Contribution ID: **260**

Type: **not specified**

Untrusted/External devices management

Wednesday 26 August 2020 08:15 (25 minutes)

Location v/s Trust

- Currently firmware can mark ports as external-facing (and thus indicates any devices downstream that port are external). PCI & IOMMU subsystem treats external devices as untrusted (ATS is not allowed, sets up bounce buffers, and uses "strict" iommu).
- We should separate "Location" from "Trust". (Not all internal devices may be trustworthy).
- Location of a device should be exposed to the user space as a read only property. (E.g. use case: user may want to keep statistics about external devices plugged, and differentiate it from internal devices).
- It is OK if we want to treat external devices as untrusted (as current). But we should expose the pci_dev->untrusted property of the device to userspace (to allow it to implement any special policies it may want to implement for untrusted devices).
- Ideally userspace should also be able to change the pdev->untrusted attribute (i.e. be able to choose which devices to treat as trusted vs untrusted). This is a harder problem to solve as pdev->untrusted is used in the boot path by IOMMU code (i.e. before userspace comes up).

I agree to abide by the anti-harassment policy

I agree

Primary author: Mr JAIN, Rajat (Google)

Presenter: Mr JAIN, Rajat (Google)

Session Classification: VFIO/IOMMU/PCI MC

Track Classification: LPC Microconference (Closed)