Platform Security: Infrastructure Protection with DMTF's Security Protocol & Data Model (SPDM)

Viswanath Ponnuru
Dell Technologies

Agenda

- Platform Security – Attack Surface
- Platform Component Security Concerns
- Security Protocol Data Model (SPDM) Overview
- SPDM Authentication
- SPDM MCTP Binding
- Alliance Partners
- Additional Information

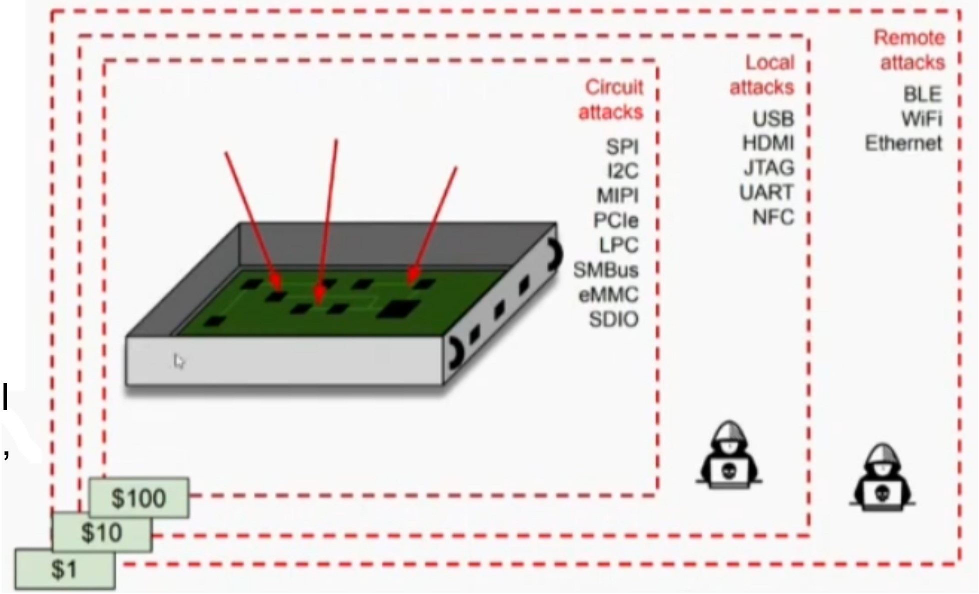
Platform Security – Attack Surface

Datacenter Service Provider Platform Security Concerns

- Detection of vulnerable hardware Components is not easy.

- Attackers are reportedly exploiting an unpatched vulnerability to take control of the platform device.

- Attackers abuse platform interface protocol analyzers to steal unencrypted information, spy on the network traffic and gather information to leverage in future attacks against the network.(I2C, SPI,..)



Ref: https://www.platformsecuritysummit.com/2019/speaker/wood/

Supply Chain Security

- Malicious code injection in the firmware
- Integrity of the firmware

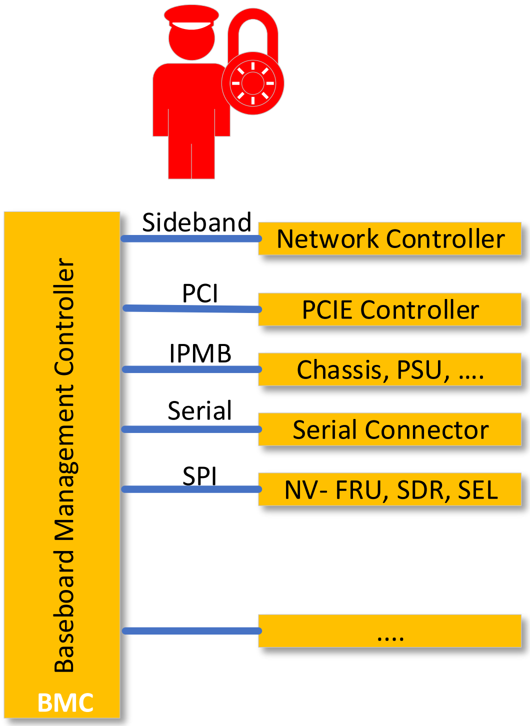
How to prevent and protect from platform component sensitive data disclosure?

Platform Component Security Concerns

These platform circuit attacks, are preying on data transfers that are unencrypted and vulnerable to eavesdropping, stealing, tampering and manipulations between the components of a platform subsystem.

Some of the security risks are:

- Sensitive (device credentials) information leakage
- Hostile component insertion, Compromised firmware(s) & Supply Chain issues
- Un-trusted device(s) snooping via probes.

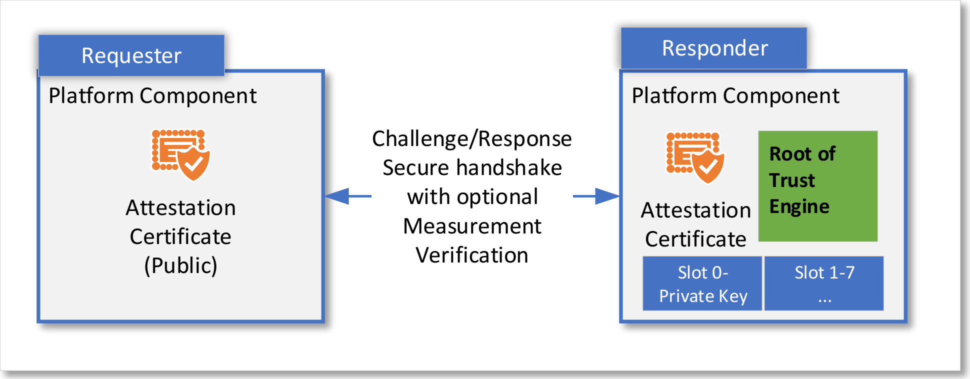


Security Protocol Data Model (SPDM) Overview

The primary goal of the Security Protocol Data Model specification is to cryptographically verify the identity and firmware integrity of each platform component is shown in diagram. And enable payload encryption and integrity protected management plane (MCTP) and other alliance partner interfaces.

Benefits:

- Certificate based authentication provides Platform Component Identity Assurance
- Facilitate privacy and data security communications over the platform interfaces.
- Root of Trust Measurement for firmware integrity checks.
- Leveraging the industry proven standards approach such TLS, USB Authentication, etc.

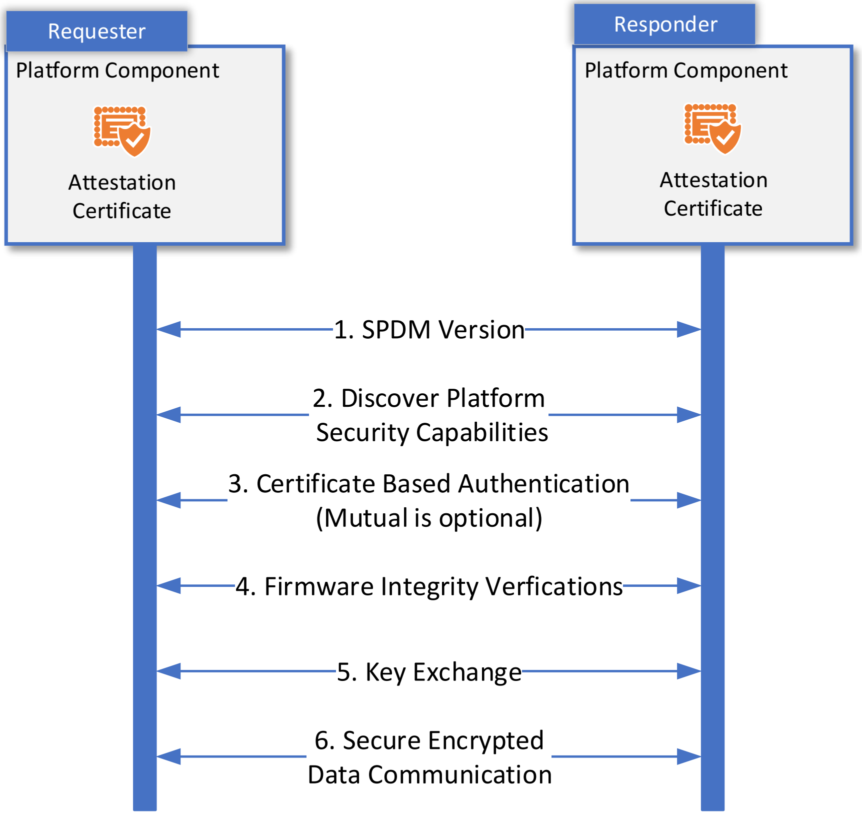


SPDM Authentication

The SPDM defines sets of messages that are exchanged between platform components for establishing the encrypted communications.

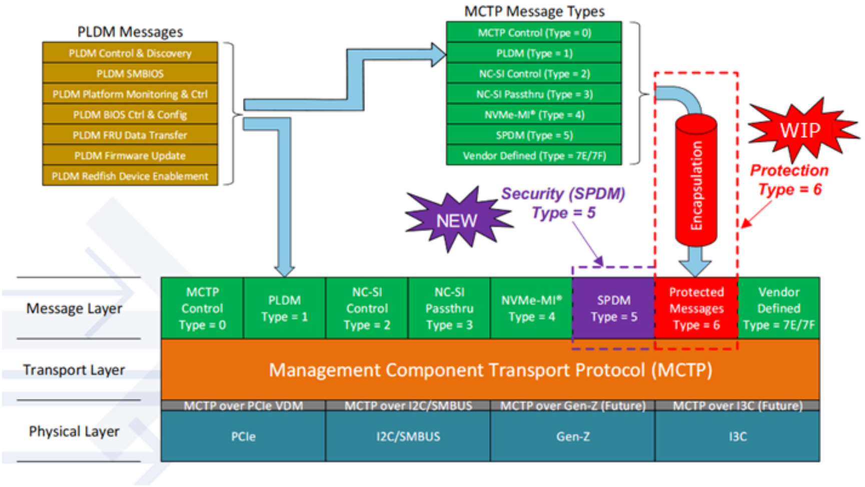
This process helps:

- Achieving both confidentiality, authenticity by verify each other identity
- Negotiate cipher suites and crypto algorithms required to establish a secure connection
- Determines what version of SPDM version will be used in the session
- Request/Response is bidirectional, any component can request for authentication.


Requester
Platform Component
Attestation Certificate
Responder
Platform Component
Attestation Certificate
1. SPDM Version
2. Discover Platform Security Capabilities
3. Certificate Based Authentication (Mutual is optional)
4. Firmware Integrity Verfications
5. Key Exchange
6. Secure Encrypted Data Communication

SPDM over MCTP Binding

- SPDM over MCTP binding defines the format of SPDM messages transported over MCTP
- MCTP Message Types for SPDM is shown in the figure and details:
  - Type 5: Device security capability discovery, initial handshake and session key exchange
  - Type 6: Encrypting the payload once type 5 is established between Requester and Responder



PLDM Messages

PLDM Control & Discovery
PLDM SMBIOS
PLDM Platform Monitoring & Ctrl
PLDM BIOS Ctrl & Config
PLDM FRU Data Transfer
PLDM Firmware Update
PLDM Redfish Device Enablement

MCTP Message Types

MCTP Control (Type = 0)
PLDM (Type = 1)
NC-SI Control (Type = 2)
NC-SI Passthru (Type = 3)
NVMe-MI® (Type = 4)
SPDM (Type = 5)
Vendor Defined (Type = 7E/7F)

Encapsulation

WIP

Protection Type = 6

NEW

Security (SPDM) Type = 5

Message Layer

MCTP Control Type = 0
PLDM Type = 1
NC-SI Control Type = 2
NC-SI Passthru Type = 3
NVMe-MI® Type = 4
SPDM Type = 5
Protected Messages Type = 6
Vendor Defined Type = 7E/7F

Transport Layer

Management Component Transport Protocol (MCTP)

MCTP over PCIe VDM
MCTP over I2C/SMBUS
MCTP over Gen-Z (Future)
MCTP over I3C (Future)

Physical Layer

PCIe
I2C/SMBUS
Gen-Z
I3C

Alliance Partners

The SPDM message exchanges are defined in generic fashion that allows the messages to be communicated across different physical mediums over different transport protocols. For the complete list of DMTF alliance partners are available in the location.

Some of the SPDM message exchange capabilities are based on security model that the USB Authentication Specification Rev 1.0 with ECN and Errata through January 7, 2019.

Additional Information

DMTF SPDM
Version 0.9 - https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_0.9.0a.pdf
Version 1.0 - https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.0.0.pdf
Version 1.1 - https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.1.0.pdf

SPDM over MCTP Binding
Version 1.0 - https://www.dmtf.org/sites/default/files/standards/documents/DSP0275_1.0.0.pdf