Contribution ID: **387** Type: **not specified**

Intel TD Partitioning and vTPM on COCONUT-SVSM

Friday, 20 September 2024 10:20 (20 minutes)

Intel's Trust Domain Extensions (TDX) coupled with Coconut-SVSM is emerging as a powerful combination for secure and efficient virtualization. This talk delves into the intricacies of Intel TD Partitioning, its role in running an SVSM, and its integration with a virtual Trusted Platform Module (vTPM).

We will provide a comprehensive overview of TD Partitioning, explaining its architecture, functionality, and how it differentiates from traditional nested virtualization. The presentation will also cover the integration of TD Partitioning into the Coconut-SVSM stack, highlighting the challenges and solutions encountered during development.

A key focus of the talk will be on the vTPM solution built on top of Intel TD Partitioning and Coconut-SVSM. We will explore how this vTPM is implemented, including the generation of vTPM identity and the mechanism for user TD attestation. The potential benefits and use cases of this integrated solution will also be discussed.

Primary authors: DONG, Chuanxiao; CHEN, Jason; Mr YAO, Jiewen (Intel Corporation); FANG, Peter; DHANRAJ, Vijay

Presenters: DONG, Chuanxiao; CHEN, Jason; Mr YAO, Jiewen (Intel Corporation); FANG, Peter; DHANRAJ, Vijay

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC