

Sécurisation de l'accès aux périphériques et *Security Protocol and Data Model (SPDM)*

Travail d'Étude et de Recherche

Léon GALL

leon.gall@etu.unistra.fr

Encadré par : Pierre DAVID

17 mai 2024



- Importance de la sécurité
 - Confidentialité
 - Authentification
 - Intégrité
 - Disponibilité
- Pas réellement de mesures appliquées pour la sécurité de l'accès aux périphériques

Menaces

- Attaque par l'homme du milieu (MITM)

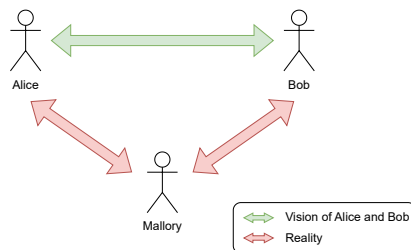


Figure 1: Attaque par l'homme du milieu

- Exemple : Keylogger, sniffer

- Attaque par l'homme du milieu (MITM)

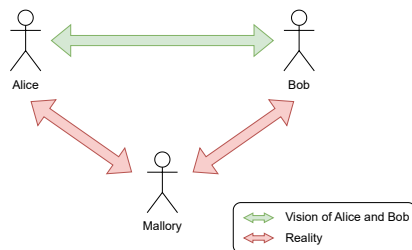


Figure 1: Attaque par l'homme du milieu

- Attaque par usurpation d'identité (Spoofing)
 - Exemple : Rubber Ducky, câble malicieux

Vecteurs d'attaque

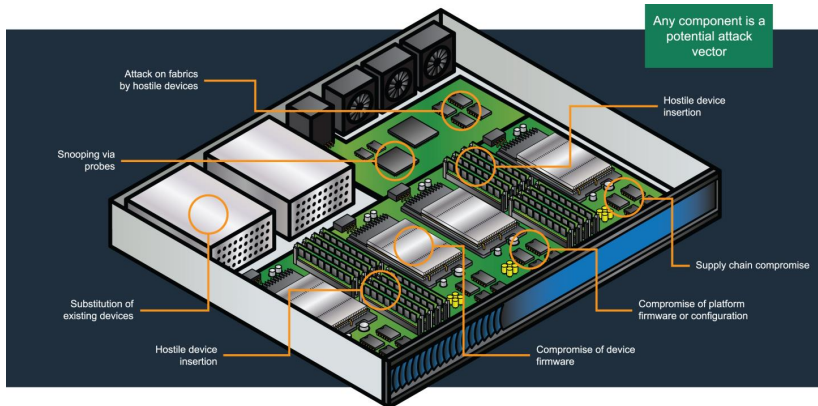


Figure 2: Vecteurs d'attaque. Extrait de [1].

Solutions existantes

Station blanche et sas

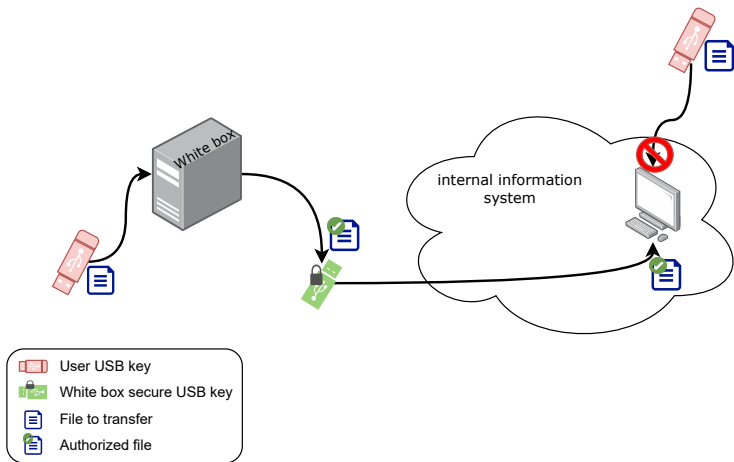


Figure 3: Exemple de station blanche (inspiré de [2])

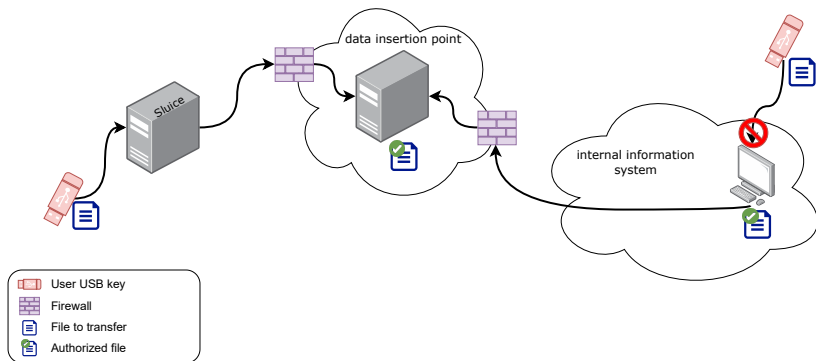


Figure 4: Exemple de sas (inspiré de [2])

