Contribution ID: **185** Type: **not specified**

Device attestation, secure channel setup / SPDM - how to make progress?

Tuesday, September 13, 2022 3:00 PM (1h 30m)

In 2021, at the Plumbers VFIO/IOMMU/PCI micro-conference, we introduced device attestation of PCI devices via CMA/SPDM (Component Measurement and Authentication / Security Protocol and Data Model). However, device attestation and SPDM is not a PCI specific topic and the decisions made for a Linux implementation need to take into account other transports and use cases. Hence this proposal for a BoF rather than session in either PCI or CXL uconf.

Whilst the 2021 session was productive in raising awareness of this important topic and finding others who had short term requirements, it was new to many of those attending so little progress was made on some of the open questions.

Moving forwards a year, interest in this space has grown with the side effect that the list of questions is getting ever longer and fundamental disagreements have occurred that would benefit from face to face discussion. As such, this BoF will assume the audience are at least somewhat familiar with the topic and what has been proposed and move rapidly onto plotting a path forwards.

Current status:

  RFC for in-kernel session establishment (March 2022) Pros and cons of performing device attestation in user-space versus in-kernel: <ul> Pro user-space: Reduction of attack surface (May 2022) Pro in-kernel: Better integration with suspend/resume and PCIe error handling (resets), avoidance of deadlocks (May 2022) Thought experiment: <ul> Kernel-bundled user-space binary to perform attestation (May 2022)

Major Proposed Topics:

  Use models / transports. Need to enumerate these to understand if one solution or several needed. Secure channel negotiation in kernel or in user-space (or novel solutions). The recent discussions of TLS negotiation are somewhat related, though the necessary flows in SPDM are highly constrained and always host-initiated, perhaps leading to a different decision. (TLS coverage on LWN.) There is not a suitable SPDM user-space library / daemon today. (Discuss adaptation of DMTF reference implementation.) Certificate management. Current proposal is simple but is it fine grained enough? Policy control. What is fall back if we can't attest the device? Device driver specific, or more general? Emulation requirements before commonly available hardware. QEMU support for the PCI/CMA transport is available, QEMU emulation MCTP over I2C PoC planned.

People likely to be interested:

  Security / attestation specialists <li> Confidential compute community <li> PCI developers (for attestation and also link encryption key exchange) CXL developers (attestation and link encryption) Those involved in kernel TLS work who may be able to advise on how to avoid pitfalls they have met. USB and others –SPDM is used on these transports, but not clear if OS level support needed. Anyone who likes reading specifications.

I agree to abide by the anti-harassment policy

Yes

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

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

Session Classification: BOFs Session

Track Classification: Birds of a Feather (BoF)