Trusted execution environment and software security

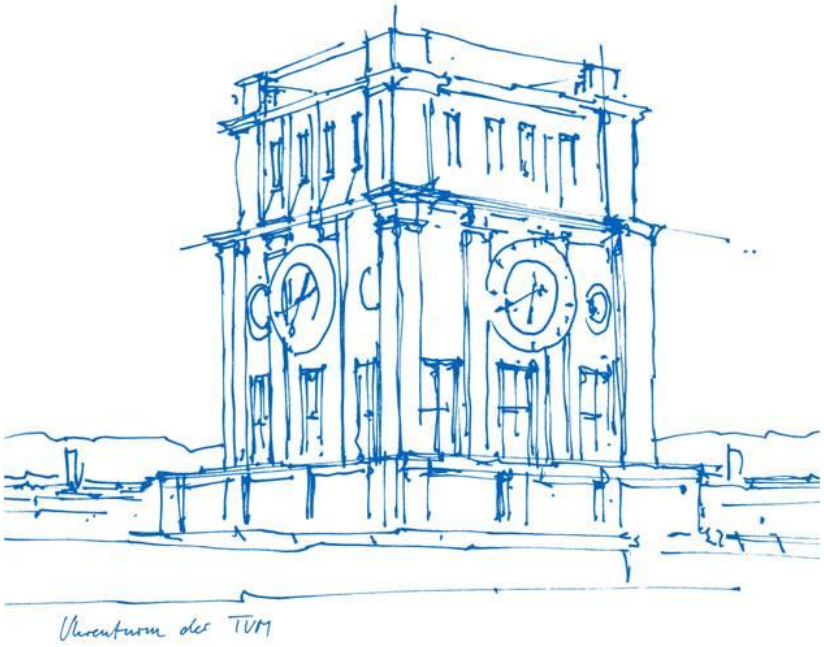
Peng Xu

peng@sec.in.tum.de

Lehrstuhl für IT-Security, Fakultät für Informatik,

Technische Universität München

23.04.2019



Agenda

- **Problems and Solutions**
  - Problems
  - Solutions
- **Trusted Execution Environment**
  - Architecture
  - Examples
- **Courses**
  - Content
  - Tasks and exercises
  - Requirements
  - Grading

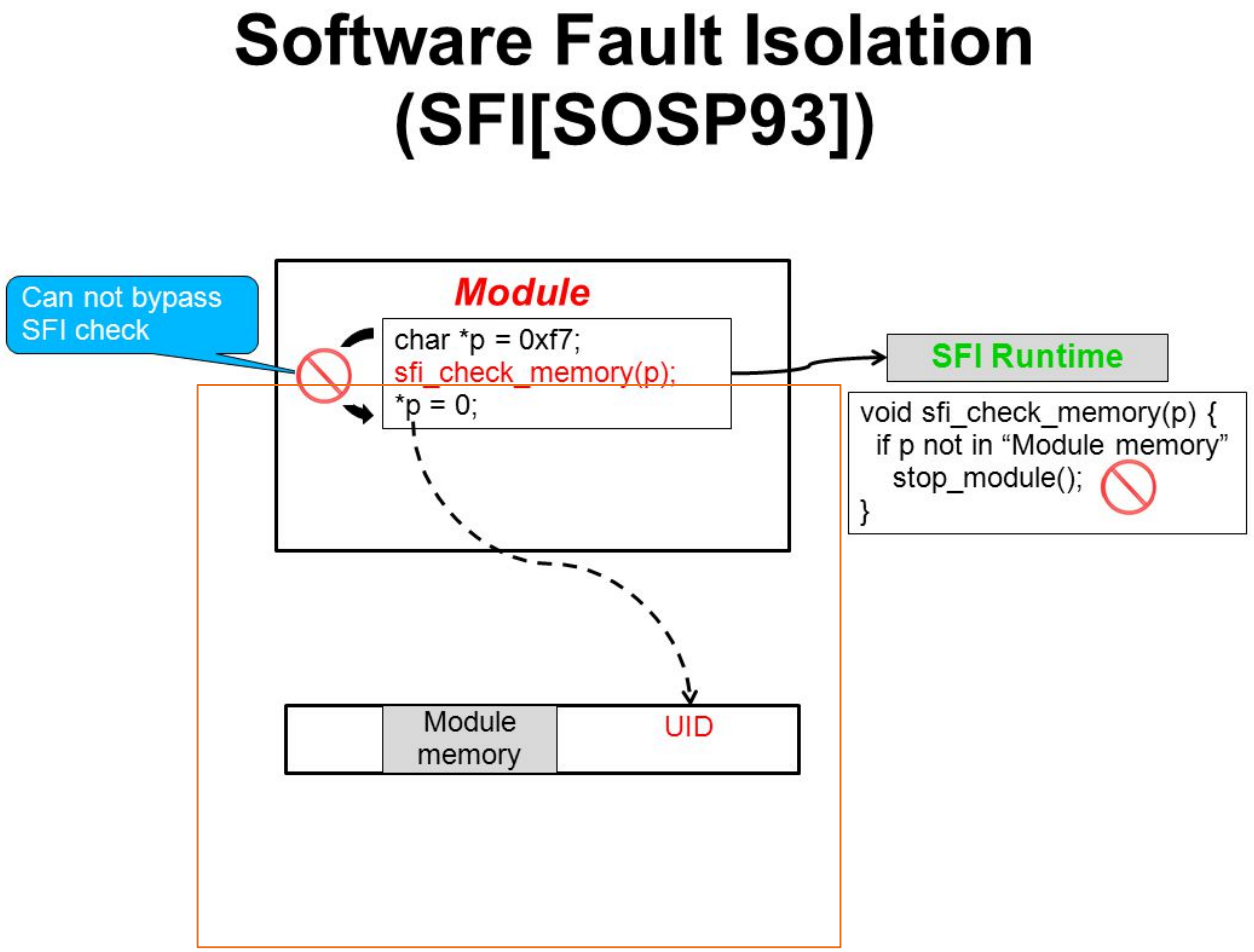
Problems?

Problems?

