Sécurité & Virtualisation

Istace Emmanuel

La virtualisation
en deux mots...

et 5 slides...

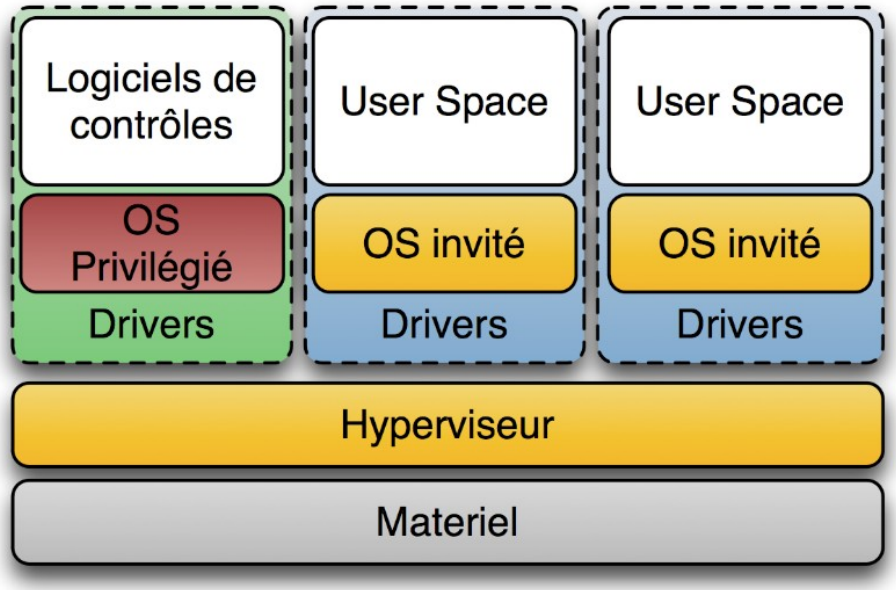
La virtualisation en deux mots...

- La virtualisation consiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts.
  Pour ce faire nous avons à notre disposition :
  - Hyperviseur de type 1 et 2
  - Isolateurs
  - User-space Kernel
  - Hardware Virtualisation

La virtualisation en deux mots...

- Un hyperviseur de type 2 est un logiciel qui tourne sur l'OS hôte. Ce logiciel permet de lancer un ou plusieurs OS invités. La machine virtualise et/ou émule le matériel pour les OS invités, ces derniers croient dialoguer directement avec ledit matériel.
- Un hyperviseur de type 1 est comme un kernel très léger et optimisé pour gérer les accès des noyaux d'OS invités à l'architecture matérielle sous-jacente. Si les OS invités fonctionnent en ayant conscience d'être virtualisés et sont optimisés pour, on parle alors de para-virtualisation

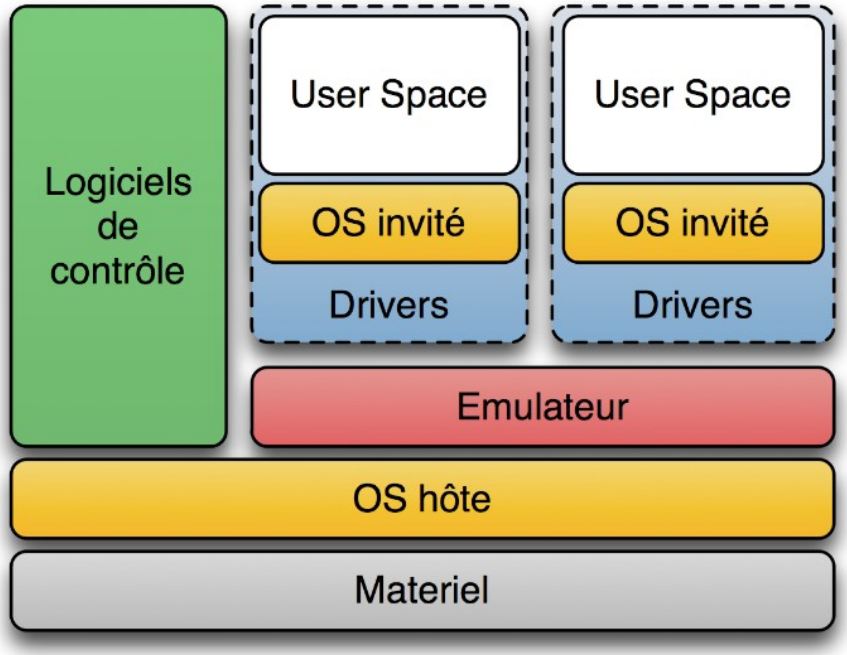
La virtualisation en deux mots...



Hyperviseur Type 1

« Para Virtualisation »

(VMWare ESX, Microsoft HyperV, Xen, ...)



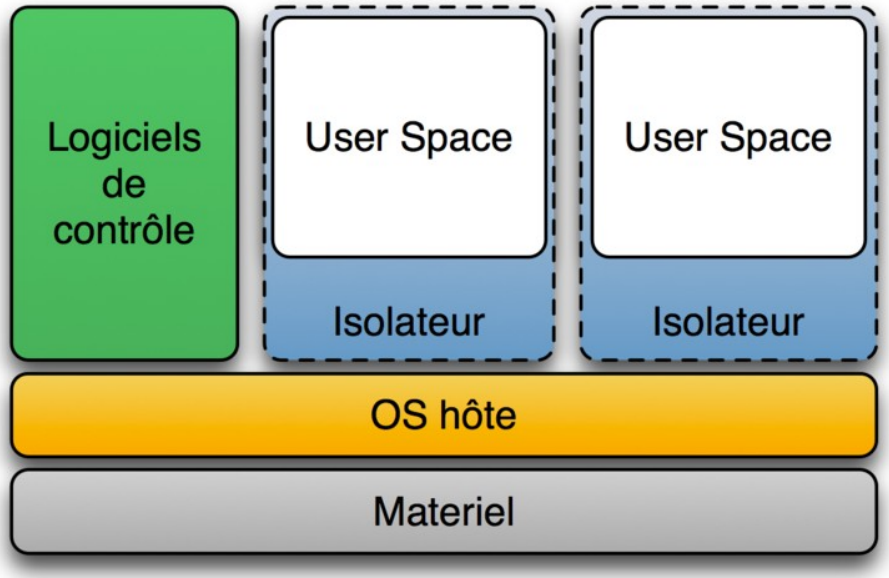
Hyperviseur Type 2

« Full Virtualisation »

(Qemu, VMWare Worksation, VirtualBox, VirtualPC, ...)

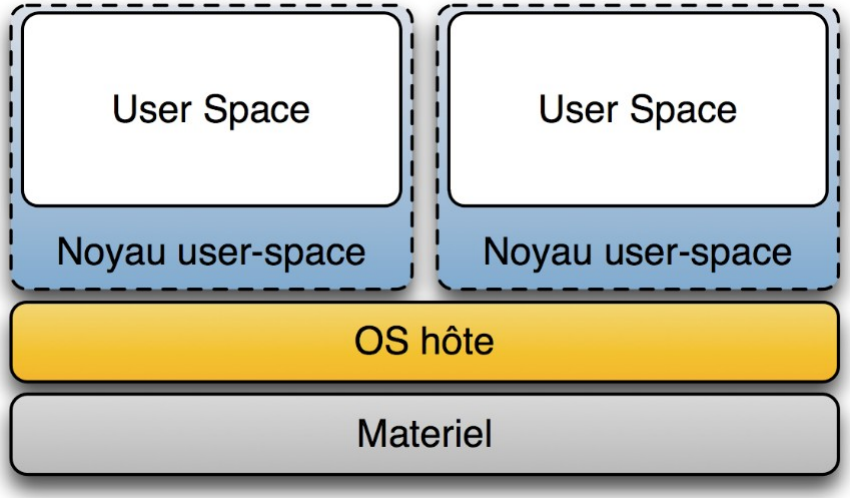
La virtualisation en deux mots...

- Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans ce que l'on appelle des contextes ou bien zones d'exécution.
  - Exemple : Chroot, OpenVZ, BSDJail, …



La virtualisation en deux mots...

- Un Kernel en espace utilisateur (user-space) tourne comme une application dans l'espace utilisateur de l'OS hôte. Le noyau user-space a donc son propre espace utilisateur dans lequel il contrôle ses applications.
  - Exemple : Adeos, coLinux, ...



Hyperviseurs (Type 1)
Quels sont les risques ?

Hyperviseurs - Quels sont les risques ?

- Sur l' hyperviseur :
  - DOS/DDOS
    - Si le/les serveurs qui contiennent l'hyperviseur tombent, tous les services hostés sont inaccessibles Dans le cas d'un cluster, le DOS d'une machine se converti en DDOS grâce aux réplications.
  - Bypass isolation des VM's
    - Une faille dans l'hyperviseur peut permettre à une personne étant dans une Vm X de bypasser l'isolation et de prendre le contrôle d'une Vm Y.

