Contribution ID: **217** Type: **not specified**

PCI device authentication & encryption

Thursday 19 September 2024 15:00 (45 minutes)

PCIe 6.0 introduced device authentication and encryption (sec 6.31 and 6.33). We are bringing up kernel support, seeking consensus with the community at past Plumbers installments (2023, 2022, 2021).

We would like to continue this fine tradition by presenting our progress since last year's Plumbers and having an open discussion on the next steps towards mainline.

An updated patch set for PCI device authentication was submitted in June 2024. It addresses three key requests raised at last year's Plumbers:

- **Transparency log**:
  The kernel exposes a log of signatures received from the device in sysfs, which allows for their re-verification by remote attestation services. Requested by James Bottomley.
- **Code reuse and common ABI with ATA and SCSI**:
  ATA and SCSI are adopting the generic SPDM protocol upon which PCI device authentication is built. The kernel implementation has been amended to allow for code reuse by ATA and SCSI subsystems and a common user space ABI. Requested by Damien Le Moal.
- **Coexistence with TSMs**:
  Recent CPUs are integrating Trusted Security Modules (TSMs) which set up PCI device authentication and encryption for confidential DMA from a device into encrypted guest memory. Dan Williams is working on a patch set to negotiate between kernel and TSM which of the two is responsible for PCI device authentication and encryption.

We are particularly keen to hear feedback on the user space ABI for certificate and signature exposure and on remaining blockers seen by community members.

We would also like to discuss upcoming features such as certificate provisioning, measurement retrieval and encryption setup.

The audience of this BoF includes PCI, CXL and confidential computing developers.

Primary authors: WUNNER, Lukas; CAMERON, Jonathan (Huawei Technologies R&D (UK))

Presenters: WUNNER, Lukas; CAMERON, Jonathan (Huawei Technologies R&D (UK))

Session Classification: Birds of a Feather (BoF)

Track Classification: Birds of a Feather (BoF)