Thèse CIFRE

Mécanismes de monitoring sémantique dédiés à la sécurité des infrastructures cloud IaaS

Yacine HEBBAL

Sylvie LANIEPCE

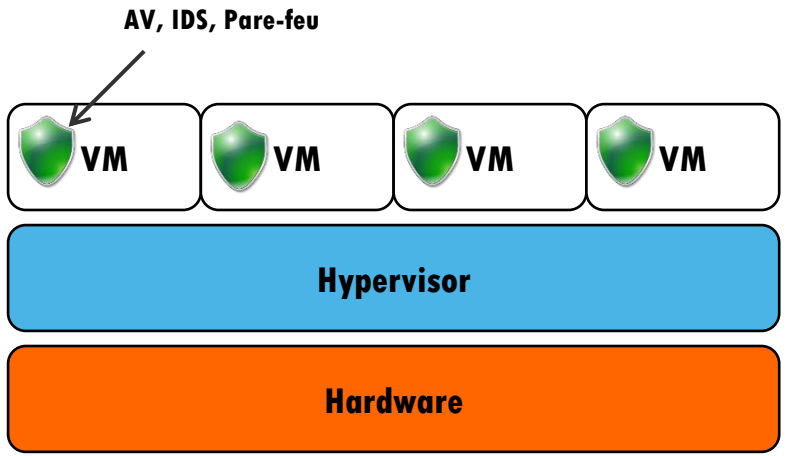
Jean-Marc MENAUD

Début de thèse : octobre 2014 (1ière année)
SEC2 : 30 Juin 2015

Contexte et sujet

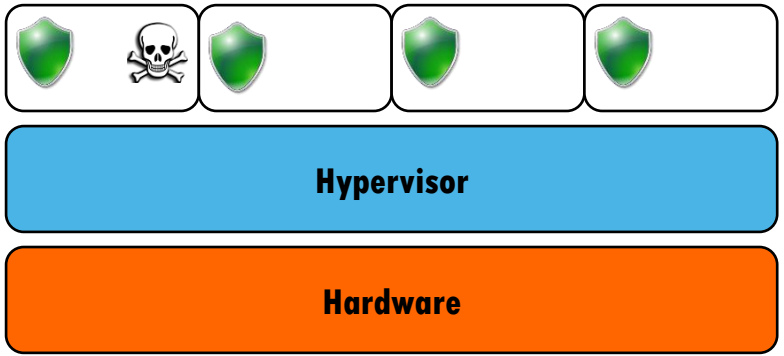
Modèle traditionnel de la sécurité des VMs

- Les VMs sont assimilées à des machines physiques
- Chacune des VMs contient un (des) système(s) de sécurité traditionnel(s) : Antivirus (AV), Intrusion Détection System (IDS), Pare-feu…
- Chaque système de sécurité est dédié à une seule VM
- Il détecte et empêche les attaques …… quand il peut !



Limites du modèle traditionnel de la sécurité des VMs

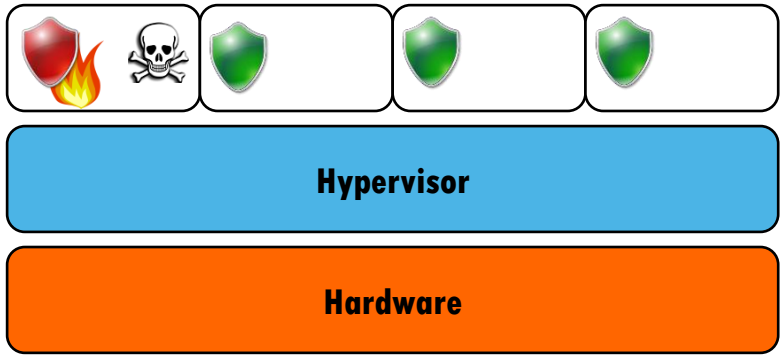
- **Un système de sécurité peut NE PAS détecter une intrusion :**
  - **Exploitation d'une faille non connue**
  - **Exploitation d'un composant non surveillé**
  - **Un malware avec une nouvelle signature**
  - **…**



Limites du modèle traditionnel de la sécurité des VMs

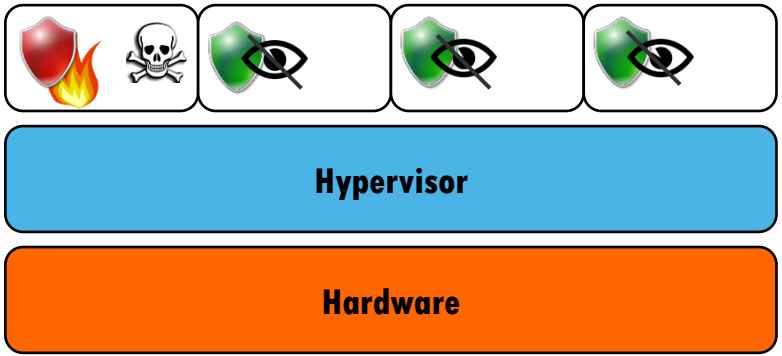
- **L'attaquant obtient généralement les privilèges de root.**

⇨ **Il peut attaquer donc le système de sécurité, le désactiver …**



Limites du modèle traditionnel de la sécurité des VMs

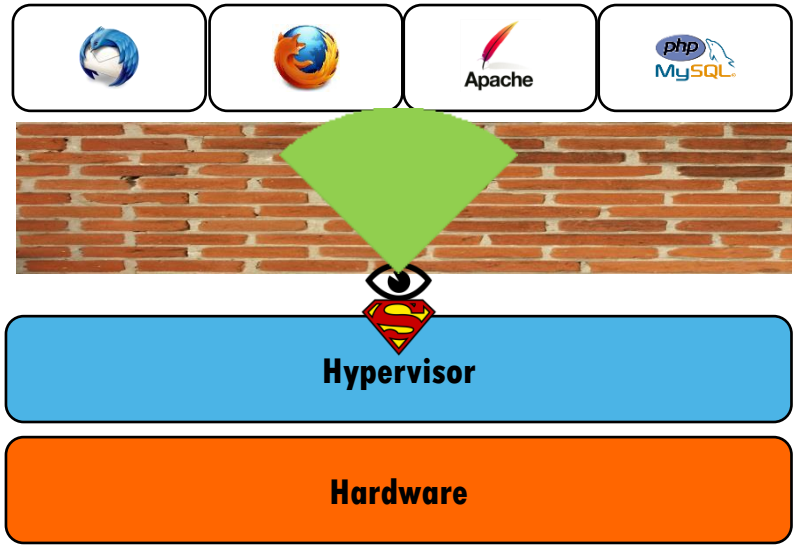
- La VM n'est plus protégée.
- Les systèmes de sécurité des autres VMs ne peuvent pas détecter cette intrusion.



Modèle alternatif de supervision des VMs

- **Monitorer les VMs depuis la couche de virtualisation (hyperviseur)**
  - **Plus de privilèges**
  - **Isolation vis-à-vis des VMs**
  - **Visibilité sur toutes les VMs (cross-VMs)**
  - **Interposition entre les VMs et le hardware.**

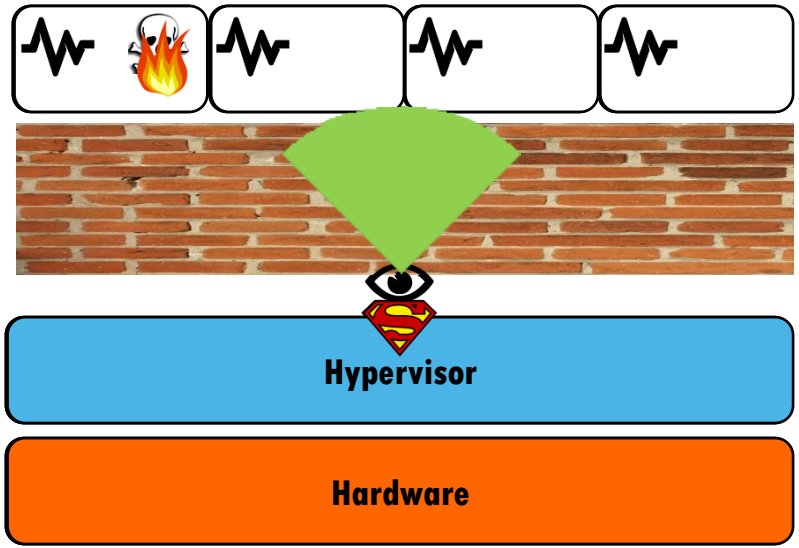
☞ **Virtual Machine Introspection [1]**



[1] Garfinkel Tal and Rosenblum Mendel. "A Virtual Machine Introspection Based Architecture for Intrusion Detection." NDSS. Vol. 3. 2003.

Virtual Machine Introspection (VMI)

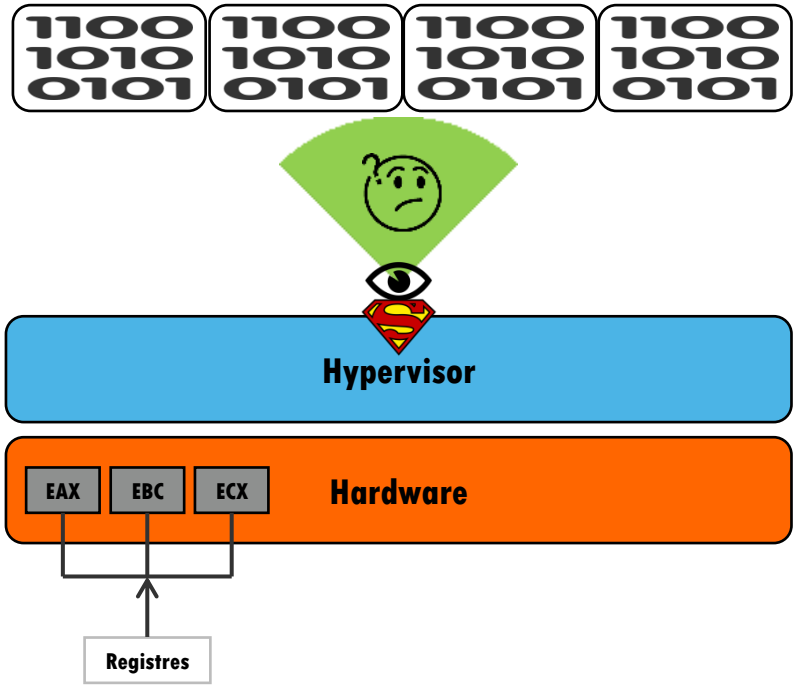
- **Détection**
- **Réaction**
- **Universalité: transparence et portabilité**



Challenge technique : Gap sémantique

- **L'hyperviseur ne voit des VMs que :**
  - **Bits et octets (mémoire)**
  - **Registres et évènements hardware**

☞ **PAS de sémantique, PAS d'abstraction de haut niveau [2] (processus, fichiers, sockets, appels système…)**



[2] Chen, Peter M., and Brian D. Noble. "When virtual is better than real." Hot Topics in Operating Systems, 2001. Proceedings of the Eighth Workshop on. IEEE, 2001.

Objectifs scientifiques de la thèse

Objectifs et verrous à lever

1. **Franchir le gap sémantique depuis l'hyperviseur pour reconstruire une abstraction haut niveau des processus, fichiers, appels systèmes…**

2. **Exploiter au niveau hyperviseur ces informations sémantiques, à des fins de supervision de la sécurité des VMs**

- **Principaux verrous à lever [3] : proposer des techniques d'introspection applicables au IaaS**

  1. **Automatiques: acquièrent et exploitent les informations sémantiques de manière automatique**

  2. **Scalables: monitorent un grand nombre de VMs simultanément**

  3. **Universelles: supportent des OS différents**

[3] Hebbal, Y., Sylvie, L., & Menaud, J. M. Virtual Machine Introspection: Techniques and Applications. In Workshop on Security and Privacy in Cloud-based Applications, International Conference on Availability, Reliability and Security (ARES). August 2015.

Perspectives de valorisation industrielle

IaaS dotée de capacité de services

- **Security-as-a-Service:**
  - **Meilleure sécurité : isolation, niveau de privilège, interposition**
  - **Visibilité cross-VM**
  - **Mutualisation (coût)**

- **Instrumentalisation de la couche de virtualisation:**
  - **Sécurité (IDS, IPS, analyse de malware, forensics, …)**
  - **Management et configuration de VMs (shell out-of-VM, hot-hardening, …)**
  - **Optimisation de l'allocation des ressources physiques (ordonnancement temps réel, …)**
  - **…**

Merci !