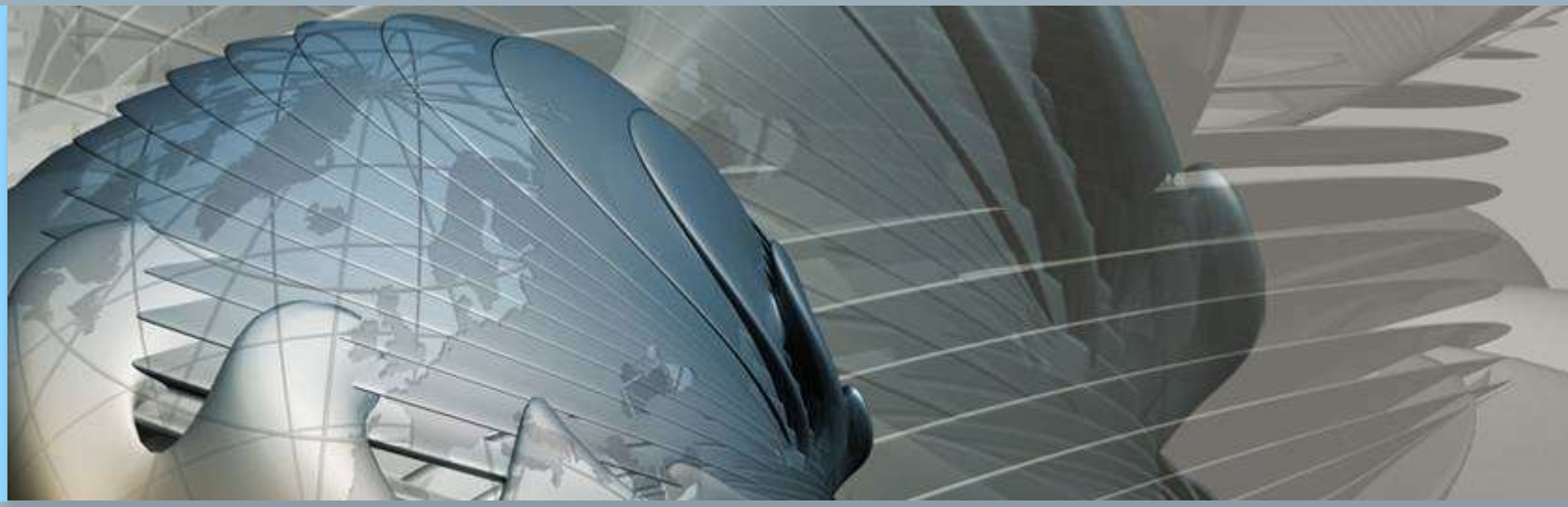
EADS INNOVATION WORKS

Virtualisation ~~et~~ ou Sécurité



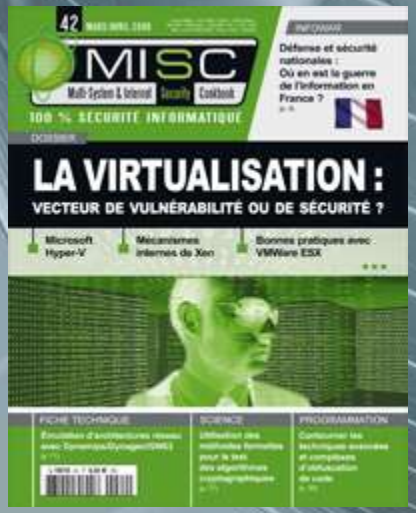
Nicolas RUFF / nicolas.ruff (à) eads.net

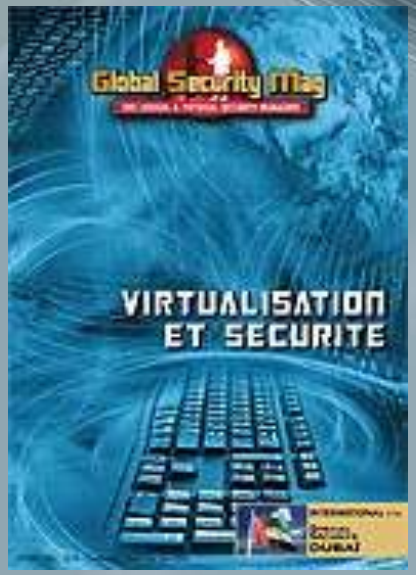
Introduction

- Virtualisation:
  - De nombreux projets en production

- Virtualisation et sécurité
  - Un sujet très débattu
  - Mais jamais tranché

  - Ou peut-être que le thermomètre a été cassé ?





Plan

- Introduction
- Définition des virtualisations
- Principes de fonctionnement (simplifiés)
- Risques pour la sécurité
- Conclusion

Définition

- Comment définir la virtualisation ?
  - *"En informatique, on appelle virtualisation l'ensemble des techniques **matérielles et/ou logicielles** qui permettent de faire fonctionner sur une seule machine **plusieurs systèmes d'exploitation** et/ou **plusieurs applications**, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes."*
  - Source: Wikipedia
    - http://fr.wikipedia.org/wiki/Virtualisation

Applicatif/Spécialisé

- Ne fonctionne que pour une application donnée, analysée en laboratoire
- Repose en général des points de contrôle précis à l'intérieur de l'application
- Ex. "bac à sable" pour Internet Explorer

Applicatif/Générique

- Fonctionne pour toute application en mode utilisateur
- Repose en général sur une interception des appels système
- Ex. Microsoft App-V, fonction native de Vista, …

Système/Spécialisé

- "Para" virtualisation
- Nécessite une adaptation de l'invité
- Ex. Xen

Système/Générique

- "Full" virtualisation
- Pas de modification de l'invité nécessaire
- Ex. VMWare, Hyper-V, Virtual PC/Virtual Server … mais aussi Xen, Bochs, KVM, VirtualBox, …

Définition

- A signaler aussi dans le panorama actuel (*liste non exhaustive*)
  - Google Native Client (NaCl)
    - Nécessite une recompilation des applications
    - Exécution de code vérifiable dans un "bac à sable"
    - Même principe qu'une machine Java ou .NET … mais pour du code x86
  - Mode x86 virtuel
    - Les processeurs x86 savent émuler des tâches en mode 8086 depuis toujours
  - Isolation "en espace utilisateur"
    - Ex. V-Server, OpenVZ, …
  - Virtualisation sur architectures non x86/x64
    - Ex. Produit Trango de virtualisation sur processeur ARM (racheté par VMWare)

Définition

- Etude Forrester 2009
  - (Non disponible publiquement mais reprise dans LMI)
  - 124 entreprises interrogées
    - 78% ont des serveurs de production virtualisés
    - 20% ont uniquement des serveurs de développement virtualisés
  - Parts de marché
    - VMWare: 98%
    - Microsoft: 17%
    - Citrix/Xen: 10%
- Conséquences pour la suite de cette présentation
  - Seul la virtualisation "système/générique" sera traitée
  - Exemples donnés principalement en environnement VMWare

Fonctionnement

- Principe de base (vu de la lune)
  - L'invité fonctionne à un niveau de privilège inférieur à celui qu'il imagine
    - Remarque: tous les processeurs modernes supportent au moins 2 niveaux de protection (*user/supervisor*)
  - Le moniteur de machine virtuelle (VMM) traite les erreurs que cela peut occasionner
- Pas facile à mettre en œuvre
  - Emulation complète de certaines fonctions CPU par le VMM
    - Ex. gestion et protection mémoire
  - Architecture x86: quelques instructions non virtualisables
    - Ex. LSL, SIDT, …
    - L'architecture x86 ne respecte pas les principes de Popek and Goldberg ☺

Fonctionnement

- Il y a très peu de "full virtualisation"
  - Les performances seraient inacceptables !
- Coopération de l'invité souhaitée
  - Echange à travers des *hypercalls*
  - Principe des VMWare Tools, Hyper-V Integration Components, etc.
- Si le système invité ne coopère pas
  - Différentes techniques pour accélérer la virtualisation
    - Ex. "remplacer" le code privilégié dans l'invité

Humain	• Conception • Administration • Sauvegarde et gestion des pannes
Système invité	• Para-virtualisation et/ou traduction à la volée • "Virtual Machine Interface" (ex. VMWare Tools) • Accélérations & optimisations diverses
Système hôte (ou administrateur)	• VMWare ESX: service console à base Linux • Hyper-V: partition parent • Xen: Dom0
Hyperviseur	• Matériel (support processeur et/ou chipset) • Logiciel (bogues)
Matériel	• CPU • Périphériques

Risques (humain)

- Le passage à des solutions virtualisées change la donne
  - (In)efficacité des outils de supervision "classiques"
  - Existence de "super-administrateurs" (système + réseau)
  - Peu d'expérience des outils de virtualisation
  - Procédures à revoir (dépannage, sauvegarde, etc.)
  - Point(s) de panne
    - En général le stockage
    - Voir aussi le bogue du système de licences VMWare (12 août 2008)
  - Etc.
- Cette partie est en général bien traitée par ailleurs
  - Nombreuses documentations et retours d'expérience disponibles dans la littérature
    - Cf. bibliographie

Risques (invité)

- Risques SSI "classiques"
  - Intrusion, rebond, etc.
  - Attention à la robustesse du réseau virtuel
    - *ARP Spoofing*, mode *promiscuous*, etc.
- Risque marginal: élévation de privilèges dans l'invité
  - Scénario utilisateur ➔ administrateur ou noyau
  - Ex. faille dans les composants d'intégration

Risques (invité)

- Nouveau risque: évasion de l'invité
  - Vers un autre invité, l'hôte, ou l'hyperviseur
  - Risque démontré
    - Cf. travaux de Joanna Rutkowska sur Xen
    - Cf. avis de sécurité VMWare
  - Risque difficile à maitriser
    - Complexité technique des attaques
      - A noter: peu de "preuves de concept" publiques malgré toutes les failles corrigées
    - Absence de maitrise sur les produits
      - La seule "protection" consiste en général à désactiver des options de performance
      - Nombreuses options *non documentées*

Risques (invité)

- Nouveau risque: déni de service sur les autres invités
  - Méthodes
    - Surconsommation de ressources
    - *Crash* de l'hôte ou de l'hyperviseur
  - Risque démontré
    - Cf. travaux de Tavis Ormandy
  - Risque également difficile à maitriser
    - Surtout le deuxième …

Risques (invité)

- Remarque
  - L'invité peut être victime de toutes sortes d'attaques si l'hôte ou l'hyperviseur est compromis
  - (Cela semble évident mais des conférences ont quand même été faites sur le sujet)

Risques (hôte)

- La clé de voûte de tout le système
  - Les puristes séparent l'hyperviseur de l'hôte
    - Concepts de *Thin Hypervisor*, *Bare-Metal Hypervisor*, etc.
  - Mais en pratique, la compromission de l'hôte est équivalente à la compromission de l'hyperviseur (et réciproquement)
- En général un système d'exploitation classique
  - Windows ou Linux

Risques (hôte)

- Ce qui pose de multiples problèmes
  - Durcissement
  - Gestion des droits d'accès
  - Application des correctifs
  - Etc.

- Le fond du problème
  - Les logiciels utilisés ne sont pas adaptés aux contraintes de disponibilité exigées
  - Exemples
    - Avis VMSA-2009-0003: faille dans "ed" affectant VMWare ESX 2.5.5
    - Presque tous les systèmes ont souffert du bogue WxH > 2^32

Risques (hyperviseur)

- Logiciel (approche VMWare)
  - Avantages
    - Plus rapide
    - Indépendant du matériel
  - Inconvénients
    - Plus complexe à écrire
      - Risque de bogue (avéré, cf. avis de sécurité existants)
    - Certains cas sont lourds à gérer
      - Ex. problème des instructions non virtualisables

Risques (hyperviseur)

- Matériel (approche Hyper-V)
  - Avantages
    - Plus simple à écrire
    - Fonctionnellement plus riche
  - Inconvénients
    - Lent, dépendant du matériel, et surtout …
    - Encore très mal défini dans les architectures x86 !
      - Spécificités AMD vs. Intel
      - Déjà 3 révisions des spécifications
        - » Rev2 introduit NPT / EPT
        - » Rev3 introduit Directed-IO / IOMMU
      - Le processeur Cell est bien meilleur de ce point de vue ☺

Risques (matériel)

- Périphériques
  - Le matériel peut contourner les sécurités logicielles (ex. DMA)
    - Cf. travaux de Loïc Duflot
  - Matériel bogué
    - Cf. bogue du chipset Q35 découvert par Joanna Rutkowska

- CPU
  - Les bogues CPU, mythe ou réalité ?
    - Théo de Raadt pense que certains bogues sont exploitables
    - Kris Kaspersky également (mais aucune démo)
  - Seule parade: la mise à jour du microcode …

- Remarque: le "fameux" mode SMM
  - Utilisé par Joanna Rutkowska pour contourner la technologie Intel/TXT

Virtualisation et sécurité

- La virtualisation peut aussi servir la sécurité
  - Fiabilité
    - Duplication
    - Transfert à chaud
    - Retour en arrière possible après application des correctifs
  - Forensics des invités (mais pas de l'hôte)
    - Capture mémoire & disque "parfaite"
    - Environnement d'analyse fiable (si l'hôte n'est pas compromis)
  - Malwares
    - Refusent de s'exécuter dans les environnements virtuels ☺

- Les problèmes de sécurité sont pris en compte par les éditeurs
  - Ex. sécurité des réseaux virtuels dans VMWare ESX
  - Seuls vont persister les bogues logiciels …

Conclusion

- La virtualisation de systèmes
  - Une architecture n'est jamais *plus sûre* après avoir été virtualisée
- Il est possible de limiter la casse
  - Mais l'impact d'un bogue logiciel est (et restera) souvent catastrophique
- Une architecture virtualisée ne se gère pas comme une architecture physique

Conclusion

- Le futur (ou pas)
  - Plus de fonctionnalités == plus de failles
    - VMSafe : qui veut vraiment mettre un antivirus dans son hyperviseur ?
  - La virtualisation comme moyen d'attaque
    - Mebroot + Blue Pill = catastrophe ?

Conclusion

- Qui a parlé en premier de "ring -1" ?
  - Le projet Palladium/NGSCB …
  - Avec Intel/TXT et AMD/SVM toutes les technologies sont en place
  - La preuve ?
    - Spécifications TPM disponible sous NDA uniquement
    - Mots de passe dans les processeurs (SVM_LOCK)

```
/*
Write the new EDX:EAX value into CPUID override MSR.
Second-Generation AMD Opteron™ Processors require a
32 bit password in EDI. Contact AMD to get the password.
*/

        MOV EDI, <PASSWORD>

        MOV CX, 0xC0011005h
        RDMSR
```

```
rdmsr_with_pwd proc near
push    edi
mov     edi, 9C5A203Ah
rdmsr
pop     edi
retn
rdmsr_with_pwd endp
```

Bibliographie

- Tavis Ormandy
  - An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments
    - http://taviso.decsystem.org/virtsec.pdf
- Oded Horovitz
  - Virtually Secure
    - http://cansecwest.com/csw08/csw08-horovitz.ppt
- DoD
  - ESX Server Security Technical Implementation Guide
    - http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf
- Etude Forrester
    - http://www.lemondeinformatique.fr/actualites/lire-le-stockage-au-coeur-des-problemes-de-la-virtualisation-selon-forrester-28191.html

Bibliographie

- HSC / OSSIR
  - "VMWare et sécurité"
    - http://www.ossir.org/sur/supports/2008/OSSIR_VMware_20080807.pdf
- HSC / CLUSIF
  - "Sécurité et Virtualisation"
    - http://www.hsc.fr/ressources/presentations/clusif-virtualisation/index.html.fr
- MISC Magazine n°42
  - "La virtualisation, vecteur de vulnérabilité ou de sécurité ?"
    - http://www.miscmag.com/index.php/2009/03/06/misc-n%C2%B042-la-virtualisation-vecteur-de-vulnerabilite-ou-de-securite-marsavril-2009-chez-votre-marchand-de-journaux