Trusted execution environment and software security

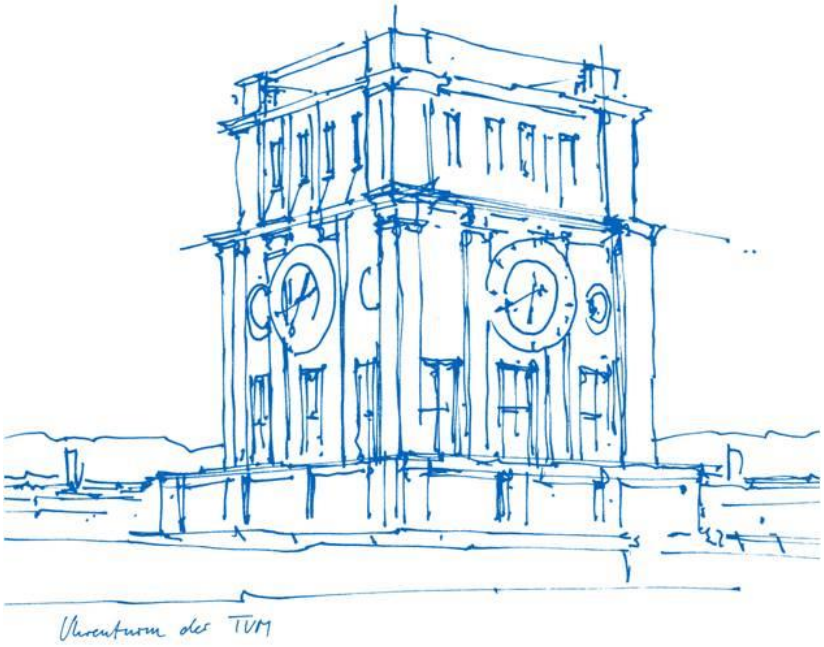
Peng Xu

peng@sec.in.tum.de

Lehrstuhl für IT-Security, Fakultät für Informatik,

Technische Universität München

28.01.2019



Agenda

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

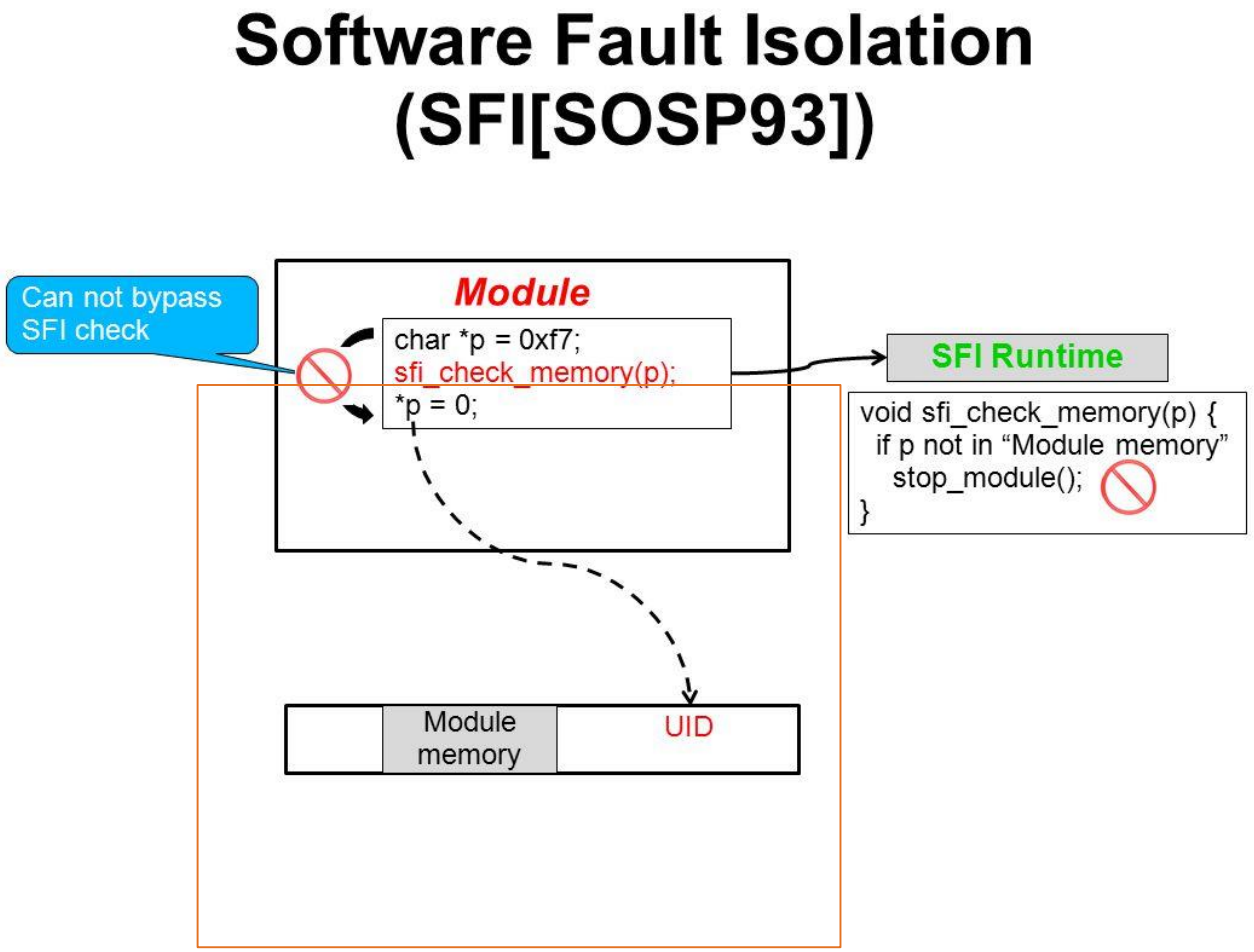
Problems?

Problems?

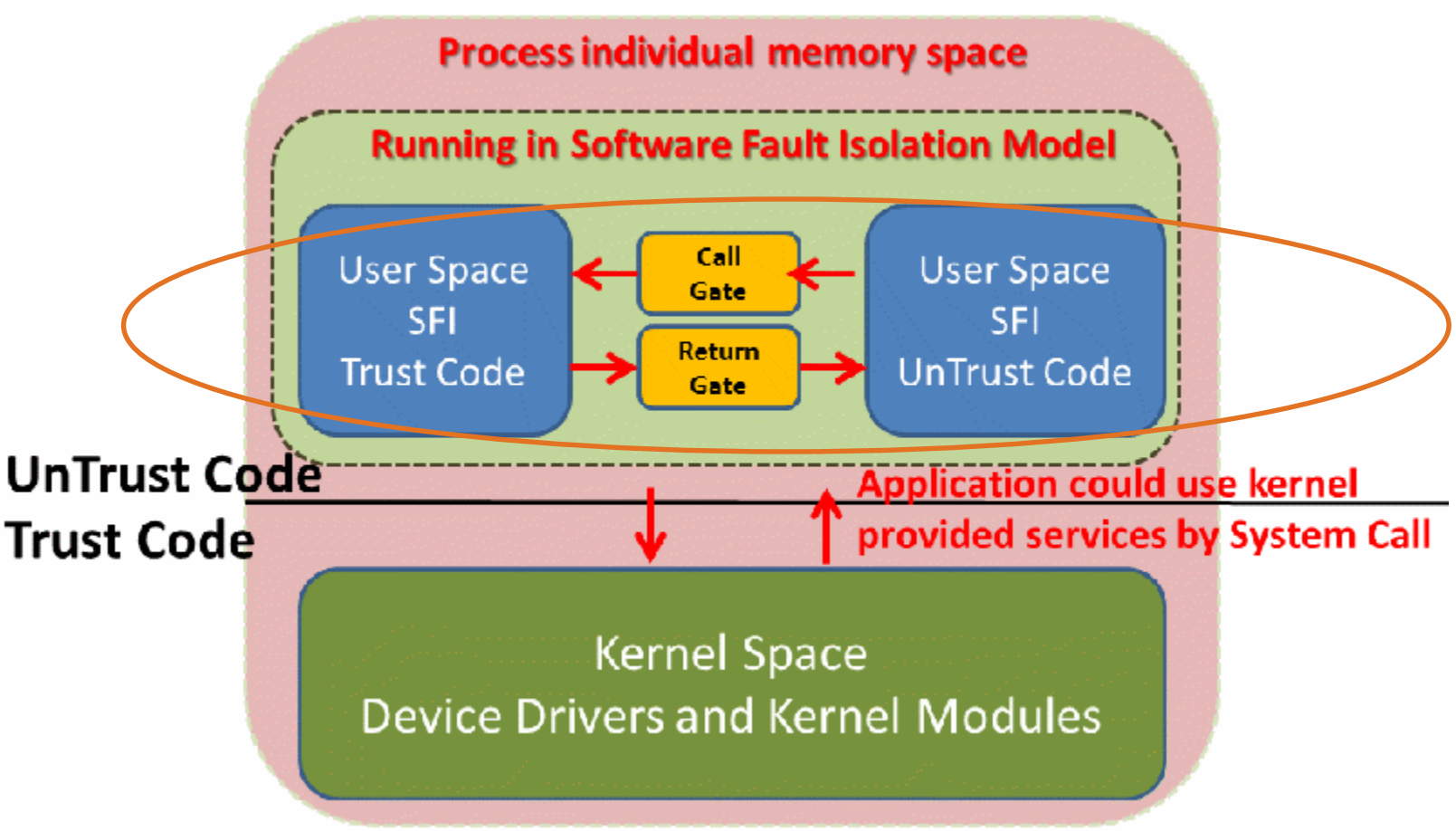
Problems?

Problems

Solutions – Software fault isolation

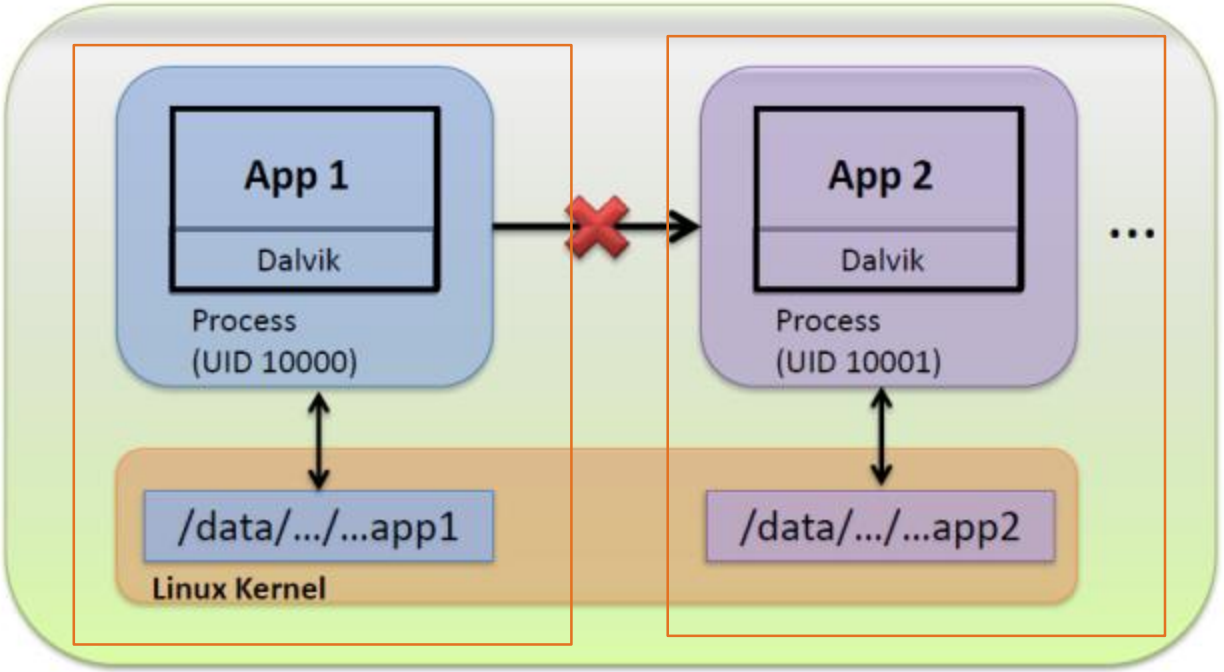


Solutions – Software fault isolation

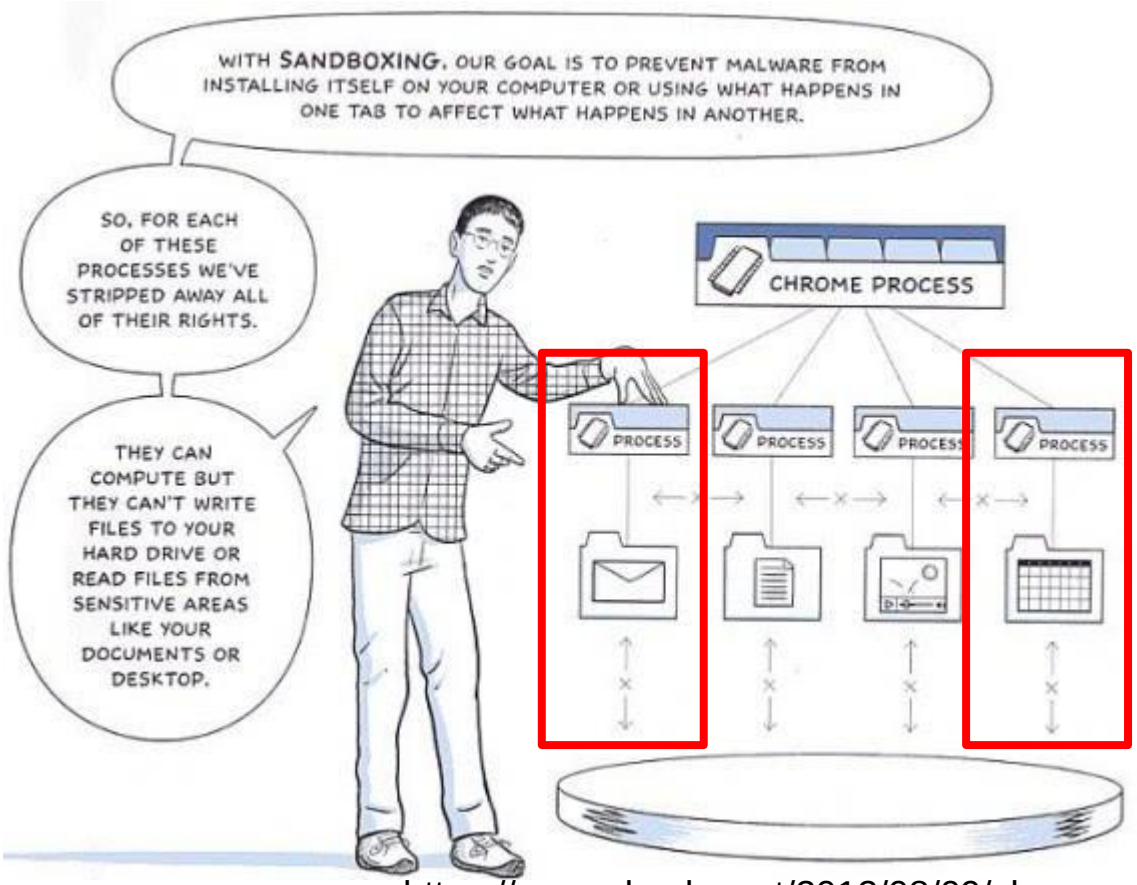


https://drive.google.com/file/d/0B5pbq4t2T2_fM2h1dnd3TFRud0E/view

Solutions – Sandbox

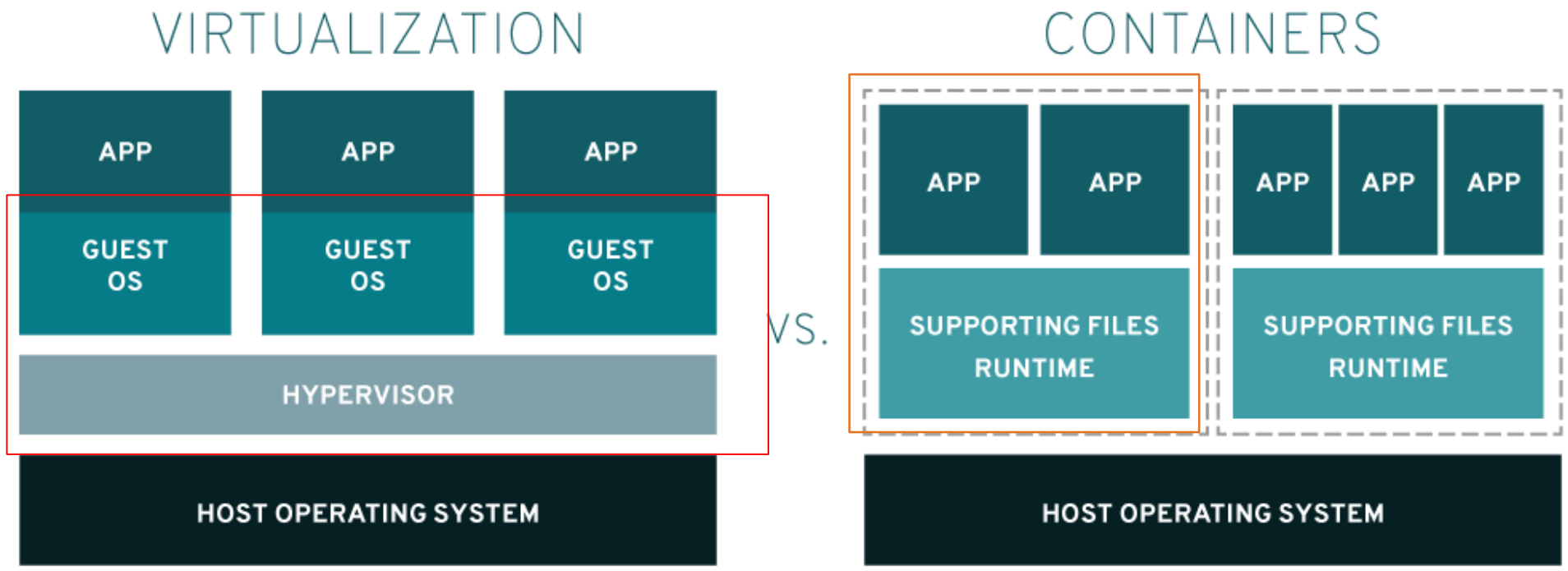


Solutions – Sandbox

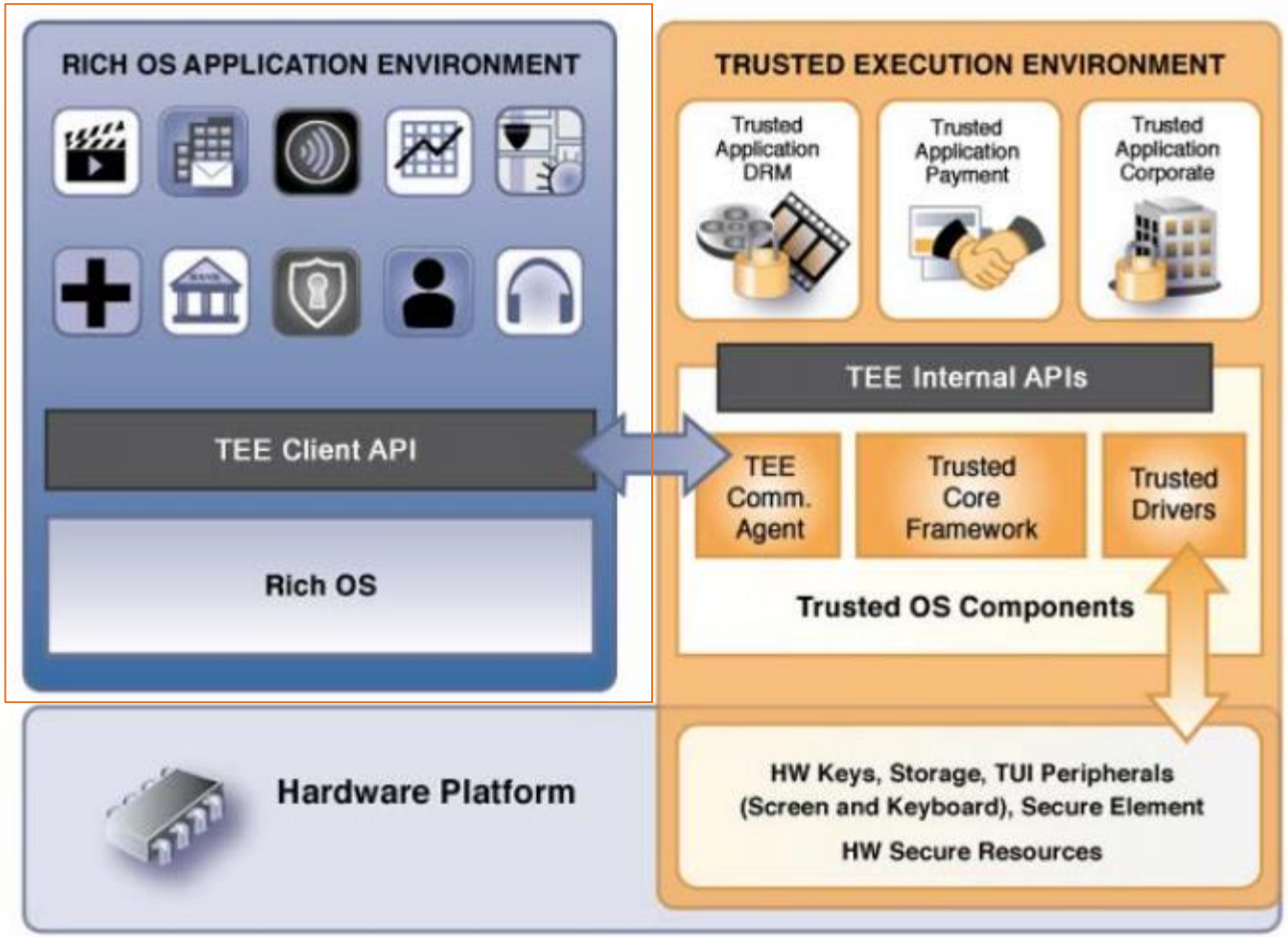


https://www.ghacks.net/2012/08/09/chromes-flash-sandbox-improves-with-better-security-less-crashes/

Solutions – Virtualization & Containers

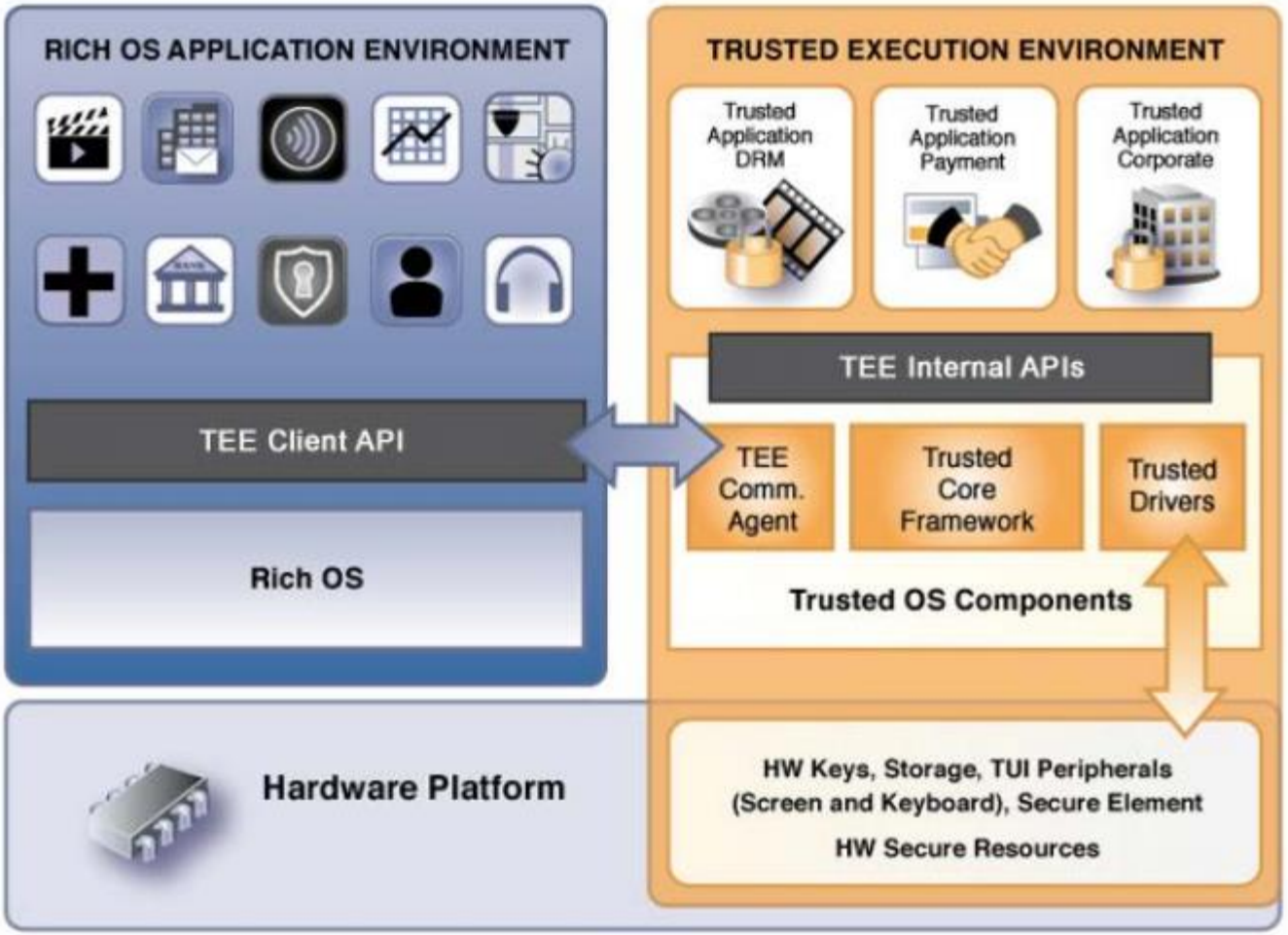


Solutions – Hardware isolation

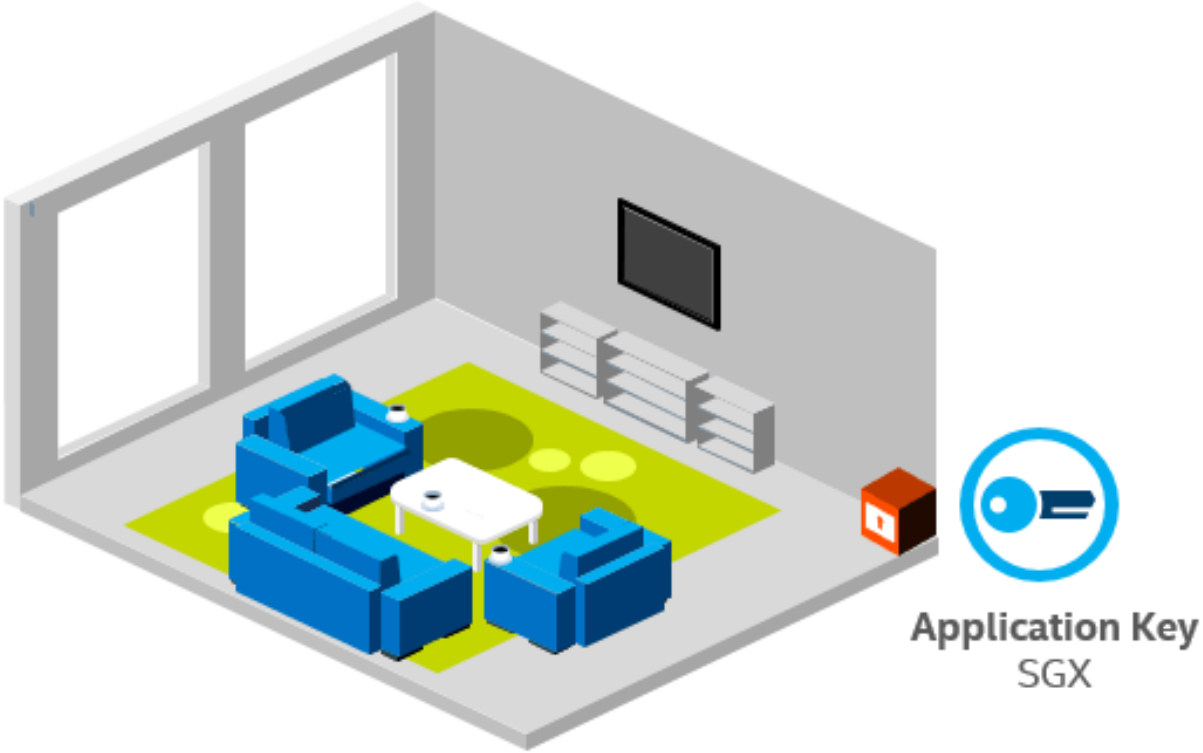


- **Problems and Solutions**
  - Problems
  - Solutions

TEE Architecture



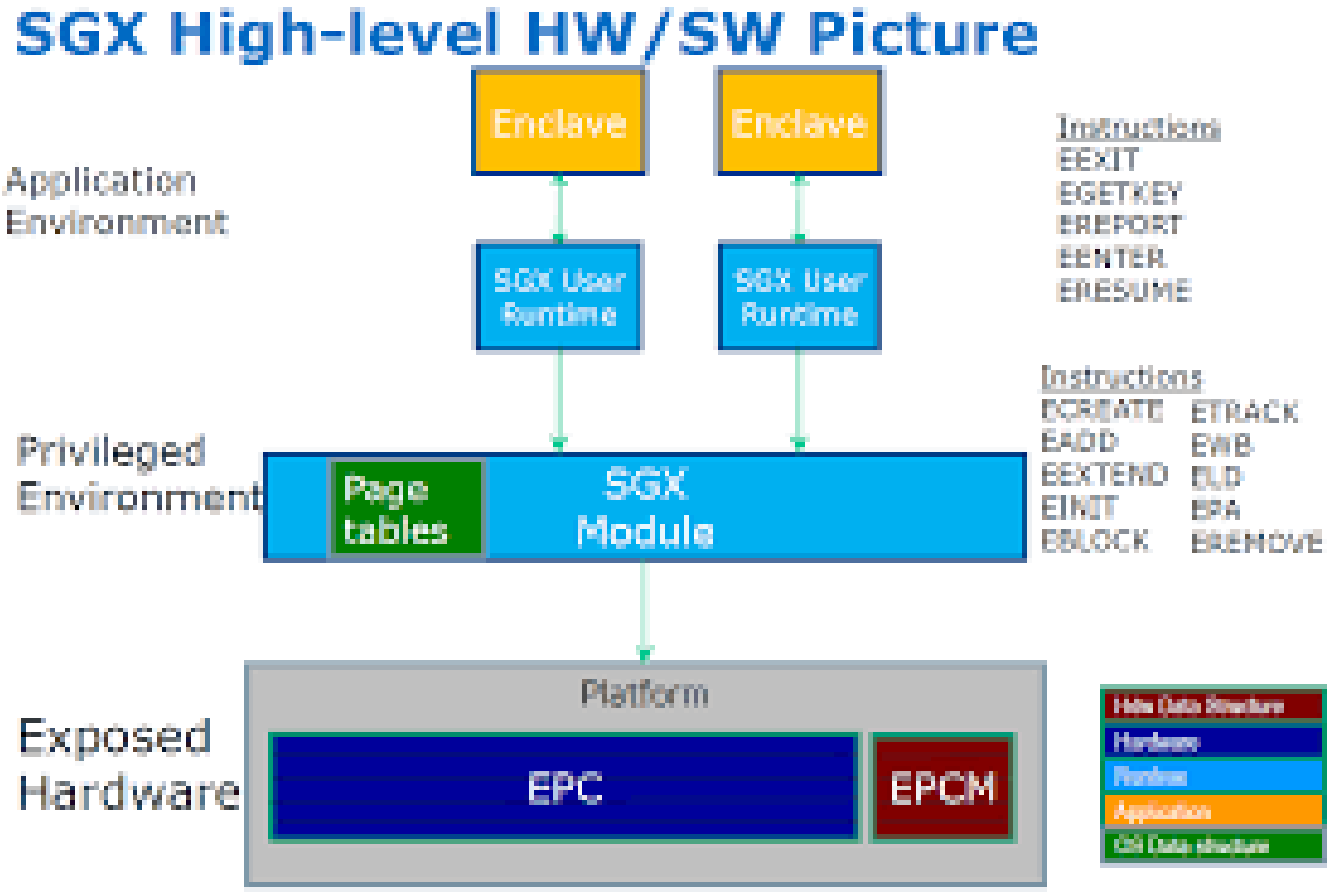
TEE Architecture – Intel SGX



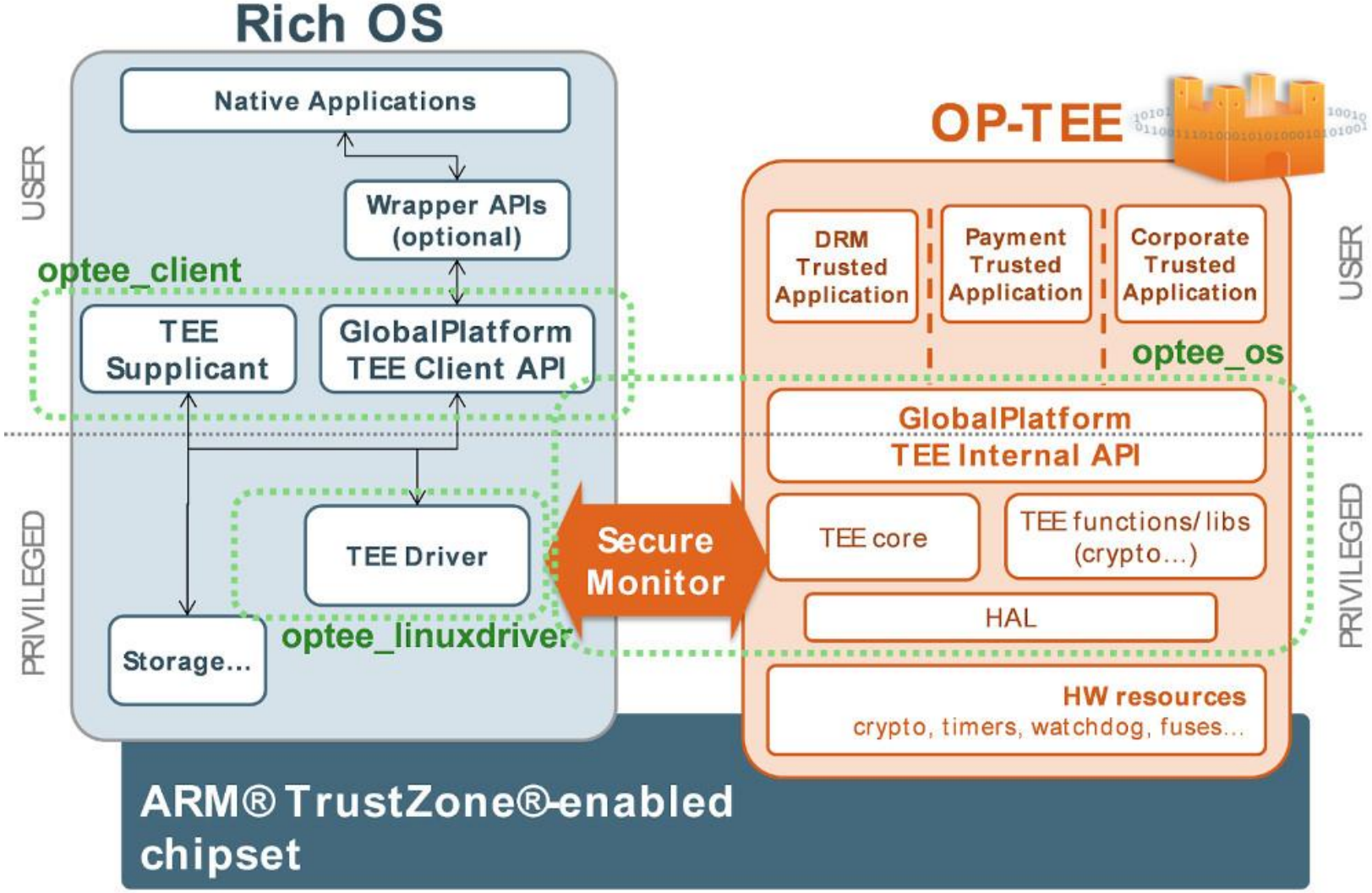
Intel® Software Guard Extensions (Intel® SGX)