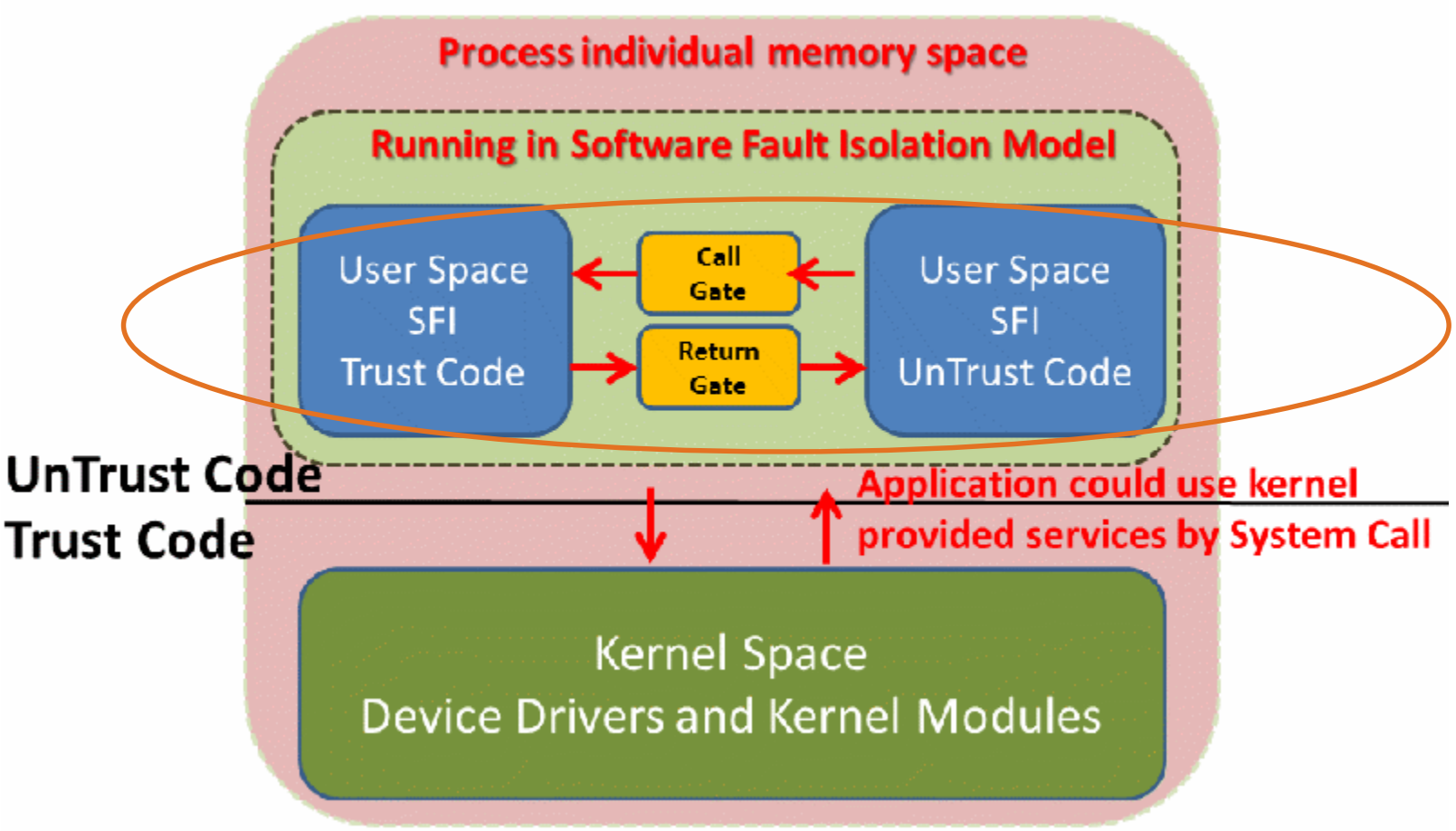
Problems?

Problems

Solutions – Software fault isolation

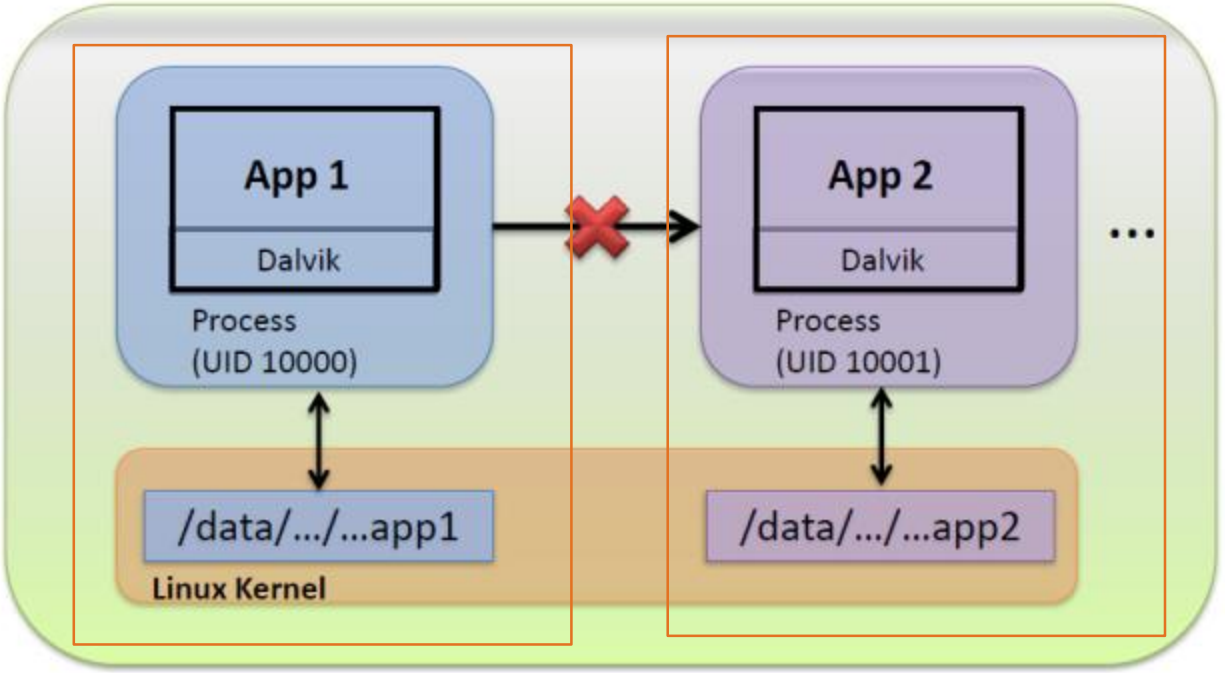


Solutions – Software fault isolation

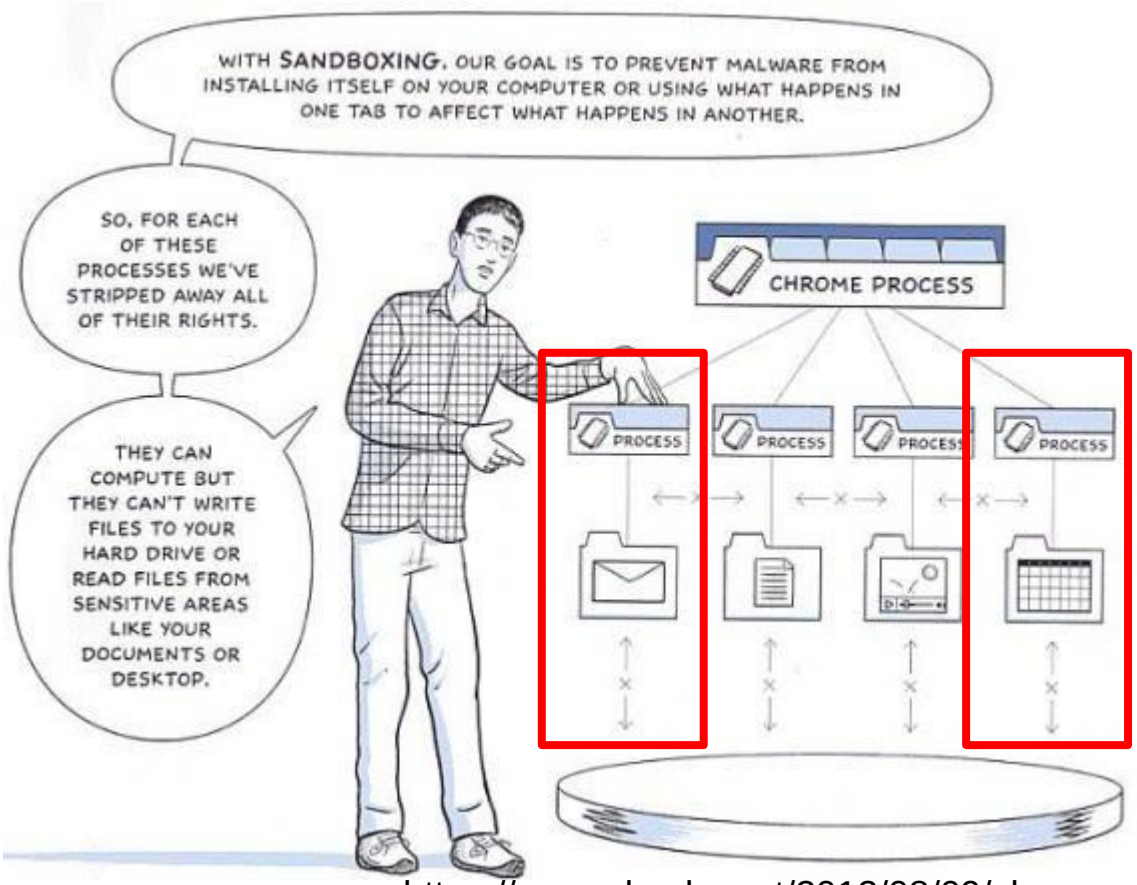


https://drive.google.com/file/d/0B5pbq4t2T2_fM2h1dnd3TFRud0E/view

Solutions – Sandbox

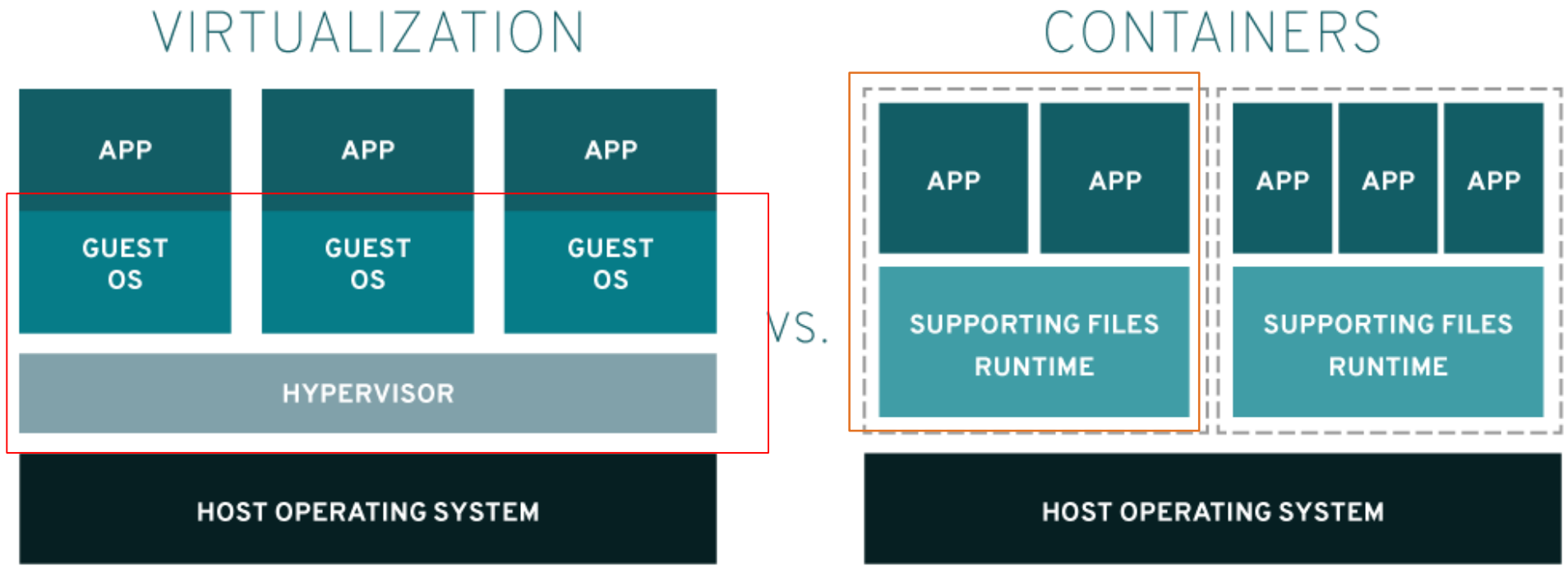


Solutions – Sandbox

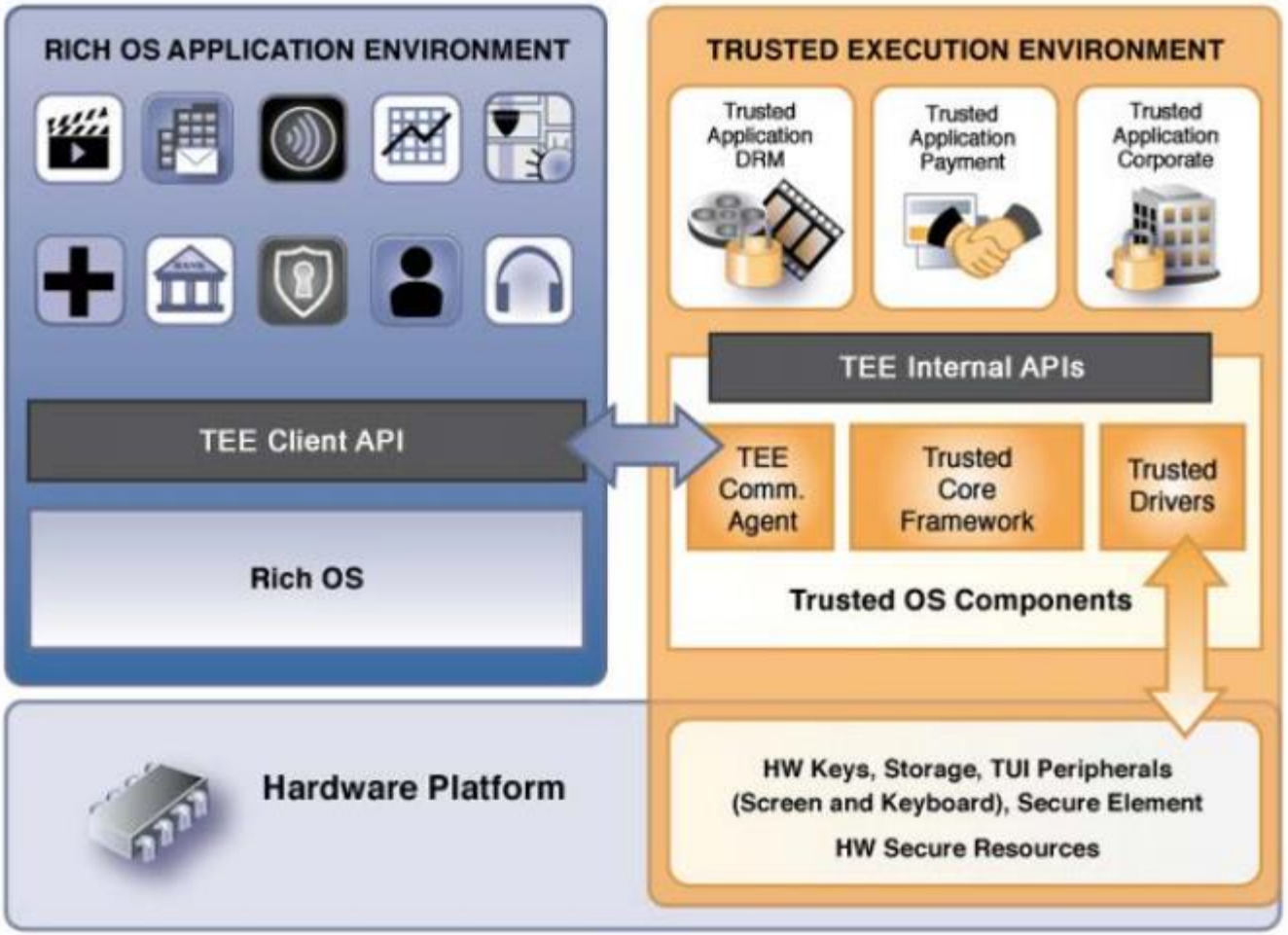


https://www.ghacks.net/2012/08/09/chromes-flash-sandbox-improves-with-better-security-less-crashes/

