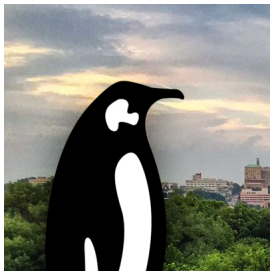

Contribution ID: **176** Type: **not specified**

Trust, confidentiality, and hardening: the virtio lessons

Wednesday, 15 November 2023 14:30 (45 minutes)

Can you trust your hardware? How do you know? And if not can you still use it?

These questions are not new, however linux currently lacks a comprehensive answer. The confidential computing platforms that are becoming more popular offer both a new perspective and new uses - and with them, a new sense of urgency - to efforts to answer these questions.

Being a common part of the hypervisor/guest interface, virtio found itself at the forefront of some of these efforts.

This talk will review several approaches to the question of trust and highlight some (sometimes subtle) differences between these.

Further, the experience in virtio driver hardening will be reviewed, including difficulties posed by existing infrastructure and issues that remain unaddressed to this day.

Finally, some ideas for unifying our approach to trust in hardware will be presented.

Primary authors: TSIRKIN, Michael S. (Red Hat); HAJNOCZI, Stefan (Red Hat)

Presenters: TSIRKIN, Michael S. (Red Hat); HAJNOCZI, Stefan (Red Hat)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track