

Side-Channel Attacks on Confidential Virtual Machines

Advisor: **Fabian Rauscher**

Motivation

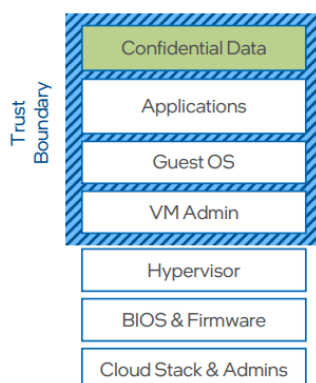
Confidential virtual machines (CVMs) are new trusted execution environments (TEEs) that allow for the execution of entire virtual machines inside a trusted environment that is protected from a potentially malicious host. CVMs are starting to be introduced on more and more CPU architectures by a variety of CPU vendors (AMD SEV-SNP, Intel TDX, ARM CCA, RISC-V CoVE).

In this thesis, you will perform side-channel attacks on CVMs. In the threat model of a malicious/compromised host an attacker has a significant amount of power which can be abused to perform previously unviable attacks.

Goals and Tasks

-  Get familiar with CVMs and side-channel attacks
-  Analyze potential attack primitives
-  Implement an attack on a CVM to leak secret information

VM Isolation *Intel® TDX*



Literature

- > [F. Rauscher et al.](#)
TDXploit: Novel Techniques for Single-Stepping and Cache Attacks on Intel TDX
[USENIX Security](#)
- > [E. Aktas et al.](#)
Intel trust domain extensions (TDX) security review

Courses & Deliverables

☒ Master Project

Project code
Report
Presentation

– OR –

☒ Master's Thesis

Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- > understanding of low level code and operating systems (SLP/OS)
- > low level programming skills (C/C++)
- > not being scared of assembly

Advisor Contact

fabian.rauscher@tugraz.at