# Seminar: Trusted Execution Environments

Benjamin Orthen, Alexander Weidinger, Hendrik Meyer zum Felde, January 31, 2022

# Outline

# Who are we?

- Short introduction of ourselves and Fraunhofer AISEC
- Research Interests

# Why register for this Seminar?

- You are interested in Operating Systems?
- IT Security has you on a hook?
- You know TEEs and the likes will only become more important in the future?
- You think microkernels do not yet have the attention they deserve?

=> Then this seminar is exactly what you are looking for!

Requirements: IN0004, IN0009
Recommended: IN2209 (IT-Sicherheit)

# Organization

- Report-Document
  - Language: English
  - Exactly 10 pages (excl. references)
  - Written in LaTeX IEEE template (`https://www.ieee.org/conferences/publishing/templates.html`)
- Review
  - Perform review of 2 papers of your fellow students
  - ~1 page per review
  - Based on the reviews received: Rebuttal + "Camera-Ready" version
- Presentation
  - Language: English or German
  - 25-30 minutes Presentation
  - ~15 minutes Discussion
- Deliverables
  - Draft and "camera-ready" Report
  - 2 Reviews
  - Rebuttal
  - Presentation + Slides
  - Active Participation in Discussions

# What are TEEs?

A Trusted Execution Environment (TEE) is an isolated environment which aims to protect executions within against high privileged adversaries.

- Software TEEs solely rely on software mechanisms for protection, while hardware TEEs use additional hardware mechanisms to protect the confidentiality and integrity of code and data within the environment.
- The most famous ones are
  - AMD SEV
  - Intel SGX
  - Arm TrustZone

# AMD Secure Encryptied Virtualization

- AMD Secure Memory Encryption (SME) allows to encrypt memory content before writing in to RAM
- Prevents an attacker from physical RAM reading attacks
- AMD Secure Encrypted Virtualization (SEV) is based on SME uses a different key for each virtual machine.
- This prevents a malicious hypervisor from reading a VM's memory content.
- Moving ciphertext between memory location is prevented by encryption of physical memory address

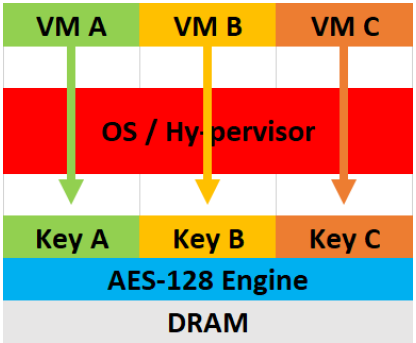


Figure: Overview of AMD SEV

# ARM TrustZone

- Hardware-enforced isolation (CPU extensions)
- TrustZone-A: for Armv7-A and Armv8-A devices
- TrustZone-M: for Armv8-M devices

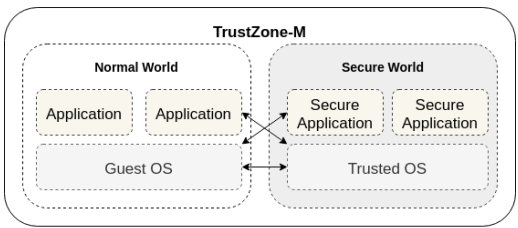


Figure: TrustZone-M Overview

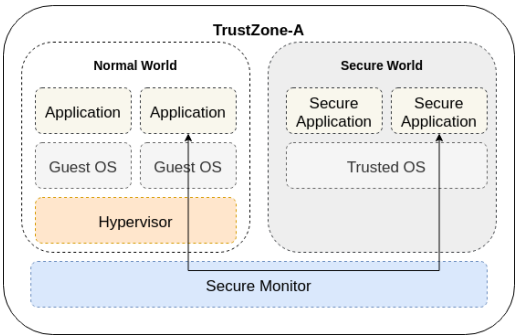


Figure: TrustZone-A Overview

# Static Attestation State-of-the-Art (TPM-based)

- Minimal Trusted Computing Base (TCB) full stack
- Hardware Trust-Anchor
- Signature scheme for software artefacts
- Authenticity verification for all components
- Typically Hashes used for measurements

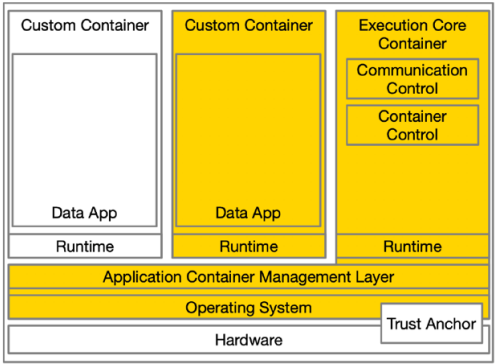


Figure: TCB attested via TPM

# Static Attestation State-of-the-Art (TEE-based)

- Strict isolation of program code and secrets by Trusted Execution Environment
- No manipulation even by the provider
- Remote integrity verification (remote attestation) before adding any secrets

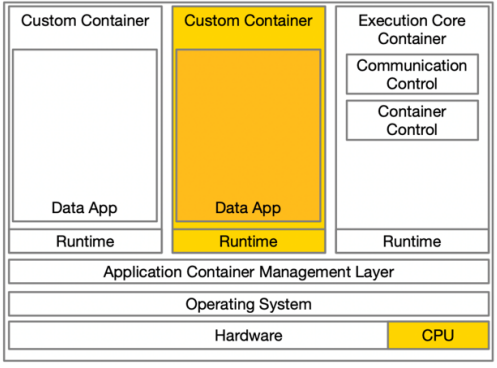


Figure: TCB attested via cloud TEEs

# Preliminary Time Table

| | |
|---|---|
| 31.01. | Preliminary Meeting (today) |
| 15.02. | Deadline for registration in matching system and E-Mail |
| 10.03. | Start of topic assignment |
| 08.05. | Submit outline + first content in bullet points |
| 19.06. | Submit your first version (outline finished, 80% of content) for review |
| 03.07. | Submit reviews |
| 17.07. | Submit your rebuttal + "camera-ready" version |
| 24.07. | Submit your presentation slides |
| 01.08. - 05.08. | Meetings: Presentations and discussion |

If possible, presentation meetings will be held at Fraunhofer AISEC. Attendance required!

# Introduction to Scientific Writing

- May be provided by chair? We will inform you beforehand
- We will provide helping material on...
  - How to read a paper
  - How to write a research paper
  - Citation guidelines
  - etc.

# Topics of Interest

TEE frameworks:

- AMD SEV, Intel SGX,TDX
- ARM TrustZone
- TEEs on RISC-V (e.g., Keystone)
- fTPM implementations in TEEs
- Attacks against TEEs / Mitigations against attacks

# Topics of Interest

TEE & Microkernels:

- TEE based on seL4
- Trusty TEE
- MicroTEE
- seL4 + Keystone
- . . . ?

# Topics of Interest

TEE & Attestation:

- Property-based Attestation in TEEs
- Remote Runtime Attestation in TEEs

And of course we always welcome topic proposals from your side.

# Next Steps

- Optional: Write us an E-Mail (<firstname>.<lastname>@aisec.fraunhofer.de) and propose a topic:
  - benjamin.orthen@aisec.fraunhofer.de
  - alexander.weidinger@aisec.fraunhofer.de
  - hendrik.meyerzumfelde@aisec.fraunhofer.de
- Mandatory: Register for this seminar via the TUM-Matching system (10.02. - 21.2.)

# Q&A