- Avantages
 - Contrôle du transfert de données
 - Journalisation
 - Isolement physique

- Avantages

- Contrôle du transfert de données
- Journalisation
- Isolement physique

- Limites

- Complexité du transfert de données
- Dépendance au serveur
- Fonctionne uniquement pour des transferts de fichiers

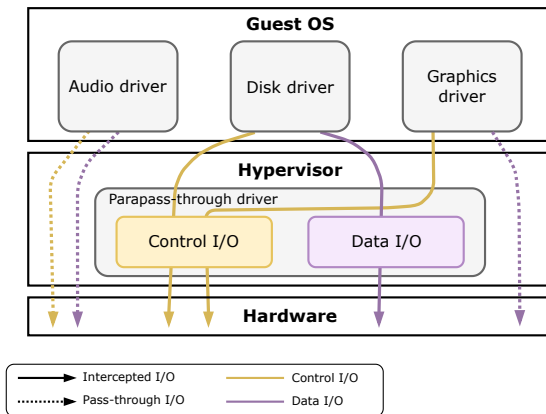


Figure 5: Exemple d'architecture paravirtualisation introduite par BitVisor dans [3].

- Avantages
 - Isolation
 - Détection des accès malveillants

- Avantages
 - Isolation
 - Détection des accès malveillants
- Limites
 - Pas d'authentification des périphériques
 - Surcoût en terme de performances
 - Dépendance à la sécurité de l'hyperviseur

Security Protocol and Data Model (SPDM)

Security Protocol and Data Model (SPDM)

- Développé par un groupe de travail du Distributed Management Task Force (DMTF)
- Première version en 2019
- Actuellement à la version 1.3 (2023)
- Inspiré par TLS
- 2 objectifs :
 - Attestation des périphériques
 - Sécurisation des communications

Security Protocol and Data Model (SPDM)

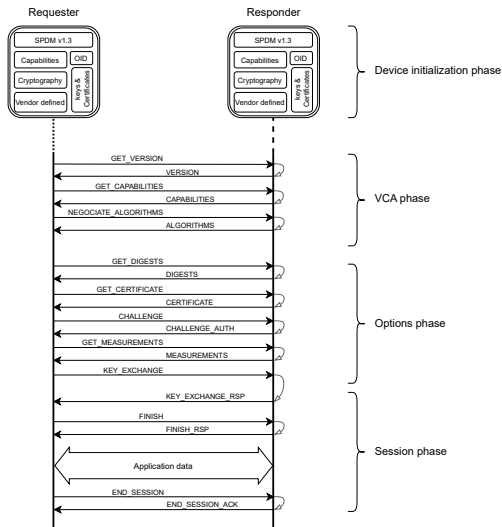


Figure 6: Flux de messages de SPDM

Phase d'initialisation

- Se produit dans un environnement sécurisé de confiance
- Sert à initialiser les parties

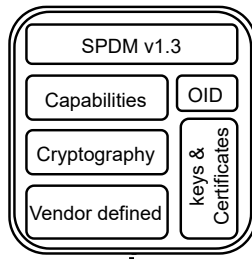


Figure 7: Phase d'initialisation

Phase Version-Capabilities-Algorithms (VCA)

- Permet aux parties de se mettre d'accord sur :
 - **Version** : La version de SPDm
 - **Capabilities** : Les opérations supportées par les parties
 - **Algorithms** : Les algorithmes de cryptographie
- À partir de cette phase des *transcripts* sont échangés

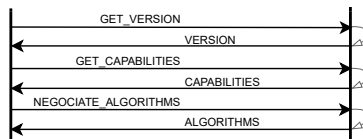


Figure 8: Phase VCA

Phase d'options

- Optionnelle
- Permet une authentification unilatérale
- Permet l'attestation du répondant

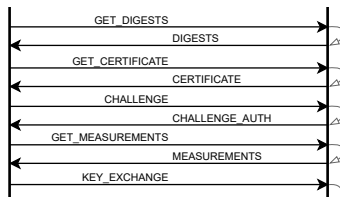


Figure 9: Phase d'options

Phase de session

- Débute par un échange de clés
 - Clés de chiffrement et déchiffrement dérivées de cette clé de session
- Échange de données (chiffrées et/ou authentifiées)
- Mise à jour des clés régulière

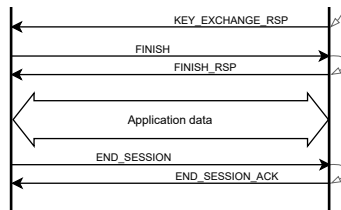


Figure 10: Phase de session

Security Protocol and Data Model (SPDM)

- Avantages
 - Permet des communications sécurisées avec des périphériques
 - Fournit une attestation des périphériques
 - Fonctionnalités principales prouvées formellement dans [4]

Security Protocol and Data Model (SPDM)

- Avantages
 - Permet des communications sécurisées avec des périphériques
 - Fournit une attestation des périphériques
 - Fonctionnalités principales prouvées formellement dans [4]
- Limites
 - Performances des périphériques
 - Peu d'implémentations réelles pour l'instant
 - Quelques problèmes de conception

Security Protocol and Data Model (SPDM)

- Avantages
 - Permet des communications sécurisées avec des périphériques
 - Fournit une attestation des périphériques
 - Fonctionnalités principales prouvées formellement dans [4]
- Limites
 - Performances des périphériques
 - Peu d'implémentations réelles pour l'instant
 - Quelques problèmes de conception
 - Attaque par déclasserement (*downgrade*)
 - Authentification avec clé pré-partagée (PSK)
 - Répondant pas forcé d'utiliser du sel en mode PSK (attaque par rejeu possible)

- État de l'art de la sécurisation de l'accès aux périphériques
- SPDm est trop récent pour avoir du recul dessus
- Quel sera l'impact de la cryptographie post-quantique sur SPDm ?

Des questions ?

Merci pour votre attention.
Avez-vous des questions ?

Références I



“Enabling Platform Integrity in a Common Way by Utilizing DMTF’s SPDm Standard,” Jan. 2024.

DMTF Technical Note.



“Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés),” July 2020.

ANSSI.



T. Shinagawa, H. Eiraku, K. Tanimoto, K. Omote, S. Hasegawa, T. Horie, M. Hirano, K. Kourai, Y. Oyama, E. Kawai, K. Kono, S. Chiba, Y. Shinjo, and K. Kato, “BitVisor: a thin hypervisor for enforcing i/o device security,” in *Proceedings of the 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, VEE '09, (New York, NY, USA), pp. 121–130, Association for Computing Machinery, 2009.

event-place: Washington, DC, USA.



C. Cremers, A. Dax, and A. Naska, “Formal Analysis of SPDM: Security Protocol and Data Model version 1.2,” 2022. Published: Cryptology ePrint Archive, Paper 2022/1724.

Bonus

Performances de SPDM

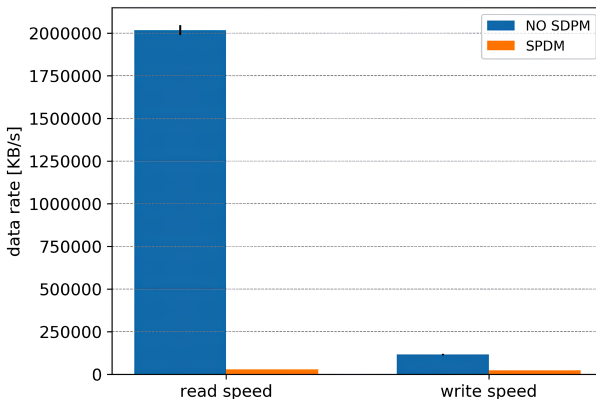


Figure: Débit en lecture et écriture d'un disque dur avec SPDM, mesuré avec *bonnie++*.

Extrait de Renan C. A. Alves, Bruno C. Albertini, and Marcos A. Simplicio Jr. *Benchmarking the Security Protocol and Data Model (SPDM) for component authentication*. [eprint: 2307.06456](#). 2023.

Performances de SPDM

- Augmentation d'un facteur 6.4 du temps d'acquisition d'un nombre aléatoire.
- Réduction de la vitesse d'écriture sur un disque de 68%, et de 99.3% en lecture.
- Lorsque de l'aléatoire est introduit dans les adresses de lecture et d'écriture, la dégradation de performance devient négligeable.

- Utilisation d'informatique mobile (*mobile computing*)
- Utilisation de *tokens* fournis par un serveur
- Utilisation de ses informations d'identification à chaque échange
- Un challenge est l'inter-opérabilité de l'authentification