

# SEV Guest Support in SWEB

Advisor: **Hannes Weissteiner**





## Motivation

Secure Encrypted Virtualization (SEV) is AMD's implementation of confidential virtual machines (CVMs)[2]. The trusted computing model protects CVMs from malicious hypervisors. The hypervisor cannot read guest data due to transparent encryption by the MMU. On previous iterations, the hypervisor could still modify the encrypted memory, which lead to compromised security of the guest.

With the extensions Encrypted State (ES) and Secure Nested Paging (SNP)[1], the AMD tries to ensure that the hypervisor cannot read register states or modify guest memory. This means that the hypervisor can no longer inspect the guest registers to handle virtualization intercepts anymore. Therefore, the guest needs to support a new exception type called VMM Communication Exception (#VC). In this exception, the guest decides which further actions to take, e.g., copying important information for the hypervisor to a shared page, or validating memory contents.

At the moment, SWEB does not support running as a SEV-SNP guest. However, having SNP support would allow us to perform more efficient, noise-free experiments on SEV-SNP, and may be used as a base for further research. Your task is the implementation of SEV-SNP guest support.

## Goals and Tasks

-  Get familiar with the topic
-  Get SWEB to run in SEV-ES mode
-  Develop further features required by SEV-SNP
-  Analyze results and performance

## Literature

- > [AMD](#)  
Strengthening VM isolation with integrity protection and more  
2020
- > [AMD](#)  
System Programming  
[AMD64 Architecture Programmer's Manual 2023](#)

## Courses & Deliverables

- Master Project**
  - Project code
  - Report
  - Presentation

## Recommended if you're studying

- CS
- ICE
- SEM

## Prerequisites

- > Interest in the topic area
- > Programming (C)
- > Completed Operating Systems course
- > Bonus: Completed CloudOS course

## Advisor Contact

[hannes.weissteiner@iaik.tugraz.at](mailto:hannes.weissteiner@iaik.tugraz.at)