

Équipe : Réseaux  
Sujet : Security Protocol and Data Model

Sujet de TER  
2023–2024

# Security Protocol and Data Model

Lieu	Équipe Réseaux, ICube (UMR CNRS 7357)
Encadrant	Pierre DAVID (pda@unistra.fr)

## Contexte

L'association DTMF (Distributed Management Task Force) regroupe des acteurs importants du matériel tels que Intel, Cisco, Broadcom, etc. Elle édite des standards dans le domaine du matériel et cherche à les promouvoir auprès d'organismes de normalisation.

L'un des standards publiés est SPDm (pour « Security Protocol and Data Model »). Initié en 2019, ce standard en est actuellement à la version 1.3.0 [1]. Basé sur les idées de TLS 1.3, il a pour but d'authentifier les périphériques d'un système et de sécuriser les échanges.

SPDM est encore trop récent pour disposer d'implémentations réelles dans des périphériques : [2] évalue ses performances à partir d'une émulation d'un disque dur et les mêmes auteurs évoquent dans [3] l'implémentation du protocole dans un environnement virtuel. En outre, [4] propose une analyse formelle du protocole en version 1.2.

## Sujet

L'objectif de l'étude est de dresser un état de l'art de la sécurisation de l'accès aux périphériques : menaces posées par l'absence de protocole de sécurité, solutions apportées avant SPDm, solutions proposées par SPDm et impact au niveau du système d'exploitation et des pilotes.

## Références

- [1] DMTF. SPDm v1.3.0 specification (DSP0274). techreport, June 2023.
- [2] Renan C. A. Alves, Bruno C. Albertini, and Marcos A. Simplicio. Securing hard drives with the security protocol and data model (spdm). pages 446–447, July 2022.
- [3] Renan C. A. Alves, Bruno C. Albertini, and Marcos A. Simplicio Jr au2. Benchmarking the security protocol and data model (spdm) for component authentication, 2023.
- [4] Cas Cremers, Alexander Dax, and Aurora Naska. Formal analysis of SPDm : Security protocol and data model version 1.2. pages 6611–6628, August 2023.