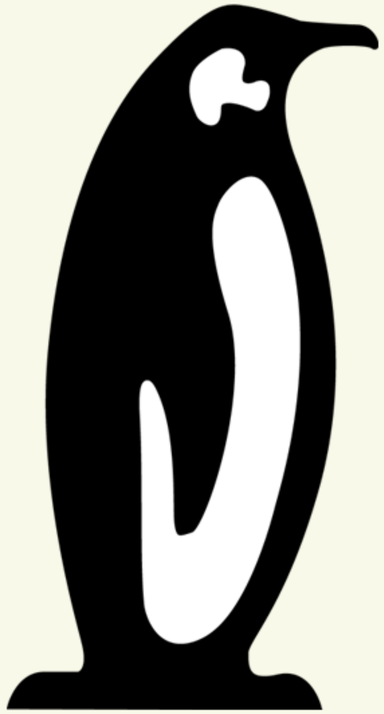


Linux Plumbers Conference

Richmond, Virginia | November 13-15, 2023

Linux
Plumbers
Conference | Richmond, VA | Nov. 13-15, 2023

PCI device authentication & encryption

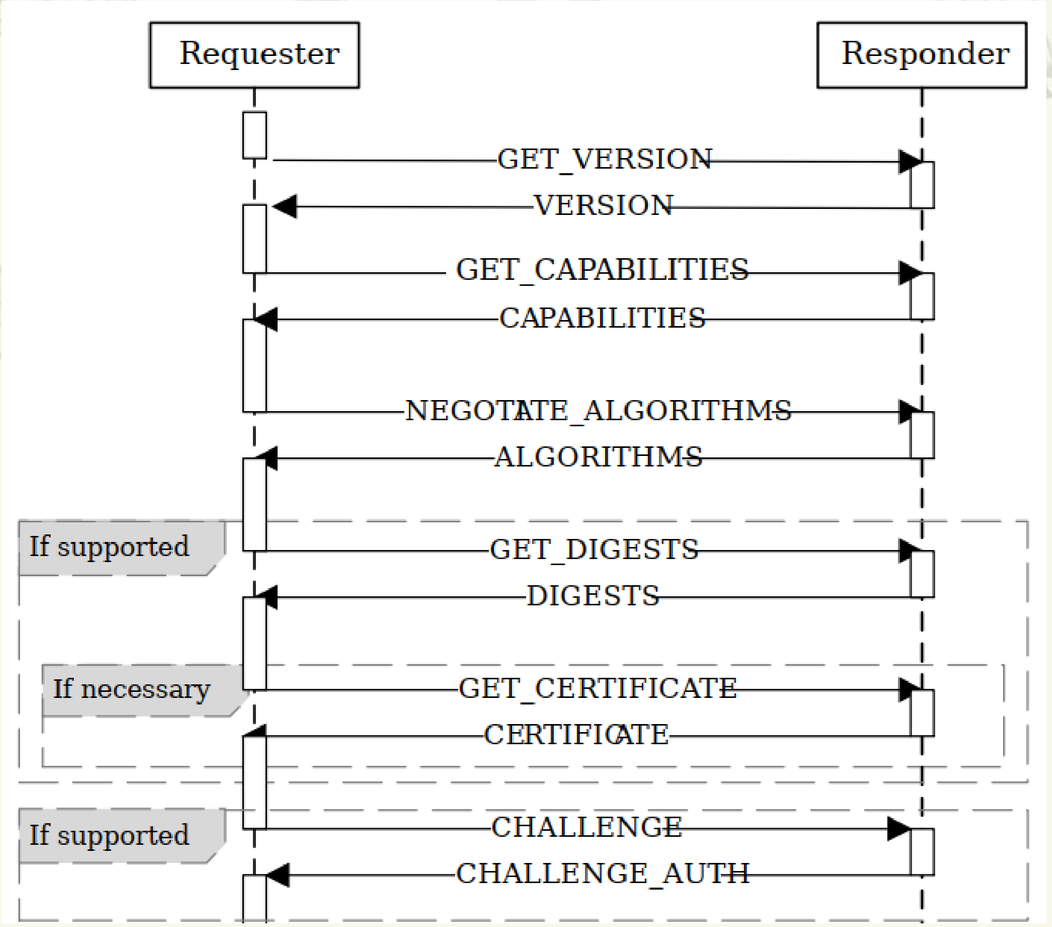
Agenda

- Report current patch status
- Present upcoming features
- Reach alignment on extant controversies

