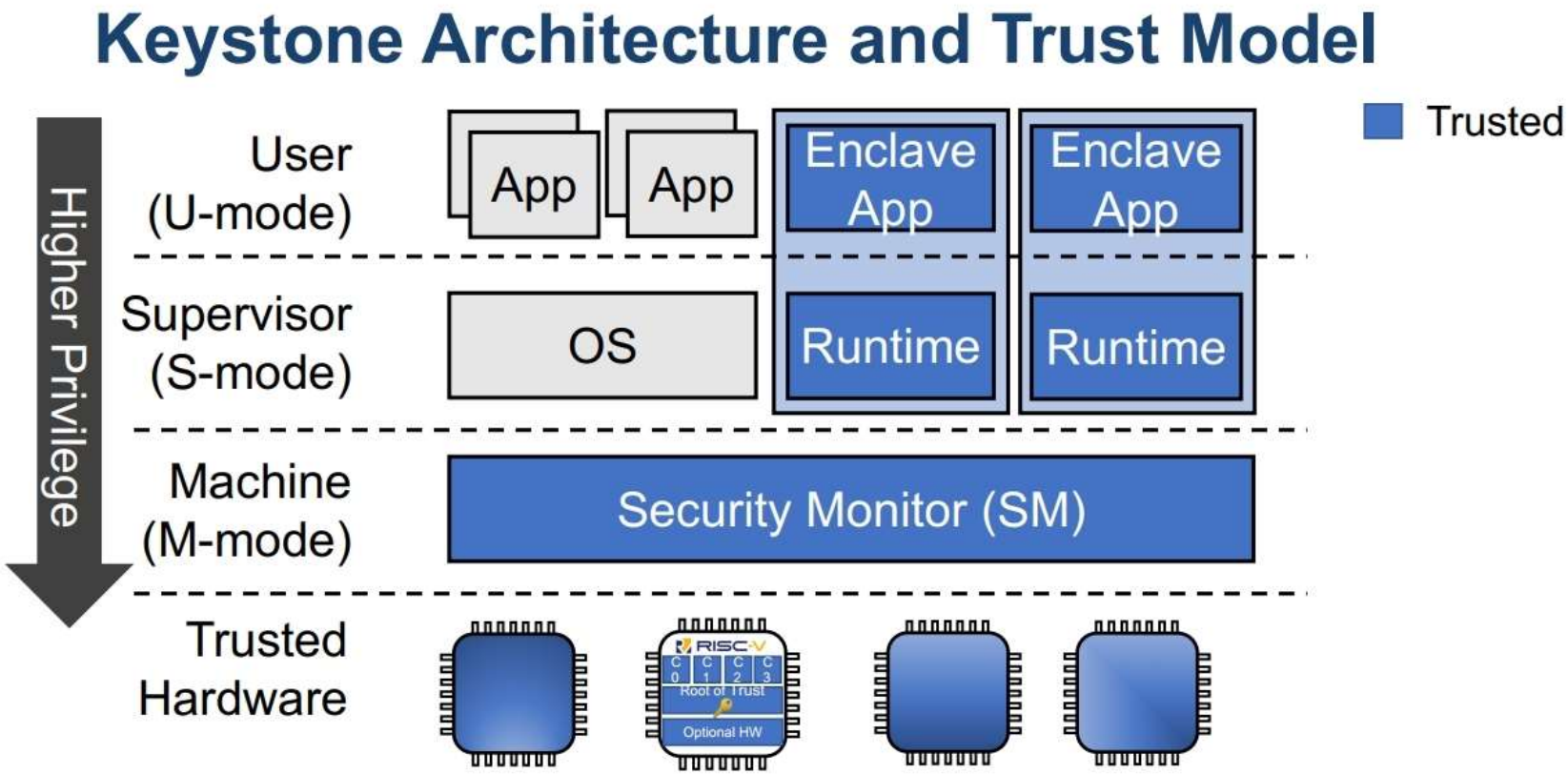
Opaque

- Opaque: An Oblivious and Encrypted Distributed Analytics Platform
  - NDSI' 17



Overall architecture of Opaque

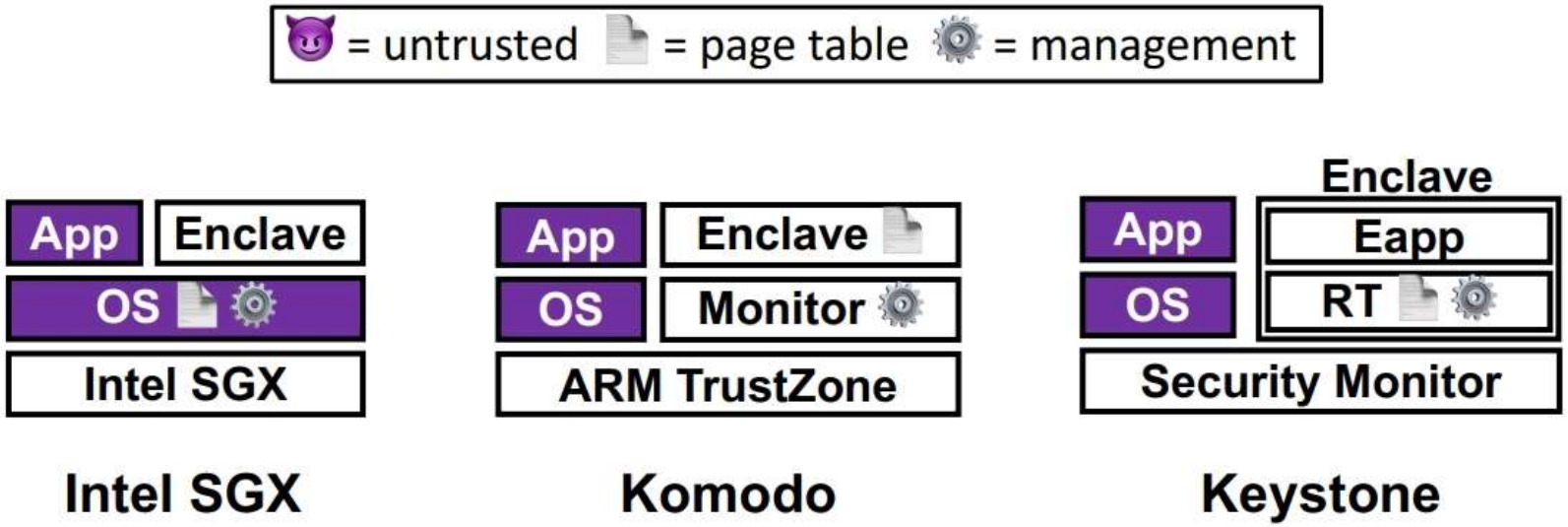
Keystone: An Open Framework for Architecting Trusted Executions



[*Keystone*]

Page Table Protection in Keystone

Memory Management in Keystone



- Enclave self resource management (e.g., dynamic memory resizing)
- Various memory protection mechanisms

[*Keystone*]

Thank You!

Eom, Hyeonsang (엄현상)

hseom@snu.ac.kr
Department of Computer Science & Engineering
Seoul National University

References

- Autarky: Closing controlled channels with self-paging enclaves, EuroSys 2020
- CoSMIX: A compiler-based system for secure memory instrumentation and execution in enclaves, ATC 2019
- Keystone: An Open Framework for Architecting Trusted Execution Environments, EuroSys 2020
- Opaque: An Oblivious and Encrypted Distributed Analytics Platform, NSDI 2016
- SCONE: Secure Linux Containers with Intel SGX, OSDI 2016