Contribution ID: **64** Type: **not specified**

Confidential Computing for RISC-V-based Platforms

Tuesday, 13 September 2022 17:00 (30 minutes)

Confidential computing aims to protect data in use on computing platforms. Via confidential computing mechanisms, we aim to remove host software (OS/VMM, service VMs and firmware), other tenants (VMs), host software developers, operators and administrators of multi-tenant systems from the Trusted Computing Base (TCB) of tenant workloads. For RISC-V-based platforms, we propose an Application Platform-Trusted Execution Environment (AP-TEE) reference architecture and the ABI between host software and the TCB components on the platform (a TEE Security Manager aka TSM). The interfaces describes the use of the RISC-V Hypervisor extension to enforce confidentiality for virtualized workloads as well as the hardware changes that should be considered to enforce mitigations for a threat model. The proposal discusses the ABI proposed for TSM-Host/VMM interactions (TH-ABI) and TSM-Guest interactions (TG-ABI), and directions of hardware/ISA extensions. In addition to the proposed normative specifications, the proposal will document implementation-specific guidelines and relevant standard protocols for attestation to assist implementers of the AP-TEE confidential computing capability on RISC-V platforms.

I agree to abide by the anti-harassment policy

Yes

Primary author: SAHITA, RAVI (Rivos)

Presenter: SAHITA, RAVI (Rivos)

Session Classification: RISC-V MC

Track Classification: LPC Microconference: Real-time and Scheduling MC