

# Réunion du 13 février 2024

## Compte-rendu de réunion de TER

**Présents :** Pierre DAVID, Léon GALL.

**Durée :** 11h15 à 11h45.

La réunion du mardi 13 février a porté sur les points suivants :

- Retour sur le travail réalisé ;
- Travail à réaliser.

## I Retour sur le travail réalisé

- Couche sous le système d'exploitation
  - Intel Management Engine ;
  - AMD Platform Security Processor.
- Sur-/sous-tension électrique
  - Circuit intégré de régulation de tension ;
  - Relève davantage de la sécurité physique.
- SPDML
  - Cible de SPDML : pas de précision dans la spécification ou sur internet. Le chiffrement des communications demande une cryptographie rapide, ce qui exclurait les périphériques peu performants ;
  - Clé symétrique pré-partagée : pas de précision sur les parties, mais elles-seules doivent être au courant de la clé ;
  - Stockage des clés ? Hardware Security Module ?
  - Lecture de parties de la spécification de la version 1.3.
- SPDML version 1.3
  - Différentes clés pré-partagées peuvent être utilisées à chaque étape. L'identifiant `PSKHint` permet de savoir laquelle utiliser, ou permet de dériver la clé partagée (évite de devoir stocker  $n$  clés).
  - Certains points corrigent des défauts de la version 1.2, en spécifiant que le compteur ne doit pas être réinitialisé durant toute la durée de vie du périphérique, et en forçant l'utilisation du sel (nonce).
- Lecture de *Securing hard drives with the Security Protocol and Data Model (SPDML)* de Renan C. A. Alves, Bruno C. Albertini, and Marcos A. Simplicio Jr.
  - L'utilisation de SPDML est coûteux pour des fichiers volumineux, du fait du chiffrement/déchiffrement, et du découpage des blocs à transmettre au disque pour qu'ils rentrent dans des paquets SPDML.

## II Travail à réaliser

- Comprendre les interactions entre les programmes sur l'Intel Management Engine et l'OS ;
- Se renseigner sur la cible et l'applicabilité, en essayant de trouver des exemples d'implémentations ;
- Se renseigner sur la possibilité de signer les communications durant la session (phase *application data*) ;
- Continuer la lecture des ressources.

## III Problèmes rencontrés

- Accès à *SpringerLink* via le reverse-proxy de l'Unistra impossible.

## IV Prochaine réunion

La prochaine entrevue aura lieu le mardi 20 février 2024 à 13h30.