Détection de défaillance de gestionnaires de machines virtuelles

Benoît Morgan, Eric Alata

Détection de défaillance de gestionnaires de machines virtuelles

Benoît Morgan — *bmorgan@laas.fr*
Éric Alata — *ealata@laas.fr*
LAAS-CNRS — Université de Toulouse — INSA Toulouse

Secure Virtual Cloud
Projet français
d'Investissements d'avenir

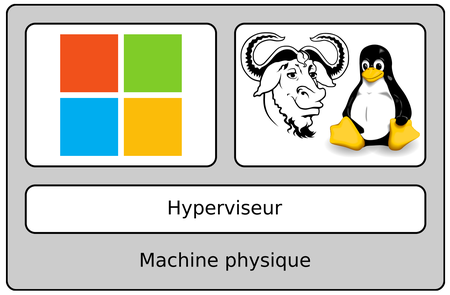
Contexte

Cloud computing

- ✔ Dynamicité
- ✔ Performance
- ✔ Flexibilité
- ⚠ Confidentialité
- ⚠ Intégrité

Virtualisation

- Partage d'une machine physique entre plusieurs machines virtuelles
- Gestionnaire de machines virtuelles : Hyperviseur
  - Segmentation spatiale
  - Segmentation temporelle
- Assistance matérielle pour la virtualisation
  - Performances
  - Sécurité
  - Simplification du développement



Problématique

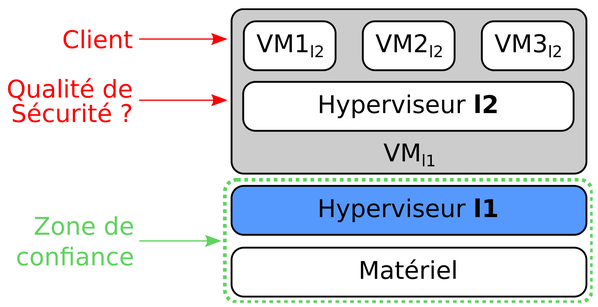
- Machine virtuelle malveillante
  - Peut compromette l'hyperviseur
  - Rupture de l'isolation spaciale et temporelle

→ **Nécessité de détecter et éviter la compromission**

Solution proposée

Insertion d'un hyperviseur entre l'hyperviseur d'origine et le matériel

- Hyperviseur imbriqué **I1**
  - Virtualise l'hyperviseur origine **I2**
  - Petit ⟶ prouvable
- Détection de la compromission de **I2**
  - Contrôle les modifications des registres du processeur
  - Analyse les transitions entre les VM
  - Contrôle les entrées / sorties
  - Contrôle l'espace de configuration PCI



- Caractéristiques de l'hyperviseur **I1**
  - Proche du matériel, *bare-metal*
  - Mise en place de la virtualisation complète
  - Intégration dans le *firmware UEFI*
    - Sous la forme d'un driver *UEFI*
    - Initialisation de VM_{I1} facilitée
  - Mise en place d'un driver *Ethernet* pour le débogage à distance

Plateforme