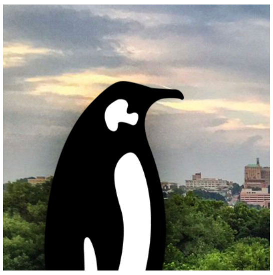
Linux Plumbers Conference 2023



Contribution ID: **134**

Type: **not specified**

PCI device authentication & encryption

Wednesday, 15 November 2023 15:15 (45 minutes)

At LPC 2022 we had a fruitful BoF session to align on an architecture for PCI device authentication (CMA-SPDM, PCIe r6.1 sec 6.31).

The BoF allowed community members' concerns to be addressed. Rough consensus on a path forwards was established, with device authentication to be performed by the PCI core before a driver is probed.

At the time, a proof-of-concept implementation of in-kernel CMA-SPDM had been submitted as an RFC.

That implementation has since been refined and extended based on what we discussed at LPC 2022, and it was submitted as a non-RFC patch set before LPC 2023.

We would like to reconvene for a face-to-face discussion on these authentication patches and the next steps to bring up measurement retrieval, certificate provisioning and encryption on top of them (IDE, PCIe r6.1 sec 6.33).

Another topic worth discussing is how this in-kernel implementation can be made to work with vendor-defined firmware implementations (such as Intel TDX Connect, AMD SEV-TIO, ARM CCA).

The audience of this BoF includes PCI, CXL and virtualization developers interested in device security.

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

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

Session Classification: Birds of a Feather (BoF)

Track Classification: Birds of a Feather (BoF)