Solutions – Virtualization & Containers

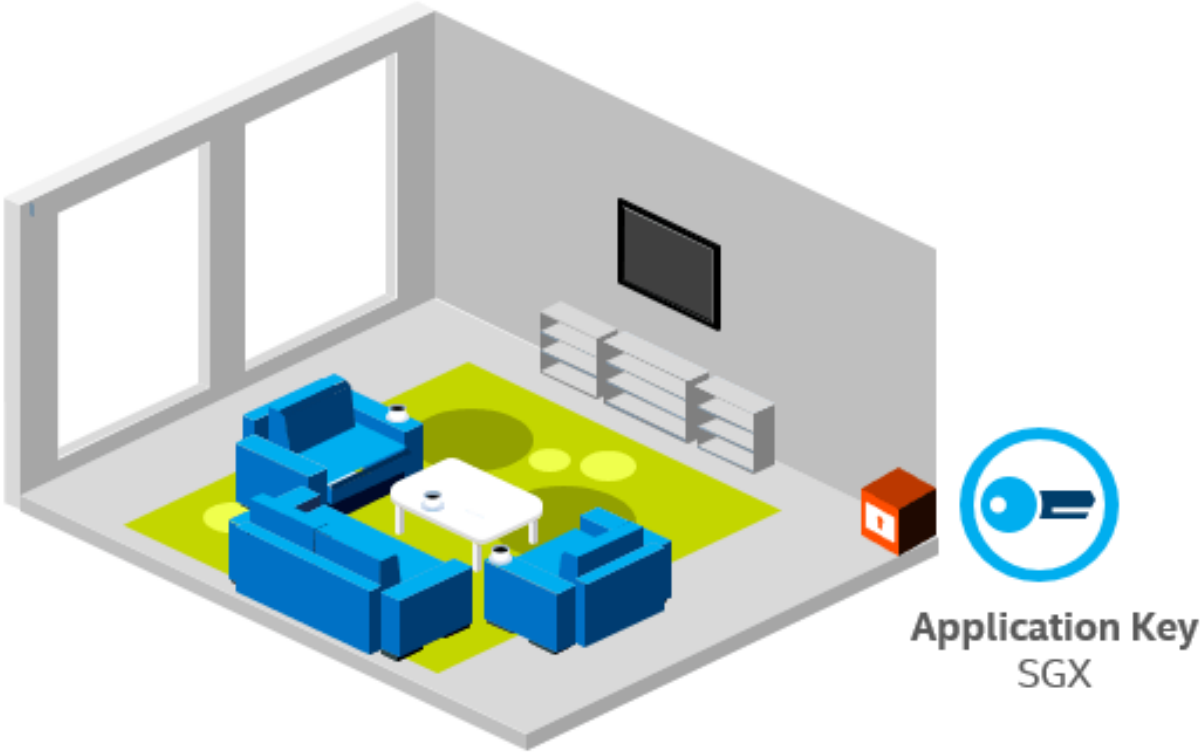


Solutions – Hardware isolation



- **Problems and Solutions**
  - Problems
  - Solutions

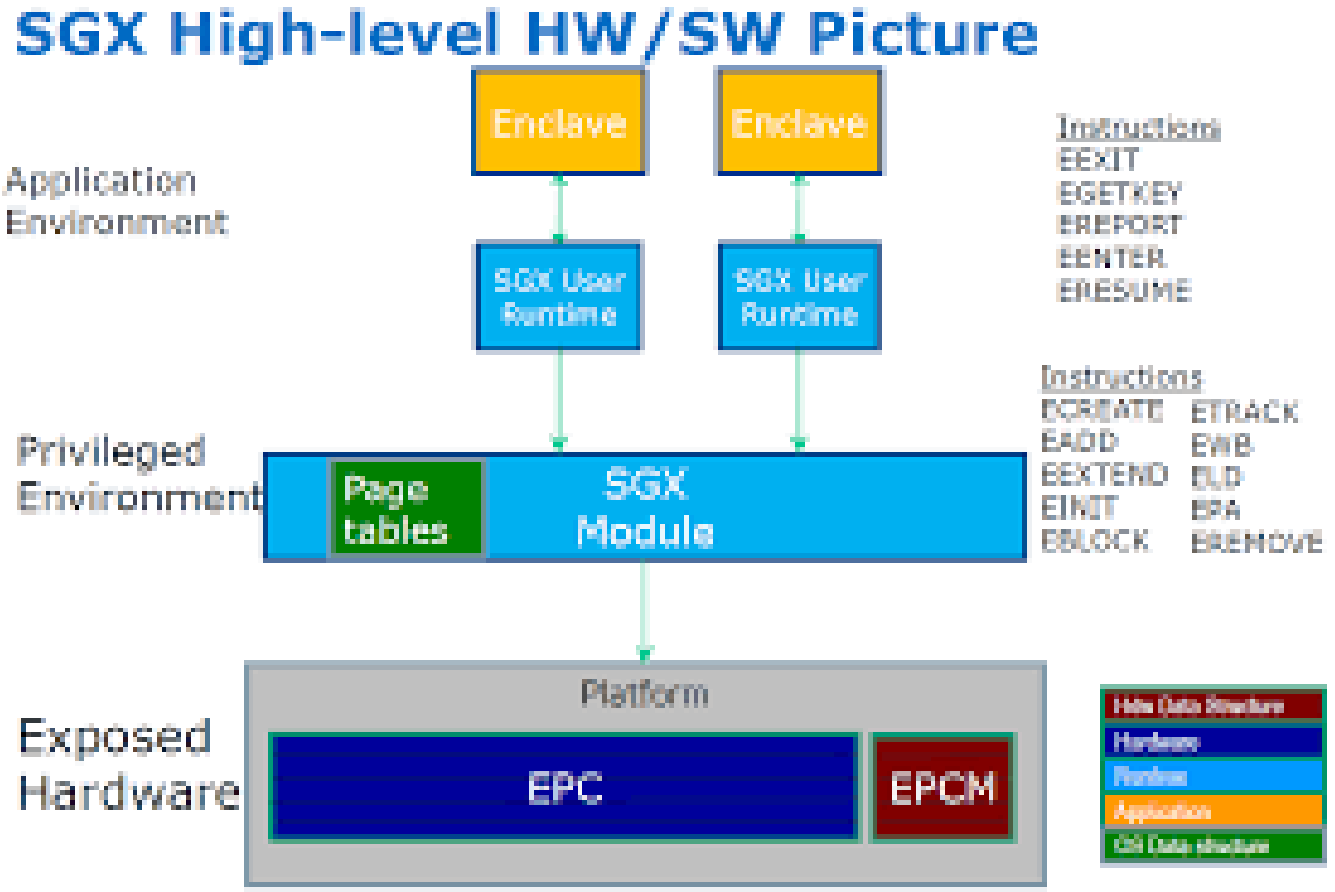
