Kick-off: Trusted Execution Environments

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

Michael Lux
michael.lux@aisec.fraunhofer.de

Hendrik Meyer zum Felde
hendrik.meyerzumfelde@aisec.fraunhofer.de

Mathias Morbitzer
mathias.morbitzer@aisec.fraunhofer.de

July 16, 2019

Outline

Organization

The seminar will be organized as a scientific conference:

1. Familiarization phase (2 Weeks)
2. Writing phase (7 Weeks)
3. Review phase (2 Weeks)
4. Improvement phase (8 Weeks)
5. Talk preparation (1 Week)
6. Talk and Discussion

Requirements

- Report
  - Written report in the form of a scientific paper
  - Mandatory length of 8 pages (references don't count)
  - Usage of LaTeX is mandatory
  - Formatting with the provided LaTeX-Style (IEEE 2-column)
- Review
  - Every Student creates two anonymous reviews
  - Review template will be provided
  - Approximately 1/2 page
  - Every Student writes a rebuttal
- Presentation
  - Presentation with slides
  - 30 minutes presentation
  - 15 minutes discussion

Grading

Fraunhofer AISEC

Grading considers all contributions to this seminar:

1. Report (50%)
   - Contents, Accuracy, Style, Effort, Grasp
2. Presentation (30%)
   - Slides, Execution, Contents, Understandability
3. Reviews (15%)
   - Written Reviews and Rebuttal
4. Participation and discussion (5%)

Time Table

16.07.19	Kick-off meeting (today)
01.-20.08.19	Topic Assignment
02.09.19	Introduction to scientific writing
25.10.19	Deadline for report (pre-final) submission
29.10.19	Status meeting (attendance mandatory)
01.11.19	Review Assignments
15.11.19	Deadline for review submission
10.01.20	Deadline for final report submission
15.01.20	Deadline for presentation submission
16+17.01.20	Presentations and discussion

Before we go on....

... any questions so far?

Topics

Fraunhofer AISEC

- Survey of Hardware TEEs (AMD SEV, ARM TrustZone, Intel SGX)
- Survey of Software Based Attestation Techniques

- Exploiting AMD SEV's missing integrity protection
- Attacking AMD SEV's memory encryption

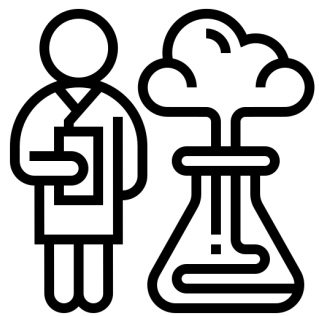
- Analysis: Intel SGX Enclaves and RAM limitation
- Analysis: Intel SGX Enclaves and TPM interaction
- Intel SGX: Attacking Enclaves

- SDKs for Trusted Execution Environments
- Emulating TPMs Using Secure Enclave Technologies
- Exploiting Speculative Execution

Survey of Hardware TEEs

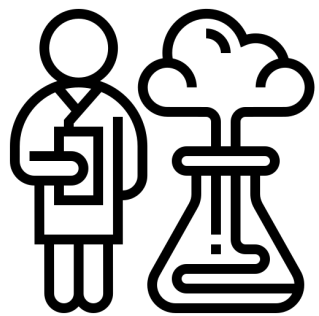
Fraunhofer AISEC

- Trusted Execution Environment (TEE) is an isolated environment which
  - aims to protect executions against high privileged adversaries
  - may use additional hardware mechanisms to protect the confidentiality and integrity of code and data (hardware TEE)
- Most famous ones are ARM TrustZone, AMD SEV and Intel SGX
- Fundamental differences in architecture and capabilities:
  - TrustZone splits OS system in a trusted and an untrusted part
  - AMD SEV protects a VM from a malicious hypervisor
  - Intel SGX protects part of a program from a malicious OS
- Goal: Get to know the TEEs mentioned (+ more)
- Goal: Analyze their differences regarding:
  - Attacker model
  - TEE privileges
  - Vulnerabilities
  - Use cases