Hyperviseurs - Quels sont les risques ?

- Sur l' hyperviseur
  - Analyse de la mémoire
    - Tous les systèmes tournent sur le même hardware, l'analyse de la mémoire depuis l'hyperviseur permettrait d'obtenir des informations sur toutes les VM en exécution. Lors de la mise en veille d'une VM, un snapshot est pris, ce dernier peut être aussi exploitable. Il en est de même pour les snapshots fonctionnels.

Hyperviseurs - Quels sont les risques ?

- Dans un cluster
  - Corruption de données
    - La corruption d'un système ou de données dans le cas d'un cluster reste tout a fait possible. Contrairement à ce qui est dit, la virtualisation n'est pas plus sécuritaire à ce niveau qu'une architecture 1 service / 1 machine.
  - MITM
    - Un MITM dans un cluster virtualisé permet d'obtenir le trafic (de réplication le plus souvent) de tout les systèmes hostés

Hyperviseurs - Quels sont les risques ?

- Storage
  - Corruption du système
    - Les VM et leurs data sont le plus souvent hostés sur des SAN. Si un accès à ces SAN est possible, alors, modifier l'entièreté du système est possible très facilement ainsi que la possibilité de voler l'entièreté du système et le « rejouer » hors ligne pour l'analyser.

Hyperviseurs - Quels sont les risques ?

- Storage
  - La mine d'or
    - La virtualisation pousse à stocker sur un SAN de plus en plus de data. Ce qui avant, était stocké sur un serveur isolé du réseau, est maintenant stocké sur une VM isolée du réseau se trouvant « physiquement » sur un SAN avec d'autres systèmes.

Virtualisation d'applications & desktop

Quels sont les risques ?

Virtualisation d'applications & desktop
Quels sont les risques ?

- « On The Stream »
  - MITM
    - Un MITM entre le client et le serveur permet de récupérer l'entièreté des applications, de l'Os et des données. De plus, un spoofing permet de propager ses propres applications.
  - Corruptions de données
    - La modification d'applications ou OS sur le serveur modifie l'entièreté de l'infrastructure ayant accès à ces services.

Virtualisation d'applications & desktop
Quels sont les risques ?

- Hôte
  - DoS/DDoS Massif
    - Un DoS sur un serveur de ce type se transforme vite en DDoS car on paralyse l'entièreté de l'infrastructure.

Virtualisation d'applications & desktop
Quels sont les risques ?

- Client
  - Propagation de virus, trojans, etc,...
    - En spoofant un serveur d'application ou d'OS on peut aisément propager ses propres logiciels à tous les clients de l'infrastructure. Par exemple, distribuer un environnement très proche de l'original mais où l'antivirus été modifié et où un malware a été injecté, pour créer une armée de bots locale dans le but d'attaquer un serveur de l'entreprise.

Conclusion

Conclusion

La virtualisation apporte en terme de sécurité de nouveaux challenges auxquels beaucoup de réponses ont été apportées mais peu sont appliquées en entreprise. La virtualisation est également un acteur dans la réponse à ces nouveaux enjeux sécuritaires en apportant des facilitées qu'aucun autre type d'architecture n'est capable d'offrir. Il faut aborder la virtualisation dans le cadre d'une refonte complète de l'architecture, une architecture classique qui implémente des solutions virtualisées est vouée à l'échec.

Bibliographie

Citrix XenApp 5

Sylvain Gaumé – ENI Edition

Mastering VmWare Infrastructure 3

Chris McCain – Sybex

Mastering VmWare Vsphere 4

Scott Lowe – Sybex

The Definitive Guide To Xen Hypervisor

David Chisnall – Prentice Hall

Windows Server 2008 Hyper-V Resource Kit

Robert Larson – Microsoft Press

The Myths of Security: What the Computer Security Industry Doesn't Want You to Know

John Viega – O'Reilly

Virtualization for Security

John Hoopes -Syngress

Wikipedia.org

Des questions ?

Sécurité & Virtualisation

Istace Emmanuel

Merci de votre attention

Contact :

istace.emmanuel@hotmail.com

http://istacee.wordpress.com

Remerciements :

Gioia, Skorm, DCN, HackBBS et

toute sa communauté, la Nuit du Hack

HZH et l'organisation, templatewise.com