Emulation of Confidential Computing Hardware: AMD SEV-SNP / Intel TDX (AISEC)

Servers Confidential Computing technologies are a promising tool for cloud computing. They aim to protect data while being processed in the cloud by preventing the cloud provider and platform owner from gaining access to it. AMD SEV-SNP and Intel TDX in particular do this by providing confidential virtual machines. Memory of these VMs remains confidential and integrity-protected at all times and the technologies provide remote attestation mechanisms for verification. Extensive work has analyzed, broken and improved upon these technologies. Especially for proof of concept implementations, however, creating, testing and verifying code requires specific server hardware that is not readily available to everyone.

This thesis aims to design and implement emulators for either AMD SEV-SNP or Intel TDX.

Task Description
In this thesis, the focus lies on providing AMD SEV-SNP or Intel TDX remote attestation mechanisms to a VM hosted on conventional hardware. For this, the student researches and evaluates required components needed to emulate these. The student then creates a design and proof of concept implementation that provides the corresponding remote attestation mechanism to the guest VM, e.g., by modifying and extending the virtual machine manager (VMM) QEMU. If possible, guest VM and host kernel shall remain unchanged.

Prerequisites
* High motivation and ability to work independently
* Good understanding of virtualization concepts
* Experience with QEMU / KVM and Linux kernels

Contact
Joana Pecholt
E-Mail: joana.pecholt@aisec.fraunhofer.de

Simon Ott
E-Mail: simon.ott@aisec.fraunhofer.de

Advisors
Georg Sigl
Joana Pecholt + Simon Ott (Fraunhofer AISEC)