Contribution ID: **318** Type: **not specified**

Updates on RISC-V Confidential VM Extension (CoVE) and CoVE-IO

Friday, 20 September 2024 13:00 (10 minutes)

This session will discuss the ongoing development of the RISC-V architecture for Confidential VM Extension (CoVE) and related CoVE-IO (for TEE-IO). The discussion will cover both the WIP ISA (CPU) and non-ISA (ABI, IOMMU and other platform aspects) extensions. The WIP ISA extensions will cover the proposed Smmtt (memory isolation) and related extensions for interrupts isolation, IO-MTT and external debug. The proposed CoVE ABI nears STABLE status and is entering the public review phase. The common aspects (that are cross-architectural) for Linux/KVM will be discussed to enable interoperability across different platforms for Confidential VMs. The discussion is to cover common flows that influence the public review of the specs by Q3'24.

Primary author: SAHITA, RAVI (Rivos)

Co-authors: PATRA, Atish; ORTIZ, Samuel

Presenter: SAHITA, RAVI (Rivos)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC