

# Réunion du 20 février 2024

## Compte-rendu de réunion de TER

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

**Durée :** 13h30 à 14h.

La réunion du mardi 20 février a porté sur les points suivants :

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

## I Retour sur le travail réalisé

- Possibilité de signer les communications dans la phase *application data*, via des transcripts.
- Recherches sur l'Intel Management Engine (IME).
  - > Lecture d'une présentation d'Igor Skochinsky (Hex-Rays)
  - > Communications avec l'OS via l'*Host Embedded Controller Interface* (HECI)
  - > Tout le code exécuté par l'IME est signé, et vérifié à l'exécution.
  - > Une partie du code de l'IME est compressé via un code de Huffman, avec un dictionnaire inconnu.
  - > *Nighthawk* utilise l'IME pour vérifier l'intégrité du noyau, d'un hyperviseur ou bien du firmware du système.
- De plus, il monitore l'état du système.
- Recherche de documents sur des usages de SPDM (Nvidia, Cisco).
- Recherche de documents sur la sécurité des périphériques.

## II Travail à réaliser

Le sujet étant étroit, et SPDM n'étant que peu documenté, une ouverture du sujet à deux nouvelles pistes a été proposé par l'encadrant :

- En quoi la virtualisation, peut-elle permettre à un système d'exploitation de se défier des périphériques ?
- Comment les périphériques IoT peuvent-ils authentifier leurs communications (i.e. savoir qu'ils communiquent avec le bon appareil) ?

De plus, il faut continuer la lecture des différents documents.

## III Prochaine réunion

La prochaine entrevue aura lieu le vendredi 1<sup>er</sup> mars 2024 à 9h30.