

Linux Plumbers Conference 2025



Contribution ID: 399

Type: **not specified**

Discussion: TDISP, VM migration, and paravisors

TDISP, designed to allow a confidential VM to establish a trust relationship with a PCI device, creates new headaches for the Linux PCI stack and for virtualization components:

- Evaluating whether a device is trustworthy.
- Establishing trust with the device.
- And in particular, re-establishing trust across a VM migration to a different physical device, without workload disruption.

Solving these problems natively in the Linux PCI stack comes with one set of challenges. Solving this underneath Linux in a trusted paravisor comes with a different set of tradeoffs.

We propose to guide a discussion around different solutions to this to determine what's most acceptable for the Linux community.

Potential interested stakeholders:

- * Joerg Rodel
- * Dan Williams

Primary authors: OO, Chris (Microsoft); STARKS, John (Microsoft); LANGE, Jon (Microsoft)

Presenter: STARKS, John (Microsoft)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC