Contribution ID: **298** Type: **not specified**

Confidential Devices (TEE I/O): A series of modest proposals

With required updates to the PCI core, device core, CPU arch, KVM, VFIO, IOMMUFD, and DMABUF the TEE I/O effort has a significant amount of work to do reach the *starting line* of the race to address Confidential Device use cases. Then, the mechanisms for devices to enter the locked state, the attestation and policy infrastructure for deploying secrets to TEE VMs, and the ability to recover a Trusted Computing Base (TCB) when errors inevitably occur , is all follow-on work to that initial base.

This discussion will quickly review what has happened since last Plumbers and then open a discussion on the remaining challenges. Particular focus to be paid to the host side challenges (VFIO, IOMMUFD, DMABUF, KVM) as those are likely to still be open well into the new year.

Primary author: WILLIAMS, Dan (Intel)

Presenter: WILLIAMS, Dan (Intel)

Session Classification: VFIO/IOMMU/PCI MC

Track Classification: VFIO/IOMMU/PCI MC