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

Software Fault Isolation (SFI[SOSP93])

```c
void sfi_check_memory(p) {
    if p not in “Module memory”
        stop_module();
}
```
Solutions – Software fault isolation

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

WITH SANDBOXING, OUR GOAL IS TO PREVENT MALWARE FROM INSTALLING ITSELF ON YOUR COMPUTER OR USING WHAT HAPPENS IN ONE TAB TO AFFECT WHAT HAPPENS IN ANOTHER.

SO, FOR EACH OF THESE PROCESSES WE’VE STRIPPED AWAY ALL OF THEIR RIGHTS.

THEY CAN COMPUTE BUT THEY CAN’T WRITE FILES TO YOUR HARD DRIVE OR READ FILES FROM SENSITIVE AREAS LIKE YOUR DOCUMENTS OR DESKTOP.

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

VIRTUALIZATION

CONTAINERS

APP
GUEST OS
HOST OPERATING SYSTEM

APP
GUEST OS
HOST OPERATING SYSTEM

APP
GUEST OS
HOST OPERATING SYSTEM

APP
SUPPORTING FILES
RUNTIME
HOST OPERATING SYSTEM

APP
SUPPORTING FILES
RUNTIME
HOST OPERATING SYSTEM

APP
APP
APP
HOST OPERATING SYSTEM
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

Rich OS

Native Applications

Wrapper APIs (optional)

TEE Supplicant

GlobalPlatform TEE Client API

TEE Driver

Storage...

OP-TEE

optee_client

optee_os

Secure Monitor

ARM® TrustZone®-enabled chipset

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...
TEE examples – Bitcoin wallet

**Normal OS**

**Secure OS**


Peng Xu, I20, peng@sec.in.tum.de
TEE examples – Remote attestation

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/
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.

TEE examples – Privacy preserving machine learning

https://twitter.com/rzshokri/status/985792775189757952
• Problems and Solutions
  • Problems
  • Solutions

• Trusted Execution Environment
  • Architecture
  • Examples
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