Conception et implémentation d'un langage dédié à l'introspection de machine virtuelle

Lionel Hemmerlé, Guillaume Hiet, Pierre Wilke, Frédéric Tronel, Jean-Christophe Prévotet

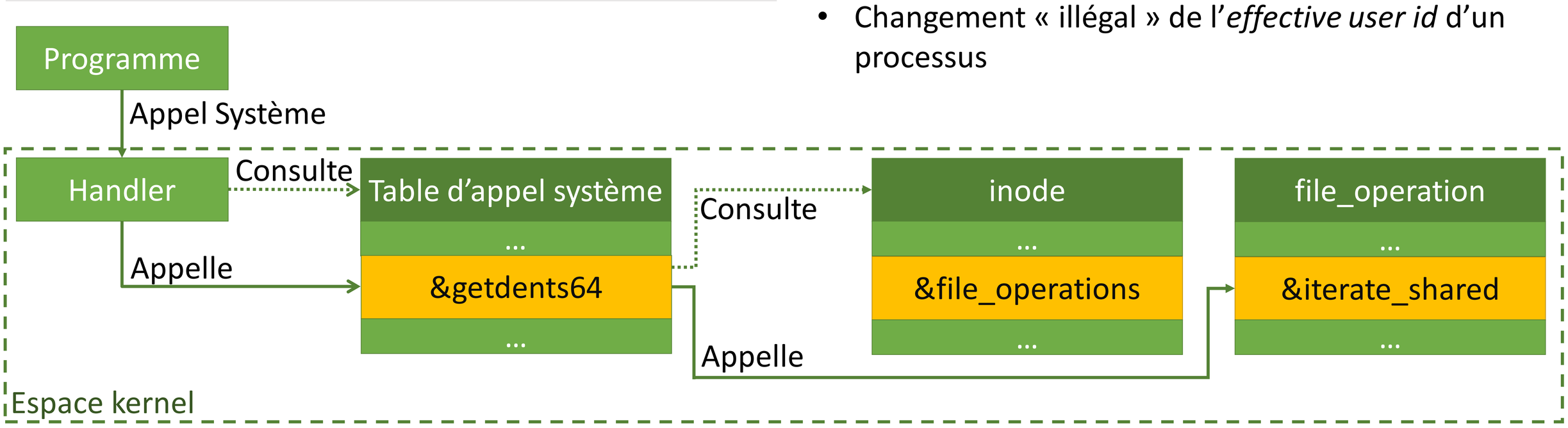
CentraleSupélec — UMR IRISA — Université de Rennes

Contexte

- Comment détecter un rootkit kernel ?
- Pas de confiance aux informations renvoyées par le système d'exploitation