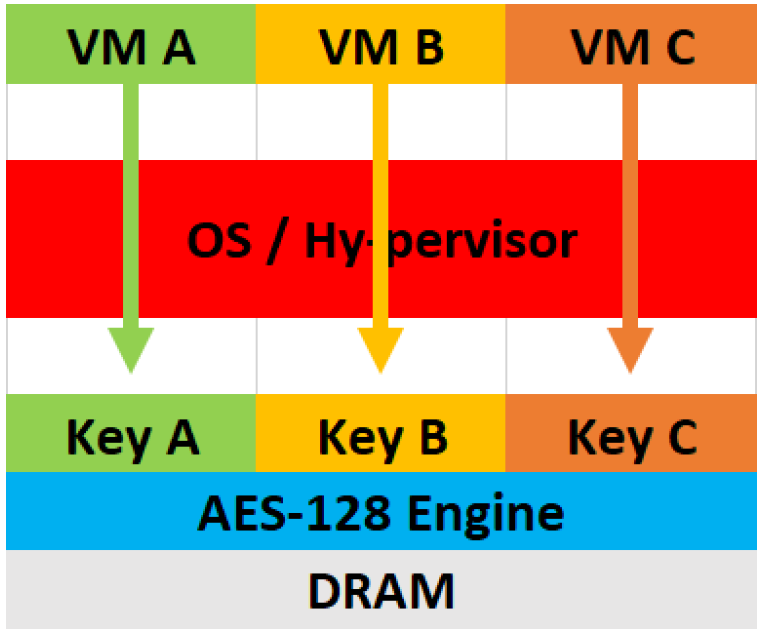
Survey of Software Based Attestation Techniques

- Remote attestation usually requires a hardware anchor
- Common case Trusted Platform Module (TPM)
- TPM not always provided due to HW limitations
- Multiple attestation techniques were developed solely via software mechanisms
- Goals:
  - Research existing software based attestation techniques
  - Analyze their differences regarding:
    - Attacker model
    - Requirements
    - Limitations
    - Use cases



Exploiting AMD SEV's missing integrity protection

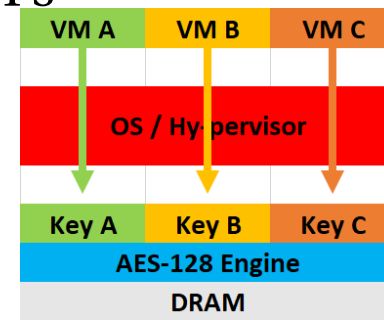
- AMD Secure Memory Encryption (SME) allows to encrypt memory content before writing in to RAM
- Prevents an attacker from physical RAM reading attacks
- AMD Secure Encrypted Virtualization (SEV) is based on SME uses a different key for each virtual machine.
- This prevents a malicious hypervisor from reading a VM's memory content.
- Attacks were published which circumvent SEV (often due tp lack of integrity protection.)
- Goal: Understand the attacks, design a protection mechanism for AMD SEV



Attacking AMD SEV's memory encryption

Fraunhofer AISEC

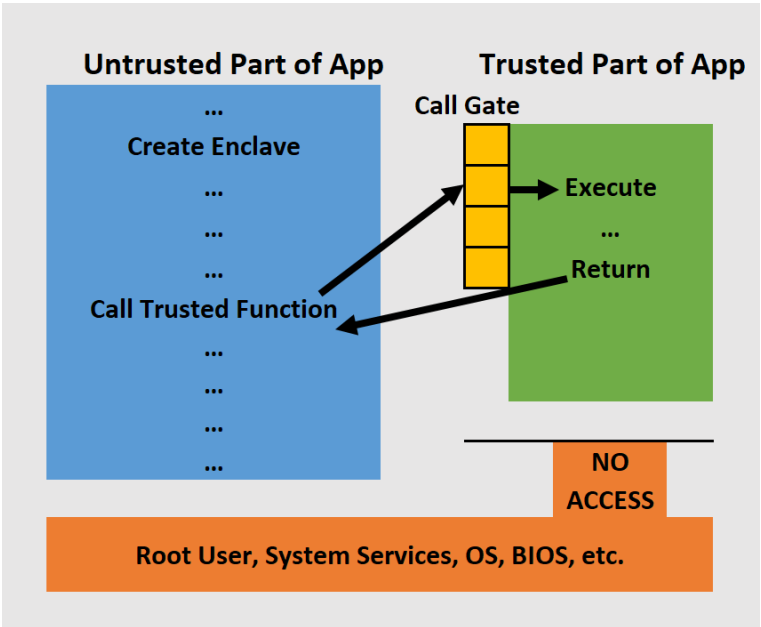
- AMD Secure Memory Encryption (SME) allows to encrypt memory content before writing in to RAM
- Prevents an attacker from physical RAM reading attacks
- AMD Secure Encrypted Virtualization (SEV) is based on SME uses a different key for each virtual machine.
- This prevents a malicious hypervisor from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



- Moving ciphertext between memory location is prevented by encryption of physical memory address
- Problem caused: swapping or VM migration not possible
  - Topic: Understand AMD SEV's encryption mechanisms, propose changes that allow the hypervisor to move cipherblocks if required

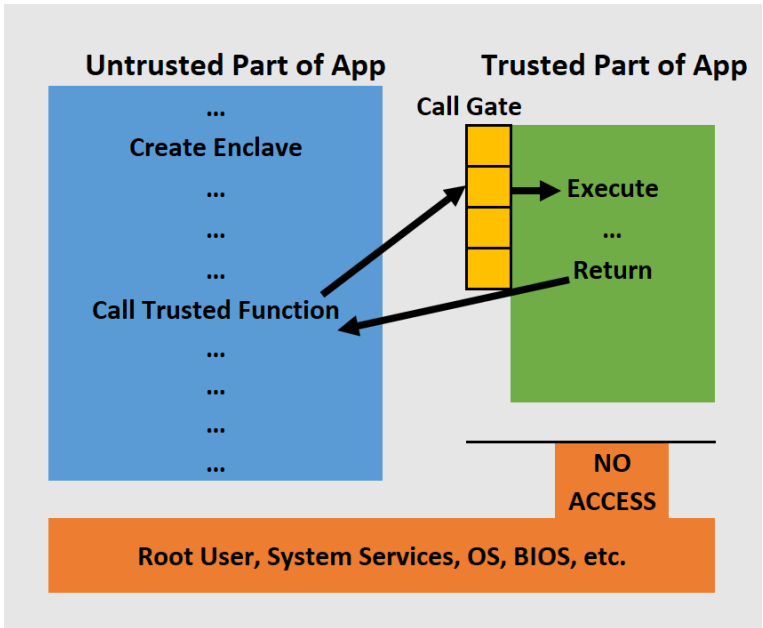
Analysis: Intel SGX Enclaves and RAM limitation

- Shipped within every Intel Skylake CPU of the 6th generation
- Allows code parts to be executed in hardware separated enclave
- Limit 128MB RAM simultaneous usage of SGX enclaves
- Possible to attest that code is running inside an SGX enclave
  - TLS session can be terminated directly in enclave
  - Typical monitoring capabilities
  - Intense bug fixing history
  - Enclave guarantee's correct code execution despite malicious OS
- Goal: find limitations and possibilities with respect to RAM limitation.



Analysis: Intel SGX Enclaves and TPM interaction

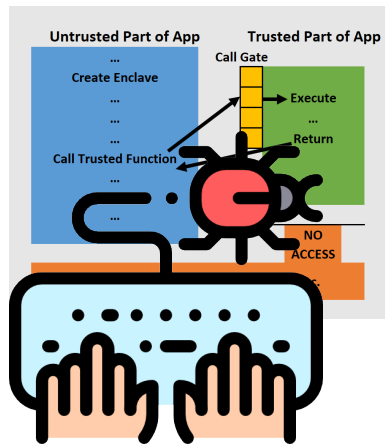
- Shipped within every Intel Skylake CPU of the 6th generation
- Allows code parts to be executed in hardware separated enclave
- Limit 128MB RAM simultaneous usage of SGX enclaves
- Possible to attest that code is running inside an SGX enclave
  - TLS session can be terminated directly in enclave
  - Typical monitoring capabilities
  - Intense bug fixing history
  - Enclave guarantee's correct code execution despite malicious OS
- Goal: find limitations and possibilities with respect to TPM interaction.



Intel SGX: Attacking Enclaves

Fraunhofer AISEC

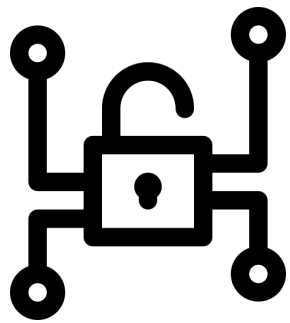
- Shipped within every Intel Skylake CPU of the 6th generation
- Allows code parts to be executed in hardware separated enclave
- Limit 128MB RAM simultaneous usage of SGX enclaves
- Possible to attest that code is running inside an SGX enclave
  - TLS session can be terminated directly in enclave
  - Typical monitoring capabilities
  - Intense bug fixing history
  - Enclave guarantee's correct code execution despite malicious OS
- Goal: research other attacks on SGX (there are plenty, quite a bug fixing history)
- Consider possible defense mechanisms



SDK for Trusted Execution Environments

Fraunhofer AISEC

- Frameworks dealing with TEEs have been developed.
- Multiple frameworks exist claiming to work with different types of TEEs.
- Goals:
  - Understand AMD SEV, Intel SGX, Google Asylo (+ more TEE frameworks)
  - Design a uniform interface for SEV and SGX



Emulating TPMs Using Secure Enclave Technologies

Fraunhofer AISEC

- Secure enclaves are a subcategory of Trusted Execution Environments.
- TPMs and Secure Enclave Technologies have some but not all capabilities in common.
- Can Secure Enclave Technologies completely emulate the behaviour of a TPM?
- A TPM can store hashes of system configuration during boot-up phase and runtime
- Secure enclaves can perform actions during runtime

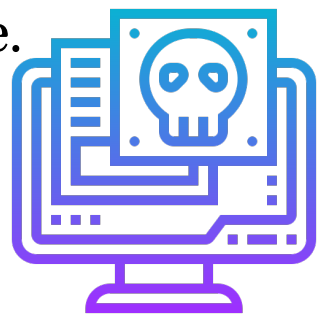
- Research approaches for a TPM emulation in Trusted Execution Environments
- using a TPM emulated by a Secure Enclave during booting phase of a system.

Exploiting Speculative Execution

Fraunhofer AISEC

- Meltdown and Spectre are two classes of vulnerabilities which are based on speculative execution in mostly Intel CPUs.
- Vulnerabilities capable of reading protected memory, potentially used by a Trusted Execution Environment.
- Critical problem in cloud infrastructure due to often shared memory among processes.
- Reducing the CPU feature "speculative execution" will cause major performance losses (about 40%).

- Goal: Research Speculative Execution Attacks on TEEs.
- Goal: Find and analyse or propose a solution to issue.



Topic assignment

Fraunhofer AISEC

After matching phase:

- We'll ask you to send your 3 top choices via email
- You may add a letter of motivation to emphasize your top choice
- We'll assign topics to students with your input
- You'll receive information and initial literature from your supervisor

Fraunhofer AISEC

Introduction to Scientific Writing

- 02.09. 10:00 - 12:00
- Crash course in scientific writing
- Not mandatory
- You may need scientific writing for
  - this seminar, obviously
  - BA or MA thesis
  - any scientific paper writing

Next Steps

- Matching and Topic assignment
  - Matching concludes 30.07.2019. After that we'll get in touch with the participants
  - If you want to deregister
    - do so until 06.08.2019 without penalty
    - or brace yourself for a 5,0
  - Participants send top 3 topics via email, we'll assign the topics
- Familiarization phase
  - Literature research
  - Get an overview of your topic
  - Create report structure
- Introduction to Scientific Writing (02.09.2019)
- Writing phase

Q&A ?