End-to-End Infrastructure Security

Security Protocol and Data Model
Scott Phuong, PMCI Security Taskforce Co-Chair,
Cisco Systems, Inc
Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change without notice. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website.

- This information is a summary of the information that will appear in the specifications. See the specifications for further details.
Cypher Security Report

- December 19, 2013
  - Target retail store data breach cost $252 million and Target’s CEO his job.

- Mid-2016
  - Yahoo user accounts were hacked, cut $350 million from Verizon’s Yahoo acquisition price.

- August 16, 2017
  - Maersk reported that the NotPetya cyberattack could cost their business $300 million in lost revenue.

- October 4, 2018
  - Bloomberg report on a physical attack on a particular server vendor’s platform.
    - Ultimately, no evidence was found but experts have re-created the alleged scenario.

- January 22, 2019
  - U.S. Cybersecurity and Infrastructure Security Agency issued an emergency directive to mitigate DNS infrastructure.

www.dmtf.org
Existing Security Solutions

- **Two Categories**
  - **Inside the Platform**
    - Security solutions that protect data inside the platform.
    - Examples:
      - Secure Boot
      - Secure Storage (of direct attach, on-board storage such as SPI Flash)
  - **Remote-based Attack**
    - Security solutions that protect data that is being remotely accessed (often over the network)
    - Examples:
      - SSL (deprecated) / TLS
      - IPSec
      - Anti-Virus/Malware/Spyware
      - Firewalls
Missing Security Solutions

- Infrastructure
  - Mainly, Building Trust from End-to-End
  - Examples
    - Chip to Chip
      - In-the-box Wires (e.g. PCIe, I2C, I3C, SPI, USB, CAN, etc…)
    - Building Trusted Channel between Components
    - The Physical Aspect of an Infrastructure.
- Platforms
  - Blades/Racks/Desktops
  - Mobile
  - IoT
- Fabric-based Platforms
  - Remote Resources (outside traditional management domain)
Building Security in Infrastructure

• Need to start from the ground up. The ground builds the infrastructure.

• What is the ground?
  • The hardware that builds the infrastructure
  • Specifically:
    • Communicating Devices (e.g. network controllers, GPUs, video devices, storage devices, etc…)
    • Non-communicating components (e.g. power supplies, fans, etc…)
    • The Interconnects (i.e. the physical wires/buses)

• Why?
  • They are all subject to attack.
    • Threats include supply-chain attacks.
  • Exploitation is shifting from software to hardware/firmware.
  • If there is gain to be had, then it will be exploited.
Security Protocol and Data Model 1.0

- How?
  - Two Major Features
    - Authentication
    - Attestation
  - Capable of being referenced by other standards.
    - DMTF is initially mapping to MCTP.
    - Alliance Partners are considering mapping SPDM to their standards.
Security Protocol and Data Model 1.0

• Other Important Features:
  • Leveraged and Extended USB authentication.
  • Extensible
  • Negotiable Communication Details (e.g. version, algorithms, capabilities)
  • Flexible for Implementors
  • Transport Agnostic: Other Standards can leverage this.
  • Platform-Independent
SPDM 1.0 – Authentication

- Allows a platform to verify the identity of the attached component.
- Redfish
  - Identity is also exposed in Redfish.
- Enables a platform to determine what to do if the identity of a component did not verify correctly.

- Cryptography
  - Leverage X.509v3 certificates

www.dmtf.org
SPDM 1.0 – Attestation

• Allows a platform to verify the state of the component.
• Multiple measurements allow platforms to verify various configurations of the component.

• Measurements:
  • Hashes of various configurations of a component

• Examples of Measurement Coverage (Implementation Choices):
  • Immutable Code
  • Mutable Code
  • Boot Stages
  • Configuration Data
  • State Variables
PMCI MCTP Security Proposal – Diagram View

**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)

**Future**
- 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**
- 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

www.dmtf.org
MCTP Message Type 5 (Security Commands) Format

Physical Medium-Specific Header

- MCTP Reserved
- Hdr Version
- Destination Endpoint ID
- Source Endpoint ID
- SOM
- EOM
- Pkt Seq #
- T O
- Msg Tag

Message Type Payload (Variable Length)
May span one or more MCTP packets

Message Integrity Check

Repeated for each MCTP packet

MCTP Message Body

- Message Type 0000101 = 5
- SPDMVersion
- RequestResponseCode
- Param1
- Param2

www.dmtf.org
SPDM 1.0 - Ladder

Requestor

Responder

Get Capabilities

Capabilities

Negotiate

Algorithms

Get Digest

Digest

Get Certificate

Certificate

Challenge

Challenge Auth

Get Measurements

Measurements
Future Work

- Protection: Encryption / Integrity
- Measurement log
- Set certificate command
- Measurement manifest (Local attestation)
Summary

• **SPDM 1.0**
  • Provides Authentication and Attestation

• **In general, SPDM**
  • Provides building blocks and tools to secure the Infrastructure.
Call to Action

- Would like the Industry to use SPDM as a security protocol for their standard(s).
- Would like the Industry to work with DMTF (PMCI Security TF) to help extend SPDM for their needs.
  - Provide feedback via DMTF Portal.
  - Help us with future specification development.
References

- DMTF
  - Main Website: https://www.dmtf.org/
  - PMCI Workgroup: https://www.dmtf.org/standards/pmci
    - Updated News for SPDM
    - Security Protocol and Data Model (DSP 274)
    - SPDM MCTP Binding (DSP 275)
    - Upcoming White Paper
  - Redfish:
    - Workgroup: https://www.dmtf.org/standards/redfish
    - Developer’s Hub: https://www.dmtf.org/standards/redfish
References

• News Links:
  • https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html
  • https://hackaday.com/2019/05/14/what-happened-with-supermicro/
  • https://cyber.dhs.gov/ed/19-01/