



Détection de défaillance de gestionnaires de machines virtuelles

Benoît Morgan, Eric Alata

► To cite this version:

Benoît Morgan, Eric Alata. Détection de défaillance de gestionnaires de machines virtuelles. SARSSI 2013 : Sécurité des architectures réseaux et des systèmes d'information, Sep 2013, Mont-de-Marsan, France. , 2013. <hal-01493469>

HAL Id: hal-01493469

<https://hal.science/hal-01493469v1>

Submitted on 3 Apr 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

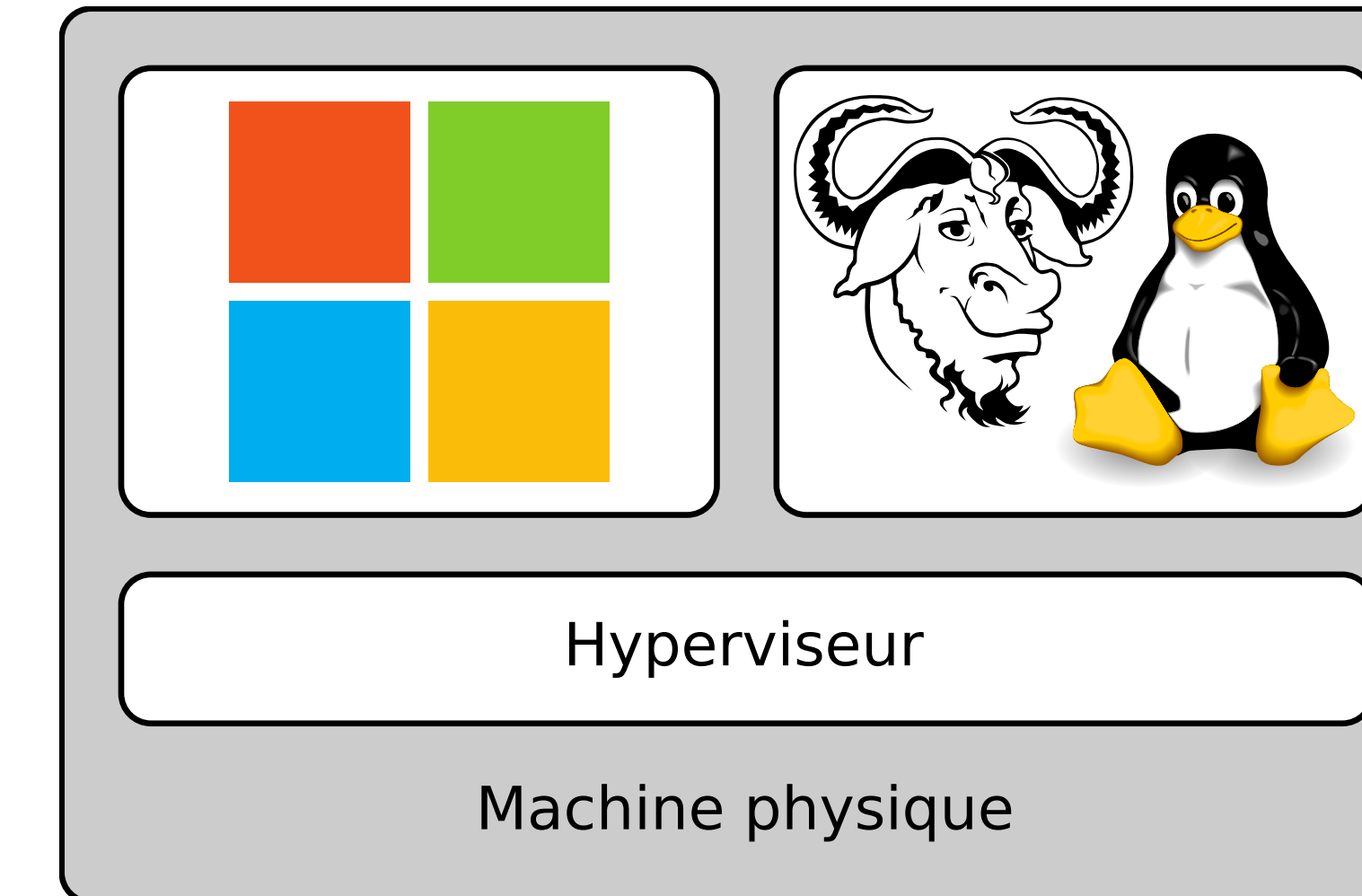
Contexte

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

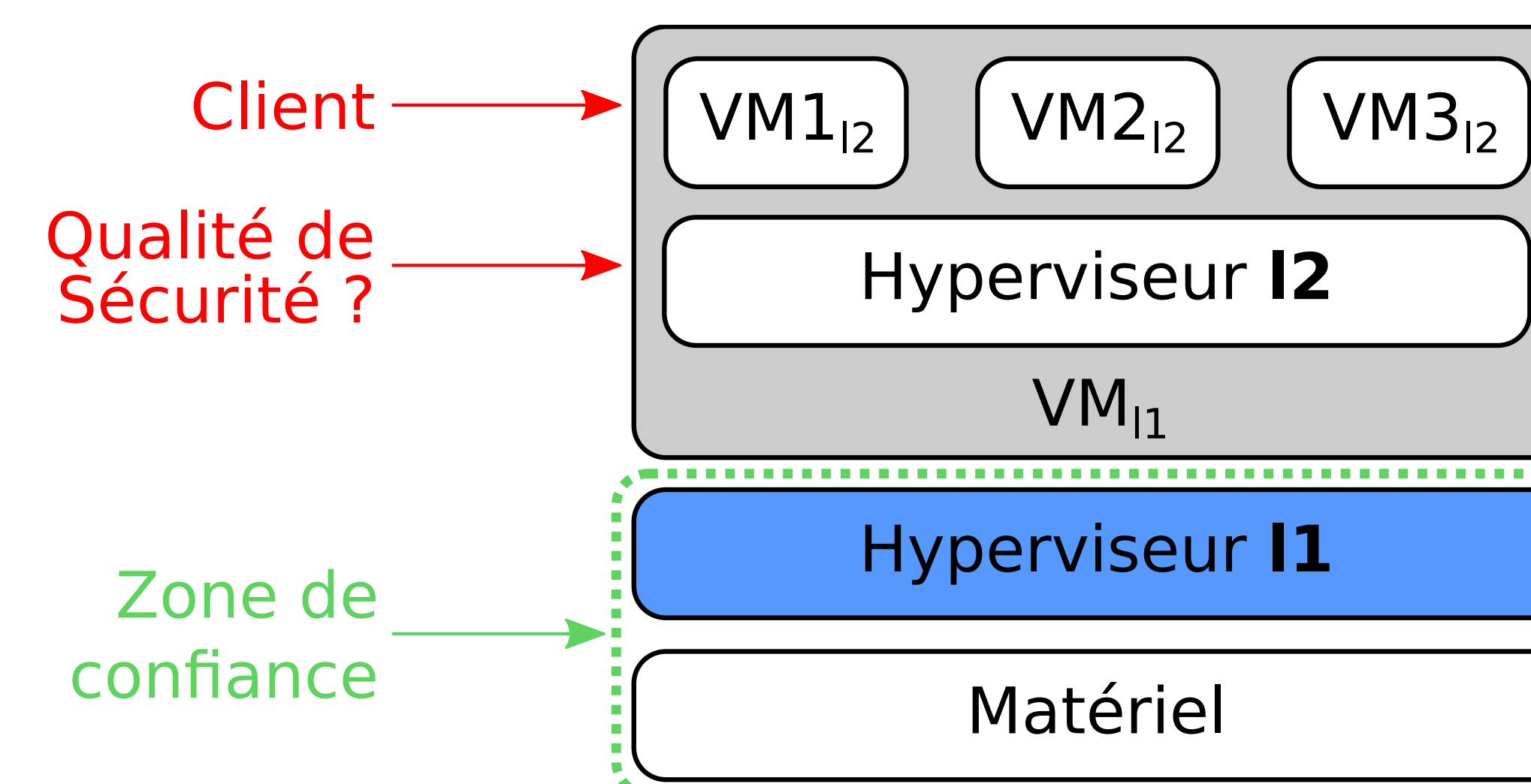
- Machine virtuelle malveillante
 - Peut compromettre l'hyperviseur
 - Rupture de l'isolation spatiale et temporelle

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

Solution proposée

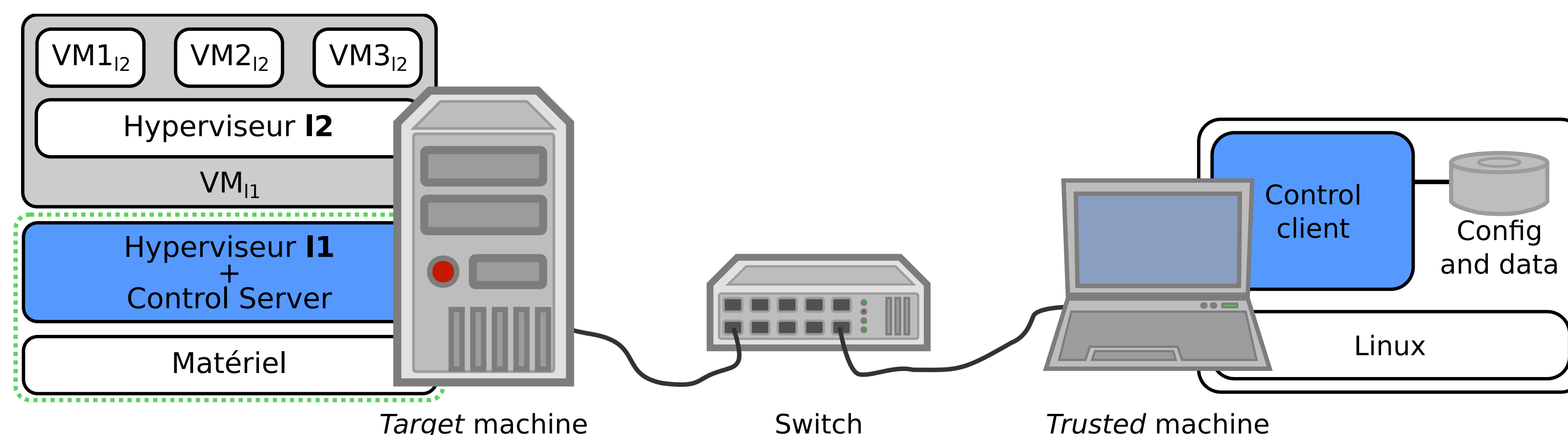
Insertion d'un hyperviseur entre l'hyperviseur d'origine et le matériel

- 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



Chaîne de démarrage UEFI

