Linux Plumbers Conference 2022

>> Dublin, Ireland / September 12-14, 2022

SPDM & Device Attestation

Linux Plumbers Conference 2022

>> Dublin, Ireland / September 12-14, 2022

Ideal Outcomes

- Clear set of requirements
- Constraints on options
- A cunning plan...

Linux Plumbers Conference 2022

>> Dublin, Ireland / September 12-14, 2022

SPDM BoF – Agenda

- Agenda Bashing
- Introduction to SPDM
- Use cases
- Contentious issues list
- Discussion

Linux Plumbers Conference 2022

>> Dublin, Ireland / September 12-14, 2022

Device Attestation – Why?

- Authenticate pluggable components
  - Repel attacks
    - replacement (attestation)
    - interception (encryption)
  - Detect incorrectly plugged components
- Verify device state
  - Repel attacks on firmware (could be changed by host, BMC etc)
  - Detect unexpected state

Device Attestation – How

- Establish device we see is the device we think it is
  - Public key crypto: device has secret, presents certificate chain
- Establish state of device
  - Signed measurements: e.g. firmware image signature
- Link protection
  - Establish secure channel, exchange encryption key

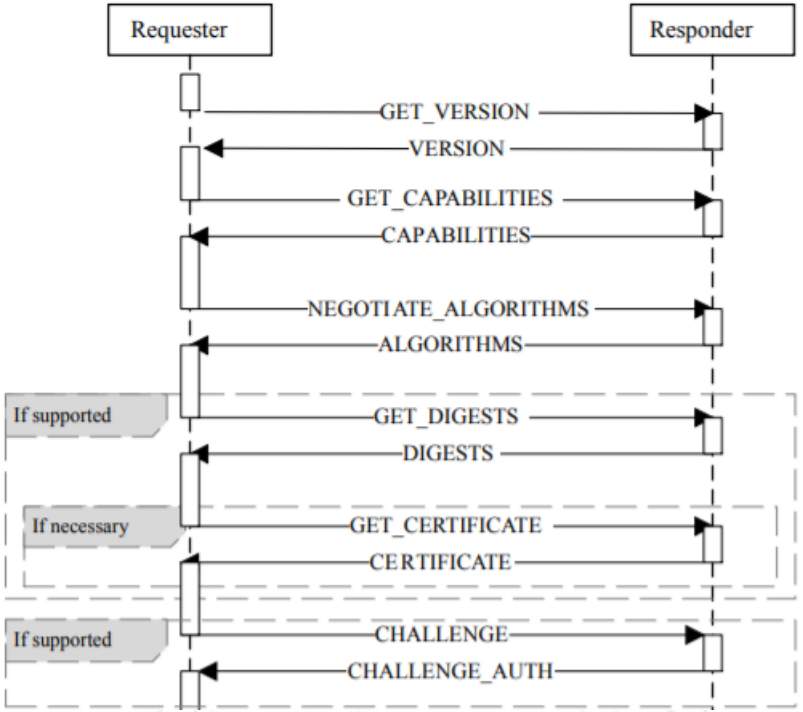
Device Attestation – Where?

- Attestation handled by Trusted Element
  - If hypervisor not trusted
  - Use case: Trusted Virtual Machines / Confidential Computing
  - Attestation probably not Linux's problem
- Attestation handled by Operating System
  - Use case: Bare metal composable servers
  - Attestation is Linux's problem, Linux may be Root of Trust

DMTF SPDM

- Security Protocol and Data Model
- Defines exchanges + state machines to attest devices, take measurements and establish secure channel
- Communicates with devices through one of several transports:
  - PCI DOE (mailbox in config space)
  - MCTP
  - Others

SPDM – Exchange



- CHALLENGE_AUTH flow establishes device identity
- Stateful, effectively single operation
- Subsequent exchange retrieves measurements
- Mutual authentication supported

SPDM – Adoption

- PCI CMA (Attestation and Measurement)
- PCI IDE (Link Encryption)
- PCI TDISP (Trusted I/O Virtualization)
- CXL
- Open Compute Project
  - NVMe
  - System Components Attestation

SPDM – What exists today

Kernel elements:

- Transports:
  - MCTP (v5.15)
  - PCI DOE (v6.0)
- SPDM library PoC
- CXL device attestation PoC

Supporting elements:

- libspdm
  - reference implementation
  - used for testing,
    not currently part of solution
- QEMU passthrough to libspdm

Linux Plumbers Conference 2022

>> Dublin, Ireland / September 12-14, 2022

Contentious Questions!

- Useful or not? (at Linux layer of stack)
- Certificate handling in kernel vs. in user space?
  - Can't depend on user space after resume
  - Potential deadlocks
- Idea: kernel-bundled user space binary (à la net/bpfilter/)?
- Security policy: hard coded vs. user configurable?