TEE Architecture – Intel SGX



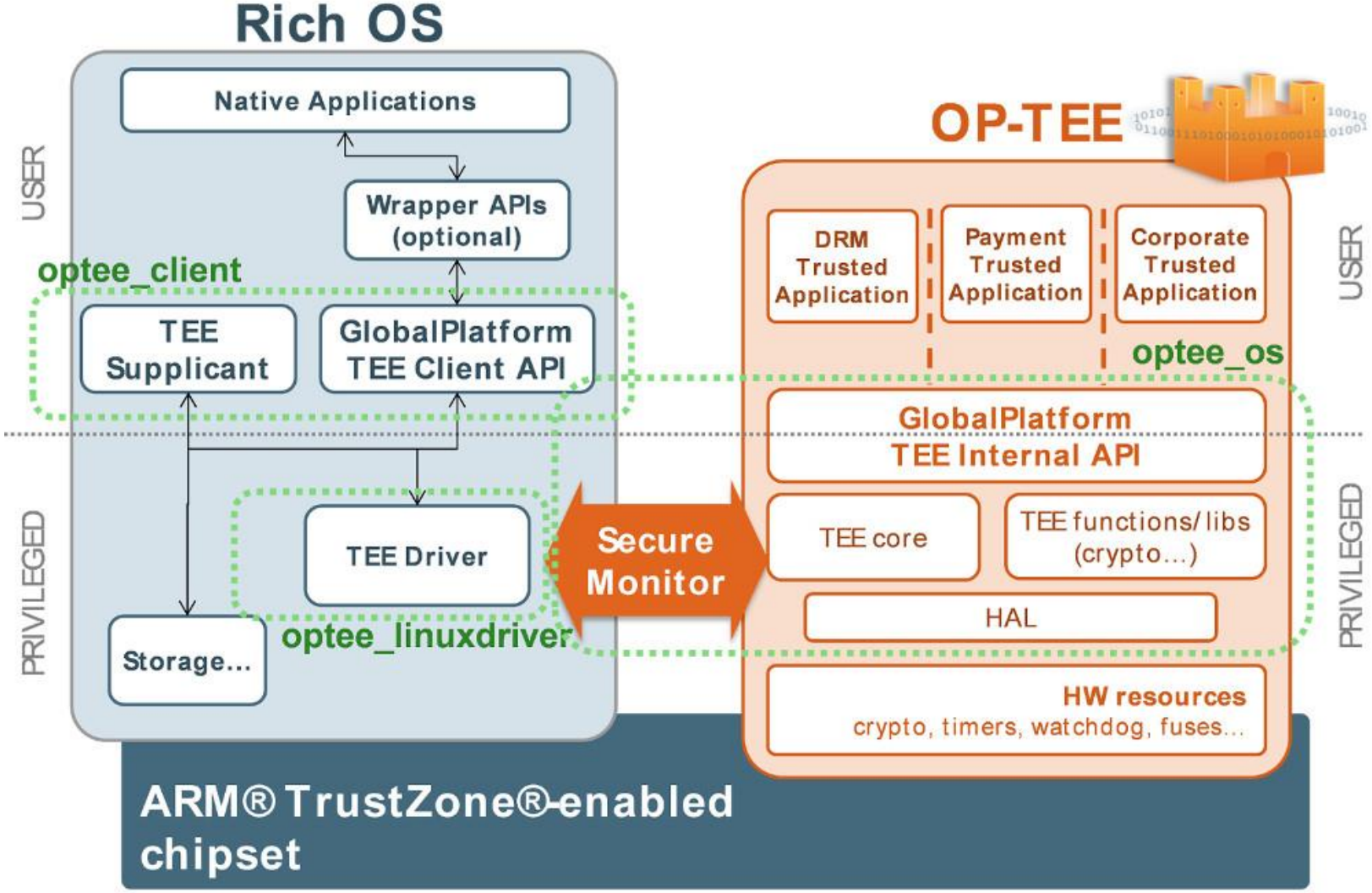
Intel® Software Guard Extensions (Intel® SGX)

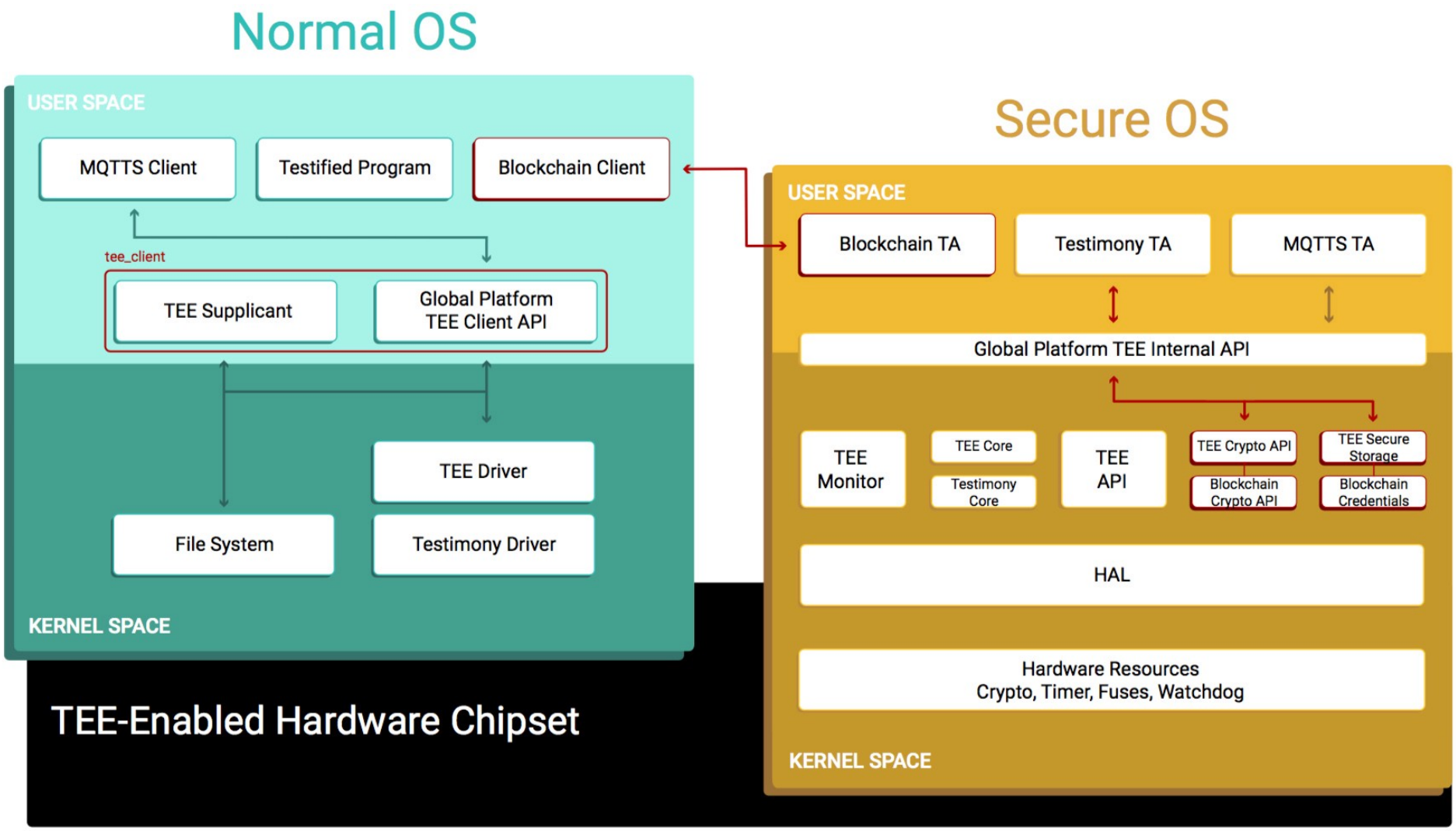
Isolation for individual application data spaces

