Réflexion sur la confiance en la confiance, appliquée au montage des infrastructures systèmes et réseaux.

XS

URL pour ces slides

- https://inda.re/interhack/bootstrap0.pdf

Objectifs

- Disposer d'un système informatique de confiance comportant un ensemble défini de services centraux privés, de services en inter-connections par Internet et de terminaux utilisateurs.

Composantes

Un système informatique de ce type est composé de plusieurs éléments physiques et logiques assurant des roles distincs:

- Environnement de fonctionnement
- Arrivée, stabilisation et redondance électrique du composant
- Protection incendie
- Interconnection locale
- Interconnection vers l'extérieur
- Sauvegardes et archivage
- Procédures manuelles
- Procédures automatiques
- Systèmes de contrôle et d'initialisation
- Services d'administration
- Services accessibles utilisateurs authentifiés
- Services accessibles utilisateurs non authentifiés
- Stockage des données actives
- Stockage de données privées

Critères

L'objectif est atteint lorsque:

- L'intégrité des données est assurée et vérifiée
- Le système est restorable intégralement ou partiellement
- Les ressources techniques répondent exclusivement à leur opérateurs selon la politique d'accès établie
- Les services sont accessibles

Problèmes

- Complexité et vulnérabilités
- Risques liés à l'activité et aux expositions
- Surface exposée à des acteurs mal intentionnés
- Criticité de boites-noires
- Indisponibilité du code source
- Pannes matérielles
- Déploiement et maintenances
- Protection de l'environnement de fonctionnement
- Gestion des imprévus
- Complexité d'administration

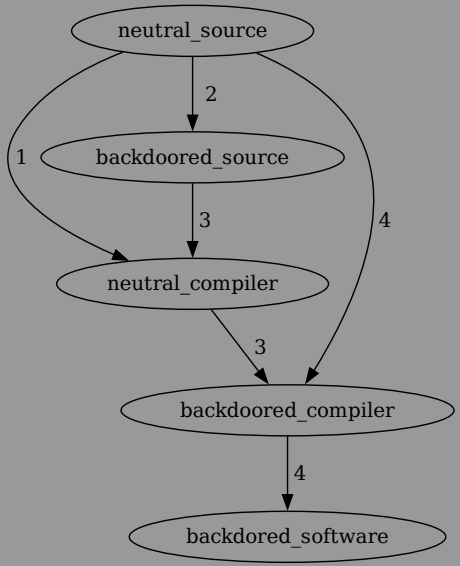
Solutions

- Sobriété, veille, architecture et isolations
- Choix du matériel
- Redondance
- Stock de rechange
- Analyse des firmwares
- Bonnes pratiques, procédures, communication
- Choix du lieu
- Disponibilité des opérateurs
- Entrainement
- Inventaire
- Surveillance

Reflection on trusting trust

- https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf

No amount of source-level verification or scrutiny will protect you from using untrusted code. - Ken Thompson


neutral_source
2
1
backdoored_source
3
4
neutral_compiler
3
backdoored_compiler
4
backdored_software

Real life

- Karger-Schell-Thompson attack in real life: https://niconiconi.neocities.org/posts/ken-thompson-really-did-launch-his-trusting-trust-trojan-attack-in-real-life/

3.4.5 Trap Door insertion (Page 16)

- 1974 Karger-Schell Multics research: https://web.archive.org/web/20030410020522/https://www.acsac.org/2002/papers/classic-multics-orig.pdf

Boostrapping d'une infrastructure

Obtenir une machine de déploiement

- Machine neuve
- Machine d'occasion
- Coreboot Laptops
- Chromebooks
- Optiplex / thinkcentre
- Board ARM
- Clavier, Écran, Souris

Matériel

- Programmeur TTL i2c/spi
- Pince SOIC-8
- Cables DB9
- Ports séries

Obtenir un réseau de confiance

- Point d'accès mobile (ROM Fiable)
- Connection du FAI
- Crosschecking
- Utilisation de tor
- DNS
- NTP

Initiator Firmwares

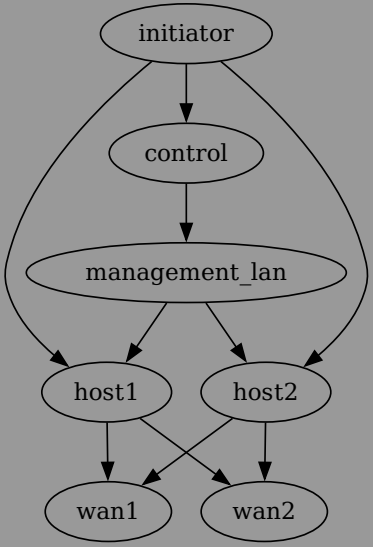
- Image BIOS
- Image BMC
- RAID Controller Bundles
- Disk firmwares

Checklist pour l'installation initiale d'un noeud

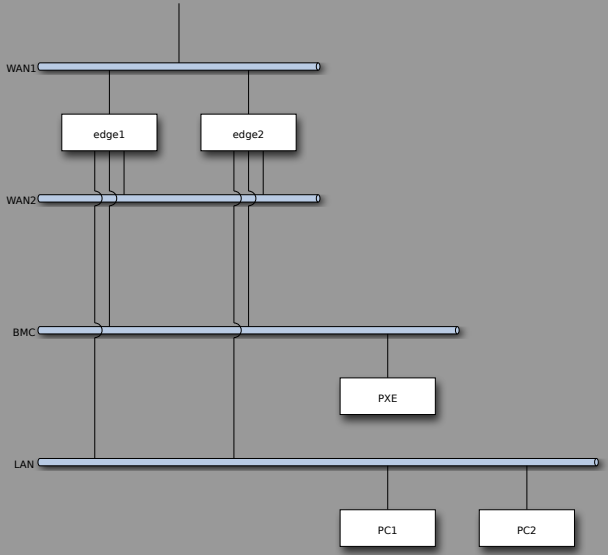
- Réseau de confiance
- BIOS + Firmwares
- Vérifications des signatures et hash

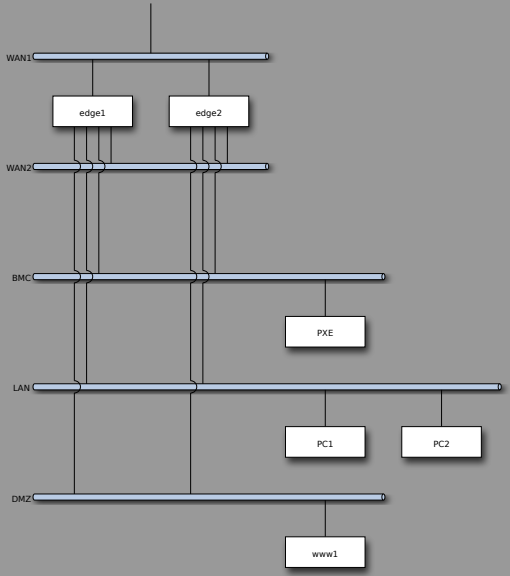
Idées

Un workflow de déployement



Architectures redondantes




WAN1
edge1
edge2
WAN2
BMC
PXE
LAN
PC1
PC2
DMZ
www1

Bootstrap to GCC

- https://lwn.net/Articles/841797/
- https://github.com/oriansj/stage0
- https://bootstrapping.miraheze.org/wiki/Main_Page
- https://bootstrappable.org

Bas niveau

- AVAR2021 Alex Matrosov Keynote: https://github.com/binarly-io/Research_Publications/blob/main/AVAR_2021/avar_2021_keynote.pdf
- Attacking Intel Bios: https://www.blackhat.com/presentations/bh-usa-09/WOJTCZUK/BHUSA09-Wojtczuk-AtkIntelBios-SLIDES.pdf
- Secure Boot chain in UEFI: https://laurie0131.gitbooks.io/understanding-uefi-secure-boot-chain/content/secure_boot_chain_in_uefi/

Matériel

- Betrusted talk: https://media.ccc.de/v/36c3-10690-open_source_is_insufficient_to_solve_trust_problems_in_hardware

AMT/ME, PSP

- https://en.wikipedia.org/wiki/Intel_Management_Engine
- https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor
- https://media.ccc.de/v/thms-38-dissecting-the-amd-platform-security-processor
- https://media.ccc.de/v/36c3-10942-uncover_understand_own_-_regaining_control_over_your_amd_cpu

ME overview and deblobbing

- Linux ME Interface: https://docs.kernel.org/driver-api/mei/mei.html
- coreboot-utils: intelmetool
  https://github.com/coreboot/coreboot/tree/main/util
- me_cleaner (également intégré à coreboot)
- https://github.com/corna/me_cleaner

BIOS/Firmwares Analysis

- https://github.com/coreboot/bios_extract
- https://www.radare.org/n/radare2.html
- https://ghidra-sre.org

ANSSI

- https://cyber.gouv.fr/publications/guide-dhygiene-informatique
- https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance