

# Réunion du 13 mars 2024

## Compte-rendu de réunion de TER

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

**Durée :** 15h35 à 16h15.

La réunion du vendredi 13 mars a porté sur les points suivants :

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

## I Retour sur le travail réalisé

### Gestion des PSK

L'étude de la fonction `libspdm_try_send_receive_psk_exchange` de la *libspdm*, m'a conduit à d'autres fonctions, jusqu'à `libspdm_psk_handshake_secret_hkdf_expand`. Dans cette fonction, la PSK est fournie en dur. C'est donc à l'implémentation de SPDm de fournir le mécanisme de lecture des PSK ; les clés étant probablement stockées dans une enclave.

### Processeurs spécialisés en cryptographie

Il y a très peu de données relatives à des petits processeurs utilisés pour de la cryptographie qui pourraient être présents dans des disques durs, ou autres périphériques.

### Lecture de l'article [1] présentant BitVisor, un hyperviseur chargé d'assurer la sécurité des périphériques

Les auteurs sont partis du constat que la virtualisation a un grand TCB. En effet, pour les hyperviseurs de type I, le TCB est constitué des différents drivers nécessaires, en plus des fonctions de management des OS invités. Pour ceux de type II, le TCB contient l'OS hôte ainsi que le code de l'hyperviseur.

Les auteurs proposent donc un hyperviseur de type I, en *parapass-trough* : un seul système d'exploitation peut être exécuté, et celui-ci peut accéder directement au matériel pour certaines instructions (*pass-trough*) telles que par exemple les sorties graphiques ou son, mais d'autres accès I/O sont interceptés par l'hyperviseur. Celui-ci peut alors vérifier que les accès sont légaux, et observer le contenu des échanges. Cet hyperviseur posséderait donc un TCB bien plus petit.

Une figure (fig. 7) et son explication (page 10) restent mystérieuses. Il est expliqué que les accès en lecture jusqu'à 521 ko se font sur le cache du contrôleur, mais qu'au dessus, les lectures sont plus lentes à cause de l'accès au média. Cela serait logique en écriture, mais reste mystérieux en lecture.

En outre, il semble que ces mesures aient plus pour objectif de protéger les périphériques que le système d'exploitation...

## II Travail à réaliser

- Continuer la lecture d'articles relatifs à l'élargissement du sujet ;
- Organiser les idées étudiées jusqu'à présent, et proposer un plan pour le mémoire. Ceci va permettre également d'orienter les lectures à réaliser.

## III Prochaine réunion

La prochaine entrevue aura lieu le vendredi 22 mars 2024 à 9h.

## Références

- [1] Takahiro Shinagawa, Hideki Eiraku, Kouichi Tanimoto, Kazumasa Omote, Shoichi Hasegawa, Takashi Horie, Manabu Hirano, Kenichi Kourai, Yoshihiro Oyama, Eiji Kawai, Kenji Kono, Shigeru Chiba, Yasushi Shinjo, and Kazuhiko Kato. BitVisor : a thin hypervisor for enforcing i/o device security. In *Proceedings of the 2009 ACM*