TEE Architecture – Intel SGX



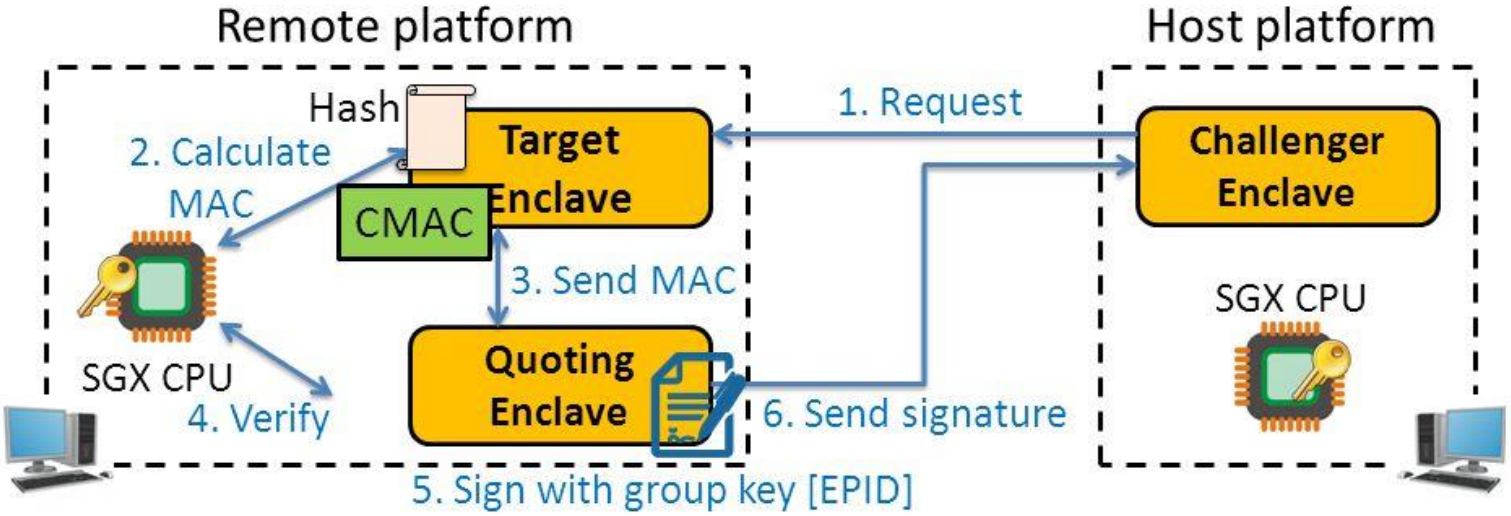
TEE Architecture – ARM TrustZone





https://medium.com/weeves-world/ethereum-wallet-in-a-trusted-execution-environment-secure-enclave-b200b4df9f5f

SGX : Remote Attestation



- Attest an application on remote platform
- Check the identity of enclave (**hash of code/data pages**)
- Can establish a **"secure channel"** between enclaves

7

https://slideplayer.com/slide/8844767/

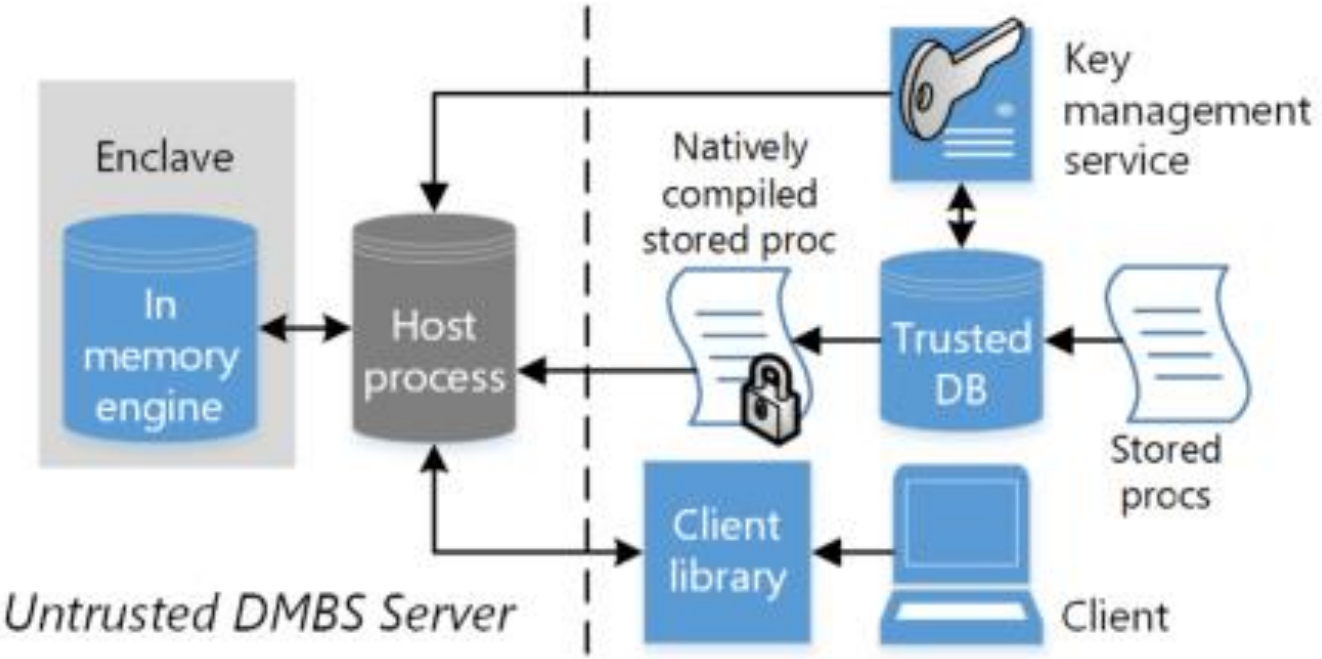
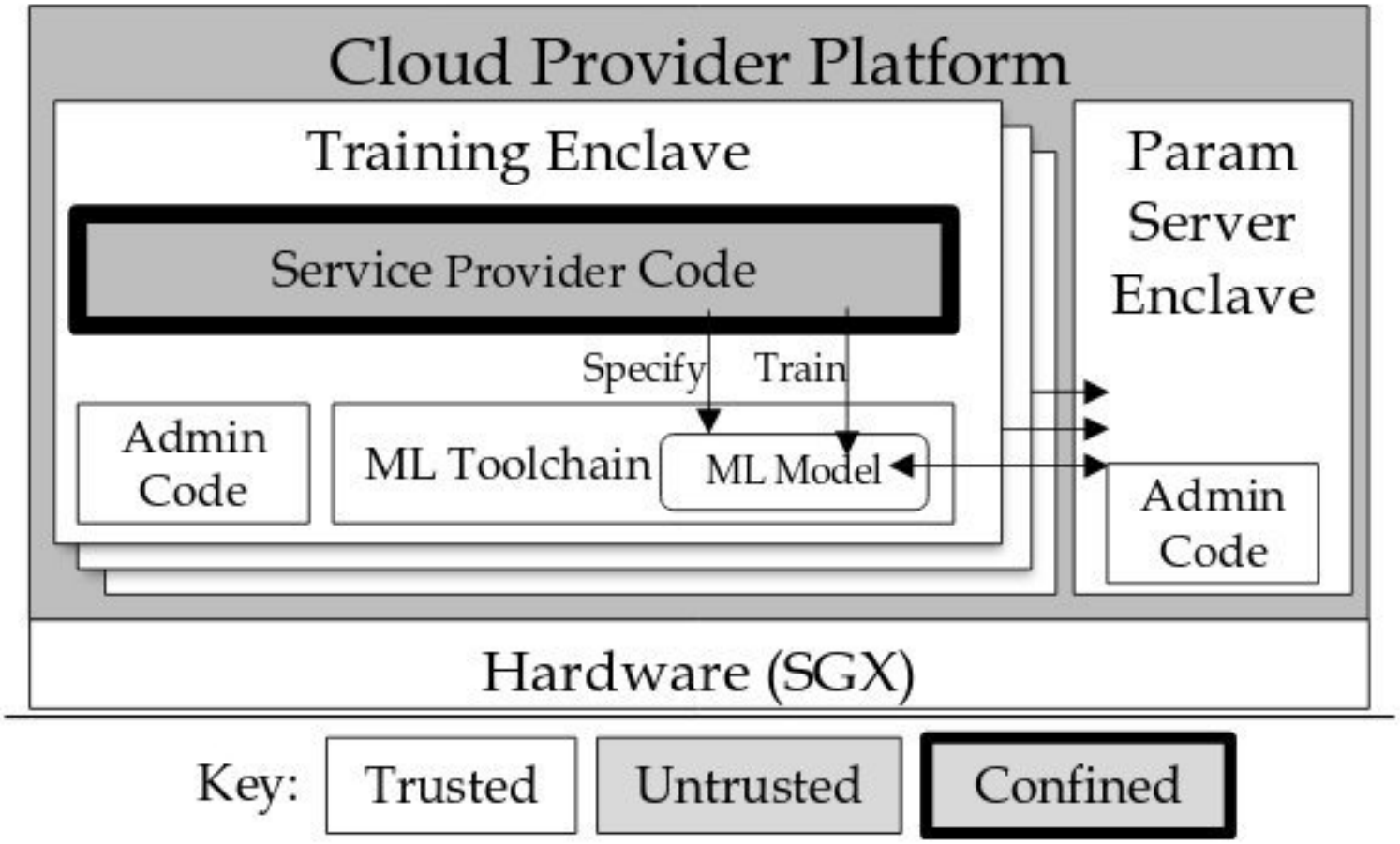


Fig. 1: Overview of EnclaveDB's architecture. EnclaveDB hosts sensitive data along with natively compiled queries and a query engine in an enclave.

https://www.microsoft.com/en-us/research/uploads/prod/2018/02/enclavedb.pdf



https://twitter.com/rzshokri/status/985792775189757952

- **Problems and Solutions**
  - Problems
  - Solutions
- **Trusted Execution Environment**
  - Architecture
  - Examples

- **Pre-knowledge**
  - C/C++ programming language
  - Basic knowledge of the operating system
  - Program analysis: static analysis and dynamic analysis
  - Knowledge of compiler is better (LLVM/GCC)
- **Sever access**
  - Ssh username@praksrv.sec.in.tum.de
  - Username and passwd, I will send them by email
  - www.in.sec.in.tum.de

- **Content and Tasks**
  - Attestation(local/remote)
  - Sealed Data storage/Secure_storage
  - Encryption/decryption
  - Random
  - SGX performance analysis tool
  - Enclave_database
  - Enclave_ssl
  - Enclave_ledger
  - Automatic program slicing

- **Grading**
  - Homework
  - Attendance
  - Discussion