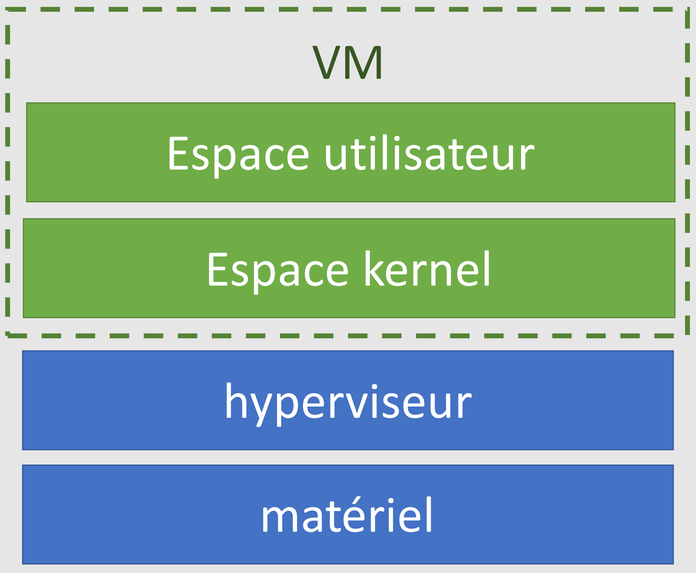
Exemples d'attaques

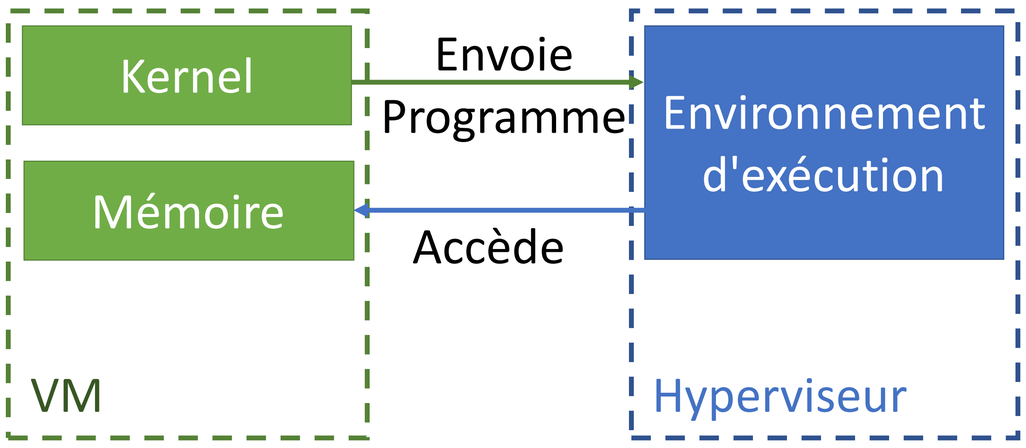
- Modification de la table d'appels systèmes
- Modification du système de fichier virtuel
- Modification des structures *pid* et task_struct
- Changement « illégal » de l'*effective user id* d'un processus



Extension de virtualisation

- Extension présente sur certains processeurs
- Permet d'exécuter le système d'exploitation protégé dans une VM
- un hyperviseur s'interpose entre la VM et le matériel
- L'hyperviseur peut être utilisé pour détecter un rootkit



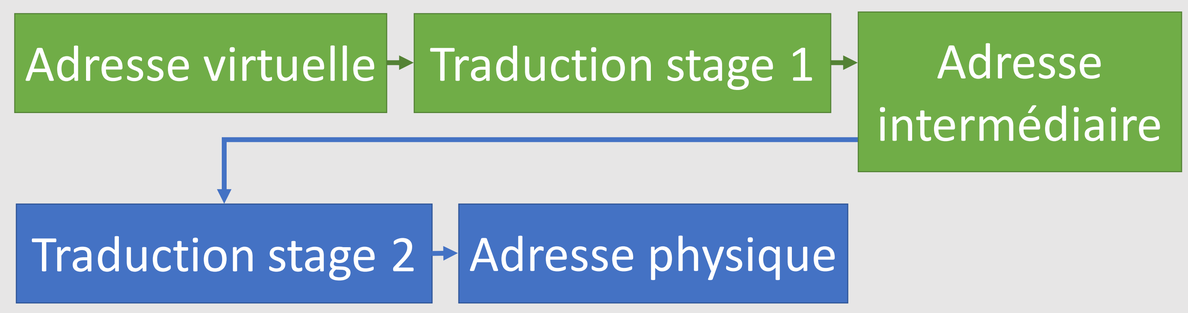


Problème du fossé sémantique

Comment retrouver les informations dans la mémoire de la VM ?

- Comment elles sont stockées ?
- Où elles sont stockées ?
- Quand-est ce qu'elles sont modifiées ?

Exemple de difficulté : traduction d'adresse partiellement contrôlée par la VM



Notre approche

Créer un langage dédié

- La VM envoie à l'hyperviseur des programmes créés dans ce langage
- L'hyperviseur exécute ces programmes
- Ils permettent de lever des alertes si nécessaire

Fonctionnalités du langage :

- Décrit comment réagir à certains événements
- Définit dynamiquement de nouveaux événements à détecter
- Événements détectables :
  - Écritures en mémoire
  - Modifications de certains registres système
  - Exécution d'une instruction à une adresse donnée

Contraintes de sécurité

- Empêcher l'envoi de programmes indésirables
- Se protéger contre la manipulation des inputs
- Interdire les lectures / écritures libres en mémoire
- Détecter les boucles infinies / vampirisation des ressources de l'hyperviseur
- Détecter les déplacement des structures dans la mémoire de la VM

Notre implémentation

- Architecture arm64
- Création de quatre rootkits (modules kernels)
- Modification de Xvisor
  - Détection des écritures en mémoire à des adresses indiquées par la VM
  - Permet de détecter deux des attaques implémentées