Contribution ID: **410** Type: **not specified**

Trusted I/O: Architectures and Implementations for Confidential Computing

Friday 20 September 2024 12:20 (30 minutes)

The secure and efficient transfer of data between confidential computing environments and the outside world is a critical challenge. This session brings together experts from different architectures to discuss the latest advancements in trusted I/O. We will explore the design principles, implementation details, and interoperability aspects of emerging standards such as RISC-V CoVE-IO, Arm CCA, AMD SEV-TIO and TDX Connect together with TDISP.

By understanding the commonalities and differences between these architectures, we aim to foster collaboration and identify opportunities for standardization and interoperability. The session will cover topics such as trusted device assignment, PCI pass-through, and the integration of trusted I/O into the Linux kernel.

Primary authors: KARDASHEVSKIY, Alexey (AMD); WILLIAMS, Dan (Intel Open Source Technology Center); Mr YAO, Jiewen (Intel Corporation); ORTIZ, Samuel; KURUPPASSERY POULOSE, Suzuki (Arm Holdings Ltd)

Presenters: KARDASHEVSKIY, Alexey (AMD); WILLIAMS, Dan (Intel Open Source Technology Center); Mr YAO, Jiewen (Intel Corporation); ORTIZ, Samuel; KURUPPASSERY POULOSE, Suzuki (Arm Holdings Ltd)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC