Références, guides et historique des vulnérabilités

Timothée Ravier
siosm@floss.social - tim.siosm.fr/cours - github.com/travier

5e année cycle ingénieur, filière STI
Option Sécurité des Systèmes Embarqués et du Cloud (2SEC)

2024 - 2025

Références, guides et historique des vulnérabilités

- Références divers liées à la sécurité des systèmes Linux
- Historique des vulnérabilités des projets mentionnés dans le cours
- Liste de guides de durcissement système

Matériel : Co-processeurs et co-OS

- Plusieurs processeurs sur une carte mère moderne
- Plusieurs OS dans un système :
  - Intel Management Engine
  - AMD Platform Security Processor
  - Attacking SMM Memory via Intel CPU Cache Poisoning
- Modems et Baseband pour les téléphones mobiles
- Carte graphiques (GPU) : XDC2012: Graphics stack security
- TPM : ROCA vulnerability
- Cartes ethernet, Wi-Fi, fibre optique, etc.

Matériel : Co-processeurs et firmwares

- Matériel plein de logiciels : Firmwares
  - Binarly Discovers High-Impact Vulnerabilities In Firmware Impacting Millions Of Enterprise Devices
  - PixieFail: Nine vulnerabilities in Tianocore's EDK II IPv6 network stack
- Mises à jour avec Linux Vendor Firmware Service (LVFS)
- Configuration du BIOS/Firmware EFI : Recommandations de l'ANSSI
- Sécurité de la plateforme :
  - CHIPSEC: Platform Security Assessment Framework
  - https://github.com/ANSSI-FR/chipsec-check

Matériel : Nombreux éléments partagés

Attaques par canaux cachés :

- Pas d'isolation physique : matériel partagé :
  - Rowhammer
  - Reverse Engineering Intel DRAM Addressing and Exploitation
  - Cross Processor Cache Attacks
- Attaques utilisant des canaux cachés (ou détournées) :
  - temps & cache : Meltdown and Spectre
  - son : RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis
  - bruit électromagnétique : TEMPEST
  - Power LED (!) : Video-based Cryptanalysis
  - Lend Me Your Ear: Passive Remote Physical Side Channels on PCs

Noyau Linux

- Faille exploitable à distance : souvent réseau, très rare
- Faille locale : appels systèmes, surface d'attaque large :
  - Gestion de la mémoire : Dirty CoW
  - Gestion des caches : Dirty Pipe Linux Vulnerability: Overwriting Files in Container Images
  - Systèmes de fichiers :
    - CVE-2015-1328 : incorrect permission checks in overlayfs
    - Enforcing mount options for sysfs and proc
  - Drivers : bluetooth, ioctl (cf. Android), etc.
    - BleedingTooth: Linux Bluetooth Zero-Click Remote Code Execution
  - Réseau : netfilter, etc.

Noyau Linux

- Très nombreux bugs découverts à l'aide du fuzzing
- google/syzkaller: Found bugs
- Defragmenting the kernel development process
- Voir les (nombreuses) présentations sur l'exploitation du noyau :
  - Linux Kernel Exploitation - Earning Its Pwnie a Vuln at a Time
  - Exploiting the Linux kernel: Measures and countermeasures

Durcissement distributions Linux

- Durcissement « classique » à l'aide de guides de recommandations :
  - Recommandations de sécurité relatives à un système GNU/Linux
  - Recommandations de sécurité pour l'architecture d'un système de journalisation
  - Sécurité des systèmes de virtualisation
  - Recommandations relatives à l'administration sécurisée des systèmes d'information
  - NIST Application Container Security Guide
  - Security Assurance Requirements for Linux Application Container Deployments
  - NIST Guidance on Application Container Security

Vulnérabilités spécifiques à LXC

- Vulnérabilités historiques :
  - à la création d'un conteneur : LXC CVE-2013-6441
  - dans les templates de création de conteneurs : Security issue in LXC (CVE-2015-1335)

Vulnérabilités spécifiques à Docker

- Démon `dockerd` et `containerd` tournent en `root`
- Opération sur des images qui ne sont pas de confiance : Before you initiate a “docker pull”
- Vulnérabilités historiques :
  - Docker 1.3.2 - Security Advisory
  - Docker 1.6.1 - Security Advisory
- Nouvelle architecture depuis la version 1.11.0

Vulnérabilités KVM

- CVE-2015-0239: Emulation incomplète de l'instruction SYSENTER
- CVE-2014-0049: Erreur dans l'émulateur x86

Vulnérabilités Xen

- XSA : https://xenbits.xen.org/xsa/
- CVE-2014-8594 / XSA-109, CVE-2015-2151 / XSA-123 : élévation de privilège
- CVE-2015-7835 / XSA-148 :
  - Nécessite d'être `root` dans une machine virtuelle PV
  - Accès à la totalité de la mémoire du système
  - Qubes Security Bulletin #22
- CVE-2015-8550 / XSA-155 :
  - Nécessite d'être `root` dans une machine virtuelle PV ou HVM
  - Elevation de privilège

Vulnérabilités QEMU (1)

- Virtunoid: A KVM Guest $\longrightarrow$ Host privilege escalation exploit (CVE-2011-1751) :
  - Bug dans la gestion du temps dans QEMU
  - Nécessite d'être `root` la machine virtuelle
  - Prise de contrôle de QEMU en Ring 3 mode VMX Root (« sortir » de la machine virtuelle)

Vulnérabilités QEMU (2)

- VENOM, don’t get bitten (CVE-2015-3456) :
  - Bug dans le pilote du contrôler de disquettes émulé par QEMU
  - Impacte tous les hyperviseurs
  - Activé par défaut dans toutes les machines virtuelles sans possibilité de le désactiver à l'exécution
  - Nécessite d'être `root` la machine virtuelle
  - Prise de contrôle de QEMU en Ring 3 mode VMX Root (« sortir » de la machine virtuelle)

Vulnérabilités VirtIO (hôte)

- Faille driver VirtIO :
  - CVE-2011-4127: privilege escalation from qemu / KVM guests
  - Nécessite d'être `root` la machine virtuelle
  - Donne l'accès total à un disque physique SCSI de l'hôte car le noyau ne vérifiait pas que les commandes SCSI correspondaient uniquement à des parties accessibles à la VM
  - Faille dans le noyau hôte

Alternatives à QEMU ? (Prototypes et expériences)

- lkvm / Native KVM tool (Stand-alone KVM tool) : virtualisateur, périphériques virtio et guests Linux uniquement
- novm (Google) : Go, périphériques virtio, expérimental
- NEMU (Intel) : version « nettoyée » de QEMU