Isolation for individual application data spaces

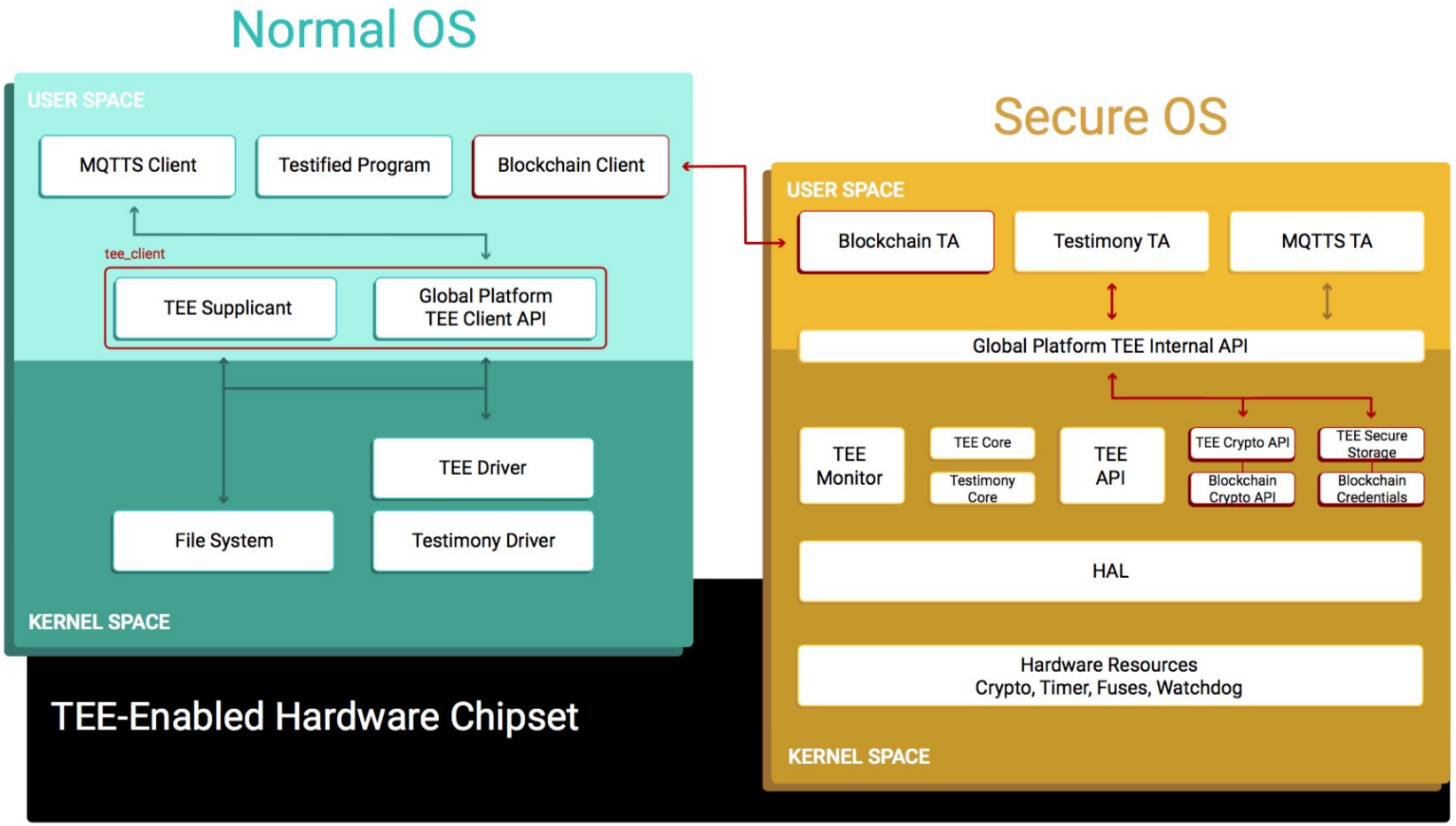
TEE Architecture – Intel SGX



TEE Architecture – ARM TrustZone

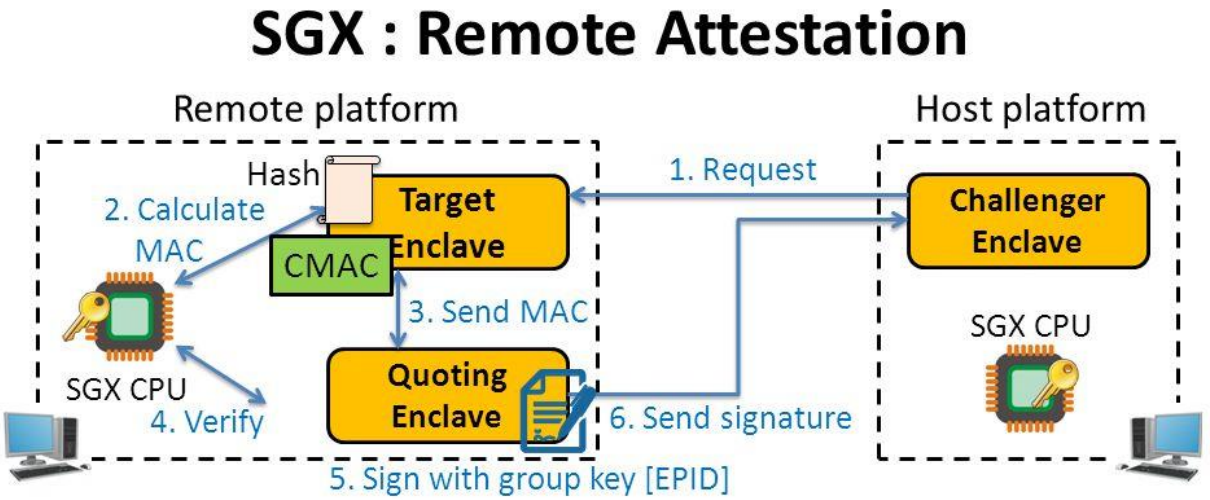


TEE examples – Bitcoin wallet



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

TEE examples – 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

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

TEE examples – EnclaveDB

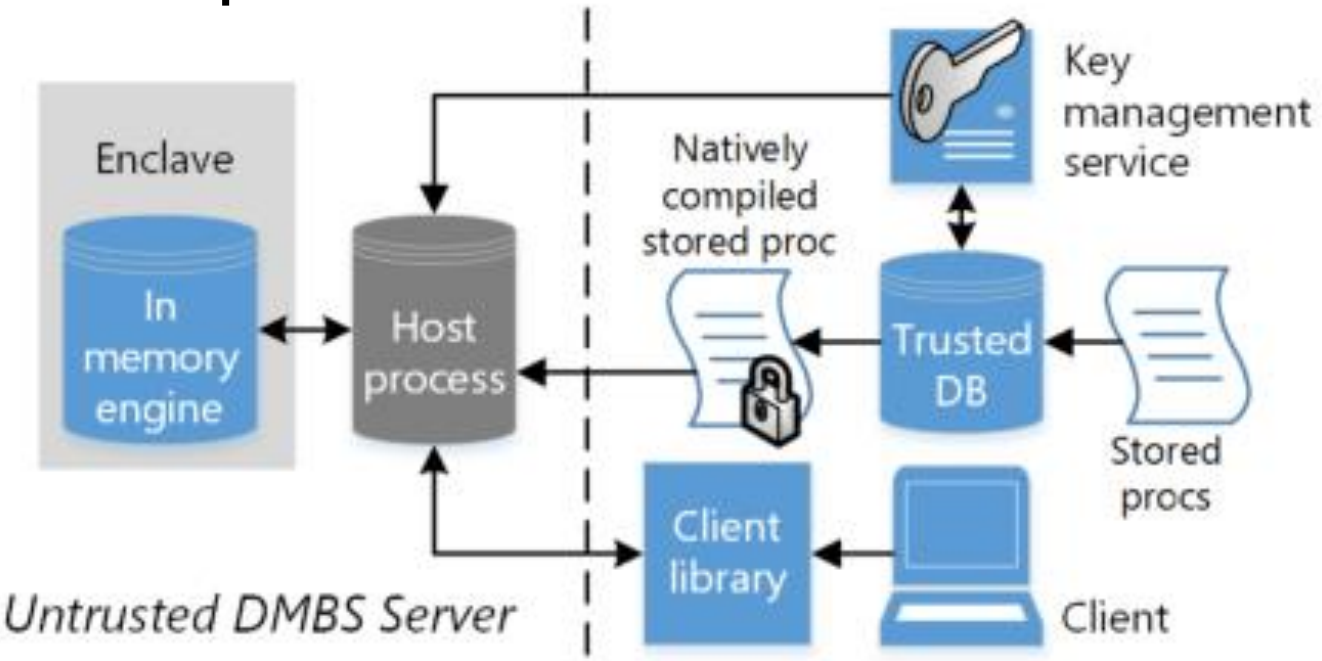
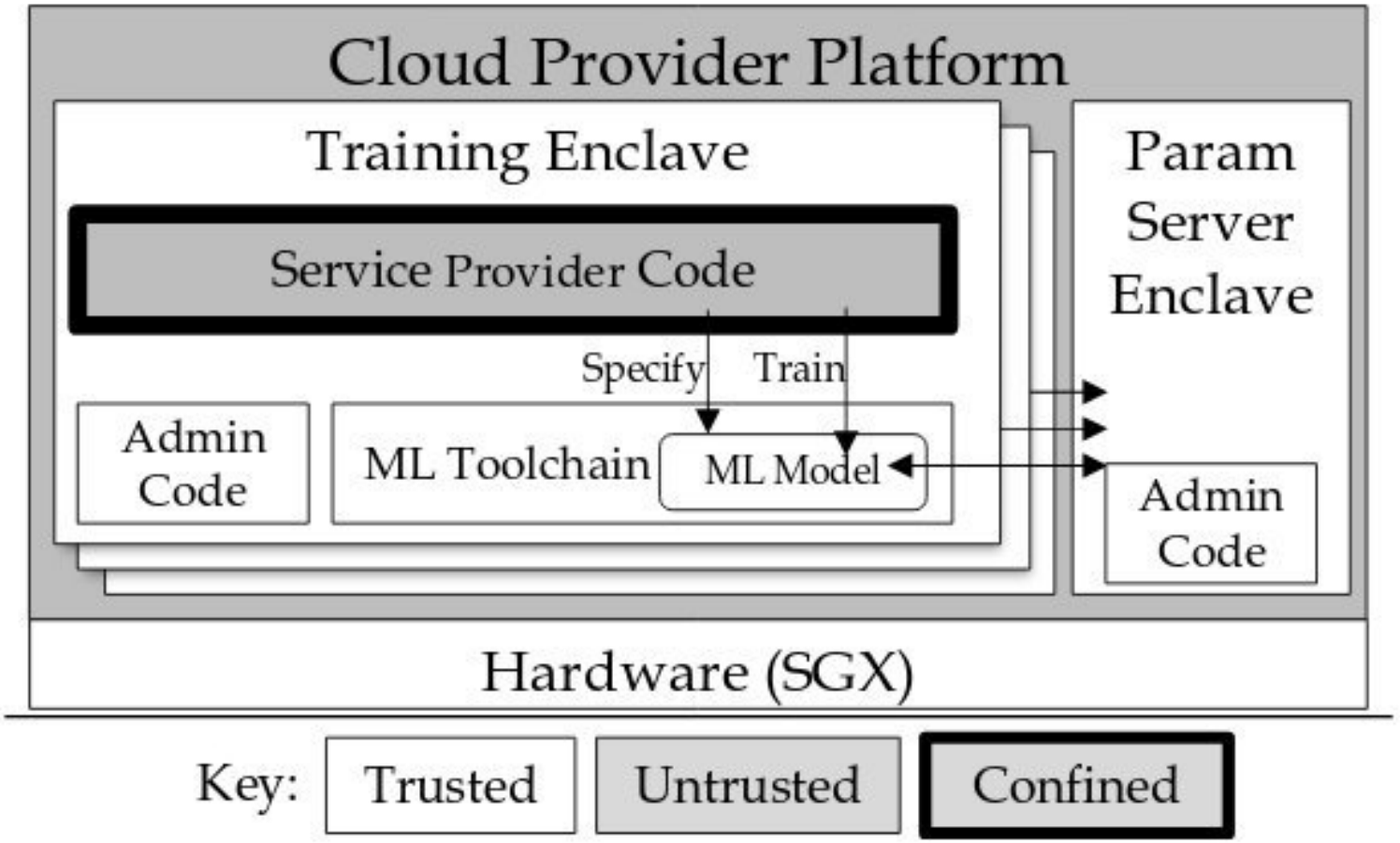


Fig. 1: Overview of EnclaveDB's architecture. EnclaveDB hosts sensitive data along with natively compiled queries and a query engine in an enclave.

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

TEE examples – Privacy preserving machine learning



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

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


COURSE

TEE and software security

Content:

1. Basic knowledge of TEE
2. Proof-of-concept programs
   - Remote/local attestation
   - Data sealing
   - Secure storage
   - Secure database
3. Program analysis and automatic program partitioning
   - Static data flow analysis (Compiler/ binary analysis)
   - Dynamic data flow analysis
   - Automatic code generation for TEE

Tasks:

1. Level-I: Easiest tasks
   - Demonstration for basic concepts
   - 40%
2. Level-II: Intermediate
   - Extended exercises for basic concepts
   - 40%
3. Level-III: Challenges
   - New ideas to extend related works
   - 10%
4. Attendance! Attendance!! Attendance!!!
   - 10%

Requirements:

1. C/C++ programming
2. Knowledge of Rust programming is better
3. Basic knowledge of operating system
4. Program analysis
5. Knowledge of compiler is better

Registration:

1. Matching system
2. Set up the development environment
   - OPTEE
   - SGX(Linux/Win10)
3. Helloworld Program with TEE

Agenda

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