

Réunion du 22 mars 2024

Compte-rendu de réunion de TER

Présents : Pierre DAVID, Léon GALL.
Durée : 9h00 à 9h30.

La réunion du vendredi 22 mars a porté sur les points suivants :

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

I Retour sur le travail réalisé

Retour sur l'article [2] présentant BitVisor

Comme expliqué lors de la précédente réunion, BitVisor permet le chiffrement des I/O, ainsi que l'inspection des I/O. Le chiffrement peut permettre la confidentialité des données entre le périphérique et l'hyperviseur, et peut également permettre de chiffrer/déchiffrer des informations sur un disque.

L'article *Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained From Live-forensic Hypervisor* [1], utilise BitVisor ainsi que le Machine Learning afin de détecter l'exécution de ransomwares sur le système invité.

Plan du mémoire

Un plan du mémoire a été proposé, et discuté. Il est disponible sur GitLab (*plan.md*). M. DAVID a rappelé l'importance d'accrocher le lecteur sur le(s) problème(s) à résoudre, en proposant notamment des scénarios concrets pour chacune des menaces.

Il peut être intéressant de rajouter une partie sur comment un système invité peut être sûr qu'il s'exécute sur le bon système, en donnant une réponse avec et sans SPDM.

Pour l'instant, l'aspect authentification en IoT peut être mise de côté, pour rédiger le reste.

II Travail à réaliser

Il faut à présent débiter la rédaction du mémoire. Une première version sera à envoyer à M.DAVID pour le vendredi 5 avril 2024.

III Prochaine réunion

La prochaine entrevue aura lieu le mardi 9 avril 2024 à 13h30.

Références

- [1] Manabu Hirano and Ryotaro Kobayashi. Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained From Live-forensic Hypervisor. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 323–330, 2022.
- [2] 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 SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, VEE '09, pages 121–130, New York, NY, USA, 2009. Association for Computing Machinery. event-place : Washington, DC, USA.