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?
Solutions – Software fault isolation

Software Fault Isolation (SFI[SOSP93])

void sfi_check_memory(p) {
         if p not in “Module memory”
         stop_module();
     }

Can not bypass SFI check

Module
char *p = 0xf7;
sfi_check_memory(p);
*p = 0;

Module memory

SFI Runtime

UID
Solutions – Software fault isolation

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

App 1
Dalvik
Process (UID 10000)
/data/.../...app1
Linux Kernel

App 2
Dalvik
Process (UID 10001)
/data/.../...app2
Solutions – Sandbox

https://www.ghacks.net/2012/08/09/chromes-flash-sandbox-improves-with-better-security-less-crashes/
Solutions – Virtualization & Containers
Solutions – Hardware isolation

[Diagram showing TEE Client API, Rich OS, TRUSTED EXECUTION ENVIRONMENT with Trusted Application DRMs, Trusted Application Payment, and Trusted Application Corporate, TEE Internal APIs, Trusted OS Components, Hardware Platform, and Rich OS.]
• 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

**SGX High-level HW/SW Picture**

- Application Environment
- Privileged Environment
- Exposed Hardware

- SGX Module
  - Enclave
  - SGX User Runtime

- Platform
  - EPC
  - EPCM

- Instructions
  - EEXIT
  - EGEXIT
  - EREPORT
  - ENTER
  - ERESUME
  - HDR
  - ECREATE
  - ETRACK
  - EADD
  - EWB
  - EEEXTEND
  - ELD
  - EINST
  - EPAR
  - EBA
  - EBLOCK
  - EREMOVE

Peng Xu, I20, peng@sec.in.tum.de
TEE Architecture – ARM TrustZone

Rich OS

Native Applications

Wrapper APIs (optional)

GlobalPlatform TEE Client API

TEE Suppliant

Storage...

ARM® TrustZone®-enabled chipset

Secure Monitor

OP-TEE

optee_os

DRM Trusted Application

Payment Trusted Application

Corporate Trusted Application

GlobalPlatform TEE Internal API

TEE core

TEE functions/libs (crypto...)

HAL

HW resources

crypto, timers, watchdog, fuses...
Normal OS

USER SPACE
- MQTT Client
- Testified Program
- Blockchain Client
- TEE Supplicant
- Global Platform TEE Client API
- TEE Driver
- Testimony Driver

KERNEL SPACE

TEE-Enabled Hardware Chipset

Secure OS

USER SPACE
- Blockchain TA
- Testimony TA
- MQTT TA
- Global Platform TEE Internal API

KERNEL SPACE

TEE Monitor
- TEE Core
- Testimony Core
- TEE API
- TEE Crypto API
- Blockchain Crypto API
- TEE Secure Storage
- Blockchain Credentials

HAL

Hardware Resources
- Crypto, Timer, Fuses, Watchdog

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

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.

Cloud Provider Platform

Training Enclave

Service Provider Code

Admin Code

ML Toolchain

ML Model

Specify

Train

Param Server Enclave

Admin Code

Hardware (SGX)

Key: Trusted Untrusted Confined

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)

• **Server access**
  - Ssh `username@praksrv.sec.in.tum.de`
  - Username and passwd, I will send them by email
  - [www.in.sec.in.tum.de](http://www.in.sec.in.tum.de)
• Content and Tasks
  o Attestation(local/remote)
  o Sealed Data storage/Secure_storage
  o Encryption/decryption
  o Random
  o SGX performance analysis tool
  o Enclave_database
  o Enclave_ssl
  o Enclave_ledger
  o Automatic program slicing
• Grading
  o Homework
  o Attendance
  o Discussion