État de l'art des hyperviseurs de confiance

Geoffrey Plouviez

Agence Nationale de la Sécurité des systèmes d'Information

La virtualisation

- Qu'est ce qu'un hyperviseur?
  - Comme un système d'exploitation en plus petit
- Quels avantages pour la confiance ?
  - Réduire la surface d'attaque
    - Exemple de la pile TCP/IP et du disque dur
      - L'attaque est confinée à l'invité compromis
- Quels risques pour la confiance ?
  - Déport des fonctionnalités d'isolation
    - Mise à 0 de la mémoire et des disques

Les catégories

- Orienté prévention d'intrusions
- Orienté détection d'intrusions
- Orienté confinement d'intrusions

Orienté prévention d'intrusions

La famille L4

- Le micro-noyau L4
  - IPC
  - Threads
  - Espaces d'adressage
  - Dépend de services au niveau utilisateur
    - Allocateur mémoire, pilotes, etc.
  - Les interruptions sont transformées en IPC
- Les familles Karlsruhe/UNSW et Dresde
  - Quelles différences ?

SeL4 (UNSW)

- Vérification de la conformité du code C à une spécification formelle
  - 8 700 lignes
  - Bon alignement mémoire, listes chaînées non circulaires et terminées par 0, etc.
- La virtualisation au dessus de SeL4
  - Portage d'un Linux
  - Le noyau Linux invité est l'allocateur mémoire de la machine
  - Les interruptions sont transférées par IPC vers le noyau Linux qui contient tous les pilotes

SeL4 (UNSW) suite

- La vérification accomplie est un travail impressionnant
  - Classification en prévention d'intrusion
- Cependant SeL4 n'est qu'une couche d'abstraction du matériel
  - Que des mécanismes, pas de politique
- La somme des failles de la plateforme est le nombre de failles SeL4 ajoutée au nombre de failles du noyau Linux

Nizza (Dresde)

- Système d'exploitation bâti sur l'implémentation L4 de Dresde
  - Réduire la surface d'attaques
  - Chiffrement et code de détection d'erreurs pour utiliser des systèmes de fichiers, des piles TCP/IP qui ne sont pas de confiance
    - Décentraliser au maximum
    - Seule l'attaque en disponibilité est possible
    - Une attaque en intégrité n'est pas immédiatement détectée
- Support d'un Linux virtualisé pour la rétro-compatibilité

Qubes

- Approche comparable à Nizza mais bâti sur l'hyperviseur Xen
  - Surface d'attaque plus élevée
    - Le noyau Linux « domain 0 »
      - Accès à tout le matériel
  - Initialement pour la performance

VaxVMM

- Réduction des canaux cachés
  - Au niveau de l'ordonnanceur
  - Mouvement du bras du disque dur
- Vérification de la conformité de la spécification formelle à la politique de sécurité
  - 30% de la vérification achevée
  - Le but n'était pas de descendre au code C

Hyper-V

- Gestionnaire de machines virtuelles pour architecture multi-coeurs de Microsoft
  - 100 000 lignes de C et 5 000 lignes d'assembleur
  - Orienté performance
  - Vérification de l’absence de débordements d'entiers et de tableaux grâce à VCC
  - Garantie de la bonne utilisation des CPU 64 bits d'intel par la modélisation de ce dernier

Tsar Hypervisor

- Gestionnaire de machines virtuelles pour architecture Many-cores
  - Les cœurs sont dédiés
  - Isolation mémoire par des mécanismes matériels
- L'hyperviseur isolé sur un cœur et vérifié avec la MéthodeB
  - Initialisation des mécanismes matériels et virtualisation des I/O
  - Absence de débordements d'entiers et de tableaux
  - Absence de débordements de buffer DMA ou de disques vituels, etc.

Orienté détection d'intrusions

Secvisor

- Valider les pages de code du seul noyau invité par une somme de contrôle
  - Ensuite les pages sont en lecture seule
- Besoin de porter le système d'exploitation à virtualiser
  - Décompression du noyau, chargement des modules noyaux et du script de lien
  - Ajout d'hypercall
- Virtualisation de la MMU pour protéger Secvisor

Analyse de sécurité de Secvisor

- Model checking à l'aide de murphi
  - Simplification de l'architecture
    - 3 pages mémoire
  - 2 failles découvertes
    - Page utilisateur en R/W pointant sur du code noyau

Conclusion sur Secvisor

- Augmente la confiance dans l'authenticité du code exécuté
- Ne protège pas contre les attaques portant sur le flux d'exécution qui représentent 70% des menaces d'après le CERT

Xom

- Modification d'un mips R10000
  - Nécessite un portage du noyau
  - Ce n'est pas un hyperviseur
- Les processus et le noyau sont enfermés dans des compartiments différents
  - Les lignes de caches sont protégées par des codes de détection d'erreurs et chiffrées
    - Une clef symétrique par compartiment
    - Les clefs symétriques sont chiffrées par la clef publique du CPU
    - La clef privée est stockée dans le CPU

Xom, les inconvénients

- Rien n'empêche d'attaquer la pile réseau du noyau
- Le risque d'un noyau attaquant un processus utilisateur par une modification du comportement des appels système n'est pas suffisamment étudié
- Problèmes avec la mémoire partagée (IPC, librairies partagées)
- Permet de détecter une attaque réussie en intégrité lorsque la ligne sera chargée

Analyse de Xom

- Analyse suivant la même approche que pour Secvisor
  - La simplification porte sur le jeu d'instructions
  - 1 faille découverte, puis une autre dans le correctif
    - Possibilité d'invalider une ligne de cache sans que celle-ci ne soit écrite en mémoire

Overshadow

- Une seule machine virtuelle supportée
- Même approche que Xom mais le chiffrement et le code de détection d'erreurs sont générés par un hyperviseur logiciel
  - Une seule clef pour tous les processus utilisateurs
  - Le noyau invité n'est pas protégé
  - Chaque page mémoire physique est stocké en version chiffrée et non chiffrée
- Risque d'attaque du processus par modification des appels système

Terra

- Solution de virtualisation reposant sur une signature du code
  - Le but est de proposer une chaîne de certification de l'ensemble du code exécuté de la machine, du BIOS aux processus utilisateur
  - Protection également contre l'administrateur de la plateforme
  - Permet d'authentifier la machine dans un réseau privé de confiance
  - Le but est d'être utilisable avec le NGSCB
  - Les virus

Orienté confinement d'intrusions

Shype

- Shype est basé sur Xen
  - Le but est d'empêcher une fuite d'informations en cas d'attaque réussie
    - Par exemple interdire deux machines virtuelles de partager le même réseau IP
- Dépend des risques de sécurité de Xen
  - Cela inclut les canaux cachés

Conclusion

- Un gestionnaire de machines virtuelles de confiance doit implanter la défense en profondeur et rentrer dans au moins deux catégories
  - Prévention d'intrusions
  - Détection d'intrusions
    - Le problème des firmwares, etc.
- Le confinement d'intrusions paraît trop difficile en raison des moyens de communication sur un PC

Questions ?