DMTF

Technical Note

Enabling Platform Integrity in a Common Way by Utilizing DMTF's SPDM Standard

Introduction

Companies face security risks, threats, and challenges to their computing infrastructure every day. Consequently, platform security is becoming increasingly important as the fundamental building block to enable infrastructure security from the ground up. As platform firmware components have become a new area for attacks, DMTF has developed the Security Protocol and Data Model (SPDM) standard to address these challenges. Developed by the Security Protocols and Data Models Working Group, DMTF has created ***the*** platform security protocol.

What does this mean exactly?

When implemented properly, SPDM is a critical component needed to ensure a complete chain of trust for the platform. SPDM defines messages, data objects, and sequences for performing message exchanges between devices and components over a variety of transport and physical media. The description of message exchanges includes authentication of hardware identities, measurement for firmware identities and session key exchange protocols to enable confidentiality and integrity protected data communication. SPDM enables efficient access to low-level security capabilities and operations.

By using SPDM, data and management traffic inside the box can be encrypted – like HTTPS encrypts your traffic over the Internet. SPDM over the data plane enables encryption of data in flight. SPDM over the management and control plan enables integrity and encryption of management traffic. Add the ability to validate firmware measurements and you have the building blocks needed by the industry to ensure infrastructure integrity. Thus, SPDM is a critical standard that enables the encryption of data and management traffic in flight within any platform adopting these standards. After all, you can't trust the workload unless you can trust the platform.

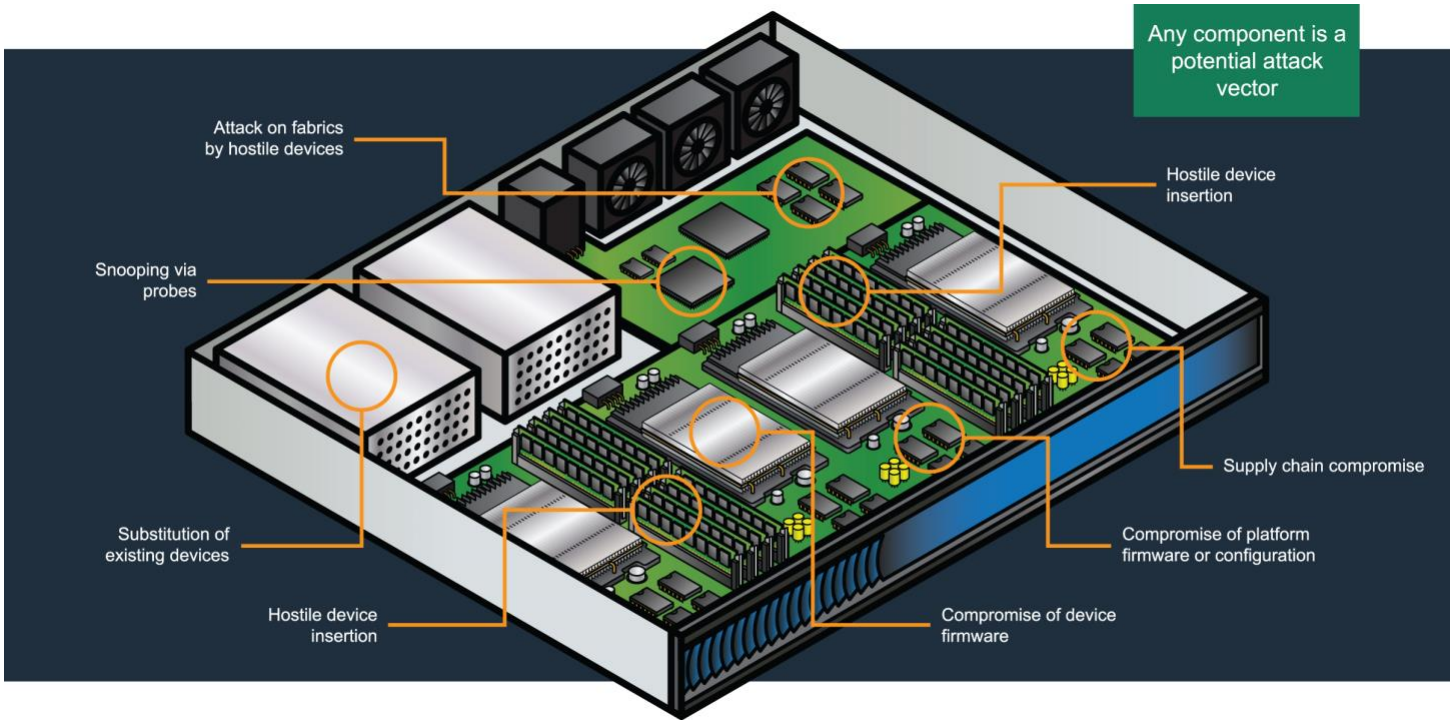
This Technical Note provides an overview of SPDM and highlights how this standard is helping solve platform security concerns in a common way and enabling platform integrity. Developers, implementers, and end users are encouraged to visit the SPDM's Working Group Page https://www.dmtf.org/standards/spdm for more in-depth information.

Enabling Platform Integrity

An attack surface is your environment's total threat exposure, and every piece of silicon, firmware, software, and workload adds to the attack surface. Without the ability to trust the validity of the components in the system, you could expose your infrastructure and not know it until an attack occurs. These platform attacks are preying on data transfers that are unencrypted and vulnerable to eavesdropping, stealing, tampering and manipulations between the components of a platform subsystem. This is true for both the control plane and the data plane.

Some of the security risks are:

- Sensitive information leakage, such as device credentials
- Hostile component insertion, compromised firmware and supply chain issues such as malicious code injection in the firmware and/or integrity of the firmware
- Un-trusted device(s) snooping via probes
- Fraudulent or vulnerable hardware components
- Attackers exploiting unpatched vulnerabilities to take control of the platform device
- Attackers abusing platform interface protocol analyzers to steal unencrypted information, spy on the network traffic or gather information to leverage in future attacks against the network (i.e. I2C, SPI)



SPDM enables authentication, attestation, and key exchange to assist in providing infrastructure security enablement. Other messages that extend functionality of SPDM as well as the development of other standards that enable and enhance infrastructure security are also developed by the SPDM Working Group and done with input based on the needs of DMTF Alliance Partners and the industry.

The goals of SPDM specifications are to cryptographically verify the identity and firmware integrity of each platform component. This enables payload encryption and integrity protected of the data plane (such as those defined by DMTF Alliance Partners) or the control and management plane.

The benefits of utilizing SPDM are:

- Certificate based authentication provides Platform Component Identity Assurance
- Facilitate privacy and data security communications over platform interfaces
- Root of Trust Measurement for firmware integrity checks

SPDM is leveraged by other industry specifications to create a common security framework. As part of our Alliance Partner program, organizations including CXL Consortium, PCI-SIG®, HDBaseT Alliance, MIPI Alliance, Open Compute Project, and the Trusted Computing Group provide crucial input to SPDM thus benefiting the industry at large. For example, PCI-SIG and CXL Consortium help SPDM validate the data plane, but management traffic and encrypting it in-flight are both important thus the SPDM Working Group collaborates within DMTF on these areas too.

The SPDM Working Group not only collaborates with other industry standards bodies, but we work closely with other DMTF groups as well. For example, the SPDM Working Group works closely with the Platform Management Communications Infrastructure (PMCI) Working Group to ensure that the management plane is trustworthy, not just the data plane. Thus, MCTP traffic can use SPDM to establish trust and encrypt the management plane.

The Working Group also works closely with the Redfish Forum to make sure that the security administrator has visibility into the platform integrity using the Redfish interface**.**

Members and non-members are encouraged to ask questions or post comments SPDM on our public forum here: https://spdmforum.com/.

SPDM Open Source

DMTF's SPDM Code Task Force has open source support of several releases – libspdm – and are available for download. You can find all of this in the group's readme at https://github.com/DMTF/libspdm/blob/main/README.md. In addition, details such as the SPDM supported commands, cryptographic algorithm support, design, threat model, and users guide can also be found in the readme in the repository (https://github.com/DMTF/libspdm/blob/main/README.md).

In addition to the core library, libspdm enables spdm-emu, which contains a full SPDM Requester and Responder; spdm-dump, which can parse SPDM messages; and the SPDM Responder Validator, which is still under development but can be used to help test an SPDM Responder implementation for its conformance to the SPDM specification. For more information about libspdm, please visit https://github.com/DMTF/libspdm.

Other mechanisms, including both non-DMTF and DMTF-defined mechanisms, can use SPDM specifications. A sample implementation from the SPDM Code Task Force can be found here: https://github.com/DMTF/libspdm.

Conclusion

The survival of a modern business depends on data security, which can impact both the organization's key assets and private data belonging to its customers. SPDM standards enable platform integrity of the computing platform. By using BMCs and other entities, SPDM can help an established root of trust widen that chain of trust to everything in the infrastructure, therefore helping to secure against outside attacks and actively helping to solve customer and end user concerns by using an open standardized platform security protocol that has been scrutinized by the industry.

SPDM specifications

- Security Protocol and Data Model (SPDM) Specification (DSP0274) defines the contents of the messages, supported exchanges, and requirements.
- Security Protocol and Data Model (SPDM) over MCTP Binding Specification (DSP0275) defines the method for transporting SPDM messages over an MCTP transport.
- Secured Messages using SPDM over MCTP Binding Specification (DSP0276) binds Secured Messages using SPDM specification (DSP0277) to the MCTP transport.
- Secured Messages using SPDM Specification (DSP0277) defines the methodology that various PMCI transports can use to communicate various application data securely by utilizing SPDM.

Note, the Security Protocol and Data Model over MCTP Binding Specification (DSP0275) and the Secured Messages using SPDM over MCTP Binding Specification (DSP0276) fall under the purview of the Platform Management Communications Infrastructure (PMCI) Working Group. The PMCI and SPDM Working Groups collaborate and work cooperatively to maintain the specifications.

Acknowledgements

To learn more about the SPDM Working Group or to get involved in this work, please visit https://www.dmtf.org/standards/spdm. Detailed information on all DMTF standards can be found at www.dmtf.org/standards. For a list of our current Alliance Partners visit https://www.dmtf.org/about/registers. Those interested in supporting and joining DMTF's efforts can learn more at www.dmtf.org/join.