PCI device authentication & encryption

Security Protocol & Data Model (SPDM)

- Generic protocol for device authentication, measurement, secure channel establishment
- Adopted by PCI, CXL and others
- Only one entity in the system may control SPDM session with a device (because GET_VERSION resets session)



Two roads diverged in a yellow wood

- SPDM handled by OS kernel
  + Seamless integration with PCI reset recovery & resume from D3cold
  + Fine-grained control of SPDM features (e.g. measurements are always fresh)
  – Virtualization issues:
    Guest needs help from host or security module for encryption setup
    Virtual functions not supported, only pass-through of full physical device

- SPDM handled by security module inside CPU (Intel TDX Connect, AMD SEV)
  – Needs to be supported by device
  – Need to trust firmware blob from CPU vendor
  – API of security module is vendor-specific, not standardized

PCI device authentication (handled by OS kernel)

- Submitted Sep 2023, respin in Q4
  https://lore.kernel.org/all/cover.1695921656.git.lukas@wunner.de/
- Guide how to test with qemu by Wilfred Mallawa
  https://github.com/twilfredo/qemu-spdm-emulation-guide
- Only controversy: SPDM control by OS kernel versus security module
- Proposed solution:
  Host OS kernel initially authenticates devices,
  hands over SPDM control to security module upon passthrough
  of physical device or one of its VFs:
  pci_cma_claim_ownership() / pci_cma_return_ownership()

PCI device measurement (upcoming)

- Expose the up to 254 measurement indices:
  /sys/bus/pci/devices/0000:00:00.0/measurements/0xab_type (ASCII hex, r/o)
  /sys/bus/pci/devices/0000:00:00.0/measurements/0xab_digest (ASCII hex, r/o)
  /sys/bus/pci/devices/0000:00:00.0/measurements/0xab_bitstream (bin_attribute, r/o)
- Retrieve measurements on-demand for freshness
- On PCI enumeration, determine which measurement indices are populated
  (retrieve digest of all measurements)
- Open question: What if signed measurements are not supported?
  (expose that fact or force user space to opt-in to unsigned measurements?)
- When SPDM is controlled by security module, must expose measurements the same way!
  (retrieve them from Device Interface Report)

PCI device authentication & encryption

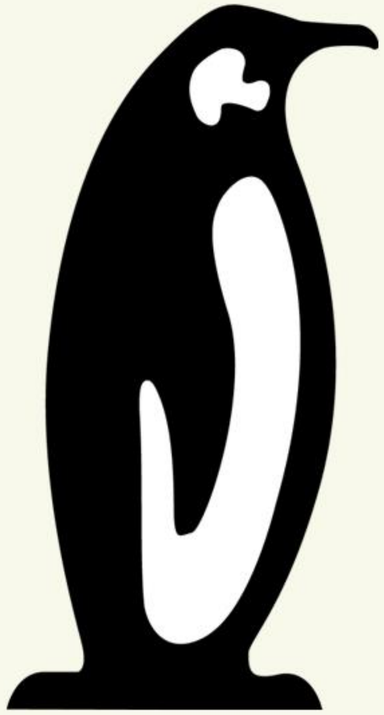
PCI certificate exposure (upcoming)

- Expose all 8 slots:
  /sys/bus/pci/devices/0000:00:00.0/certificates/slot0 .. slot7 (bin_attribute, r/w)
- Read to get X.509 cert chain, parseable with openssl
  Write to trigger SET_CERTIFICATE exchange
  Unpopulated slot has length 0
- Get a certificate signing request from device:
  /sys/bus/pci/devices/0000:00:00.0/certificates/csr (bin_attribute, r/w)
- Read to trigger GET_CSR exchange
  Write beforehand to set PKCS#10 CertificationRequestInfo (optional)

PCI device authentication & encryption

PCI secure channel establishment (upcoming)

- Unsigned measurements tolerable if transported over secure channel
- Prerequisite for PCI encryption setup by OS kernel
- Implement Diffie-Hellman key exchange
- Implement symmetric encryption of SPDM messages



Linux Plumbers Conference

Richmond, Virginia | November 13-15, 2023