Contribution ID: **293** Type: **not specified**

SoC peripheral TDISP

Friday 20 September 2024 12:50 (10 minutes)

The PCIe TEE Device Interface Security Protocol (TDISP, aka TEE-I/O) specifies requirements for a TEE Security Manager (TSM) on the host and a Device Security Manager (DSM) on a PCIe device, including an on-chip Root Complex-integrated Endpoint (RCiEP). TDISP also specifies protocols between TSM and DSM to establish trust between a confidential VM and a PCIe device or function, secure the connection between them, and attach and detach them in a trusted manner.

System-on-Chip (SoC) peripherals present unique opportunities and challenges when compared with PCIe peripherals –even compared with RCiEPs. On the one hand, being on-chip provides better architectural protection for the connection between confidential VM and peripheral. On the other hand, being on-chip and not bound to a standard interface specification enables low-level optimisations for power, performance and cost. These optimisations lead to a variety of options for secure management and peripheral partitioning as well as complex, cross-domain use cases.

As a result, there is a lack of common mechanisms to establish trust between a confidential VM and an SoC peripheral or to attach and detach them securely. PCIe TDISP and the corresponding Linux interfaces offer a promising starting point for a common abstraction between PCIe and SoC peripherals.

This presentation describes the opportunities and challenges with SoC peripherals and raises some directions for further exploration in adapting TDISP and its support in Linux.

Primary author: HARTLEY, David (Qualcomm Germany GmbH)

Presenter: HARTLEY, David (Qualcomm Germany GmbH)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC