AYI NEDJIMI Consultants

TPM et BitLocker : Cold Boot et Bypass Chiffrement

Catégorie : Techniques de Hacking Lecture : 50 min Publié le : 04/04/2026 Auteur : Ayi NEDJIMI

Guide expert TPM et BitLocker : cold boot, TPM sniffing, evil maid et bypass chiffrement

Le **TPM** (*Trusted Platform Module*) et **BitLocker** forment le duo de chiffrement de disque standard sur les systèmes Windows. Le TPM stocke les clés de chiffrement dans un coprocesseur matériel protégé, et BitLocker chiffre l'intégralité du volume système. Cependant, cette architecture présente des **vulnérabilités fondamentales** exploitées par les chercheurs et les attaquants : **cold boot attacks** (extraction des clés depuis la RAM), **TPM sniffing** (interception de la clé sur le bus SPI/LPC), **evil maid attacks** (modification du bootloader), et **direct memory attacks** via DMA Thunderbolt/PCIe. Ce guide technique couvre l'architecture TPM (1.2 vs 2.0, fTPM vs dTPM), les mécanismes de protection BitLocker (Seal/Unseal, PCR, protecteurs), les techniques d'attaque documentées et les contre-mesures effectives pour les organisations manipulant des données sensibles.

En bref

- TPM : architecture 1.2/2.0, PCR, Seal/Unseal, fTPM vs dTPM et bus d'attaque
- BitLocker : protecteurs (TPM-only, TPM+PIN, clé USB), modes de chiffrement et récupération
- Cold Boot Attack : extraction de clés AES depuis la RAM par refroidissement (cryogénie)
- TPM Sniffing : interception de la VMK BitLocker sur le bus SPI/LPC avec un logic analyzer
- Mitigations : TPM+PIN obligatoire, Secure Boot, DMA protection et chiffrement mémoire

TPM (Trusted Platform Module) — Coprocesseur cryptographique dédié, soudé sur la carte mère (dTPM) ou intégré dans le CPU (fTPM — firmware TPM). Le TPM stocke des clés cryptographiques, mesure l'intégrité du boot (PCR), et effectue des opérations cryptographiques (RSA, ECC, AES) dans un environnement matériellement isolé du CPU principal.

Architecture TPM 2.0

Composant TPM	Fonction	Vecteur d'attaque
PCR (Platform Configuration Register)	Mesures d'intégrité du boot (hash chain)	PCR replay, boot manipulation
Storage Root Key (SRK)	Clé racine pour le chiffrement des secrets	Non extractible (hardware)
Endorsement Key (EK)	Identité unique du TPM (attestation)	Attestation replay
Seal/Unseal	Chiffrer/déchiffrer lié à l'état PCR	PCR manipulation → unseal
Bus SPI/LPC	Communication dTPM ↔ CPU	Sniffing physique du bus

BitLocker : Mécanismes de Protection

BitLocker chiffre le volume avec une **FVEK** (Full Volume Encryption Key), elle-même chiffrée par une **VMK** (Volume Master Key), elle-même protégée par un ou plusieurs **protecteurs** :

- **TPM-only** (défaut) : la VMK est scellée dans le TPM et libérée automatiquement au boot si les PCR sont correctes. **VULNÉRABLE** — aucune interaction utilisateur, la clé est transmise en clair sur le bus TPM.
- **TPM+PIN** : la VMK nécessite le TPM ET un PIN utilisateur. Le PIN participe à la dérivation de la clé. **RECOMMANDÉ** — le sniffing du bus ne suffit plus.
- **TPM+StartupKey** : la VMK nécessite le TPM ET une clé USB de démarrage. Protection similaire au PIN.
- **Password-only** : pas de TPM, la VMK est dérivée du mot de passe utilisateur. Vulnérable au brute-force si le mot de passe est faible.

Cold Boot Attack : Extraction des Clés depuis la RAM

La **cold boot attack** exploite la **rémanence de la DRAM** : les données en RAM ne disparaissent pas instantanément quand l'alimentation est coupée. En refroidissant les modules de RAM (air compressé inversé : -50°C, ou azote liquide : -196°C), la rémanence peut durer **plusieurs minutes**. Le processus d'attaque :

1. **Refroidir la RAM** : air compressé inversé sur les modules DRAM (gel visible sur les puces)
2. **Redémarrer sur un OS live** : boot USB avec un outil d'extraction (cold boot tool, volatility)
3. **Dump de la RAM** : lire le contenu de la RAM avant que les données ne se dégradent
4. **Extraction des clés** : rechercher les clés AES de BitLocker dans le dump (patterns AES key schedule)

Les outils **aeskeyfind** et **rsakeyfind** recherchent automatiquement les key schedules AES et RSA dans un dump mémoire. L'attaque est efficace contre BitLocker en mode **TPM-only** car la clé FVEK est en mémoire en clair pendant toute la durée du fonctionnement.

TPM Sniffing : Interception sur le Bus SPI/LPC

Pour les systèmes avec un **dTPM** (TPM discret, puce séparée), la communication entre le CPU et le TPM passe par un bus physique (SPI ou LPC). En connectant un **logic analyzer** (Saleae, DSLogic) aux traces du bus, l'attaquant peut intercepter la VMK BitLocker quand le TPM la libère au boot :

```
# TPM Sniffing avec un Saleae Logic Analyzer
# 1. Identifier les pins SPI du dTPM sur la carte mère
# (CLK, MOSI, MISO, CS — datasheet du TPM)

# 2. Connecter le logic analyzer aux traces SPI

# 3. Capturer pendant le boot
# Le TPM envoie la VMK en réponse à TPM2_Unseal

# 4. Décoder la capture SPI
# L'outil tpm2-spi-decode parse le protocole TPM sur SPI
python3 tpm2_spi_decode.py --capture boot_capture.sr

# 5. Extraire la VMK
# La VMK est envoyée dans la réponse TPM2_Unseal
# Puis utilisée par BitLocker pour déchiffrer la FVEK

# 6. Déchiffrer le volume BitLocker avec la VMK
dislocker -V /dev/sda2 -K vmk.bin -- /mnt/bitlocker
```

Evil Maid Attack et Bootloader Manipulation

L'**evil maid attack** cible le bootloader : l'attaquant modifie le Windows Boot Manager pour injecter un keylogger qui capture le PIN BitLocker (si TPM+PIN est configuré) et le transmet à l'attaquant. Les mitigations incluent **Secure Boot** (vérifie la signature du bootloader) et **Measured Boot** (les PCR changent si le bootloader est modifié).

fTPM : Vulnérabilités du TPM Firmware

Le **fTPM** (firmware TPM) — implémenté dans AMD PSP ou Intel PTT — n'est pas un coprocesseur séparé mais un logiciel tournant dans l'environnement de confiance du CPU. Les attaques sur le coprocesseur de sécurité (AMD PSP, Intel ME) peuvent compromettre le fTPM. En 2023, des chercheurs ont démontré **faulTPM** : une attaque par injection de fautes voltage glitching sur AMD fTPM, permettant d'extraire les secrets scellés — y compris les clés BitLocker.

⚠️ **Attention** — BitLocker en mode TPM-only (la configuration par défaut de Windows) est vulnérable au cold boot et au TPM sniffing. Le TPM+PIN est le minimum requis pour une protection efficace contre les attaques physiques. Pour les données hautement sensibles, ajoutez une clé USB de démarrage en complément.

À retenir

- Le TPM stocke les clés dans un coprocesseur matériel isolé — mais la clé transite en clair sur le bus SPI/LPC
- BitLocker TPM-only (défaut Windows) est vulnérable au cold boot ET au TPM sniffing — toujours activer TPM+PIN
- Le cold boot attack exploite la rémanence DRAM — les clés AES sont en mémoire pendant toute la session
- Le fTPM (AMD PSP, Intel PTT) est vulnérable aux attaques sur le coprocesseur (faulTPM, voltage glitching)
- Secure Boot + Measured Boot protègent contre les evil maid attacks (modification du bootloader)

FAQ — Questions Fréquentes

BitLocker en mode TPM-only est-il vraiment vulnérable ?

Oui, **BitLocker TPM-only est vulnérable** aux attaques physiques. Le TPM libère automatiquement la VMK au boot sans interaction utilisateur — un attaquant peut extraire la clé via cold boot (RAM freeze) ou TPM sniffing (logic analyzer sur le bus SPI). Microsoft documente que TPM-only protège contre le vol de disque (hors machine) mais pas contre un attaquant avec accès physique à la machine complète.

Comment se protéger contre le cold boot attack ?

Les mitigations principales : **TPM+PIN** (le PIN participe à la dérivation de la clé — même avec la RAM, l'attaquant ne peut pas reconstruire la clé sans le PIN), **désactiver le boot USB** dans le BIOS/UEFI, **activer Secure Boot**, et **couper l'alimentation complètement** (pas de mise en veille/hibernation). DDR5 avec ECC a une rémanence plus courte que DDR4, mais n'élimine pas le risque.

Le TPM sniffing fonctionne-t-il sur les fTPM (Intel PTT, AMD PSP) ?

Non, le TPM sniffing ne fonctionne **pas sur les fTPM** car il n'y a pas de bus physique séparé — le fTPM est intégré dans le CPU. C'est un avantage sécurité des fTPM sur les dTPM. Cependant, les fTPM sont vulnérables à d'autres attaques : faulTPM (voltage glitching sur AMD PSP), exploitation du firmware PSP/ME, et side-channel attacks sur le CPU.

Article recommandé : Format String Exploitation : Du Crash au RCE Moderne

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.