AYI NEDJIMI Consultants

SGX, TDX et TEE : Attaques sur les Enclaves Sécurisées 2026

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

Guide expert SGX, TDX et TEE : attaques side-channel, Foreshadow, confidential computing

Les **enclaves sécurisées** — Intel *SGX* (Software Guard Extensions), Intel *TDX* (Trust Domain Extensions) et ARM *TrustZone* — promettent l'exécution de code dans un environnement isolé, protégé même contre un système d'exploitation compromis ou un hyperviseur malveillant. Ces **TEE** (Trusted Execution Environments) sont la pierre angulaire du **confidential computing**, protégeant les données en cours de traitement dans les environnements cloud multi-tenant. Cependant, des années de recherche en sécurité ont révélé des vulnérabilités fondamentales dans ces technologies : attaques par canaux auxiliaires, failles d'implémentation, et limitations architecturales. Ce guide technique approfondi analyse les mécanismes de protection SGX, TDX et TrustZone, détaille les attaques publiées avec leurs exploits, et évalue l'état réel de la sécurité des enclaves en 2026. Les architectes cloud, les développeurs d'applications confidentielles et les chercheurs en sécurité matérielle y trouveront une référence technique complète avec des exemples pratiques et des recommandations.

En bref

- Architecture SGX : enclaves, attestation, sealing et mémoire EPC
- Attaques side-channel : cache timing, page-table, branch prediction sur SGX
- Spectre/Meltdown/Foreshadow : exploitation de l'exécution spéculative dans les enclaves
- TDX et SEV-SNP : confidential VMs et leurs surfaces d'attaque
- ARM TrustZone : architecture, OP-TEE et vulnérabilités des Trusted Applications

TEE (Trusted Execution Environment) — Environnement d'exécution matériellement isolé qui protège le code et les données contre les logiciels non autorisés, y compris le système d'exploitation et l'hyperviseur. Les TEE fournissent des garanties de confidentialité et d'intégrité via le chiffrement mémoire et l'attestation à distance.

Architecture Intel SGX

Intel SGX permet aux applications de créer des **enclaves** — des régions de mémoire chiffrées et isolées par le matériel. Le CPU chiffre les données de l'enclave avec une clé matérielle (MEE — Memory Encryption Engine) avant qu'elles ne quittent le cache L3. Même un attaquant avec un accès physique ou un contrôle du système d'exploitation ne peut pas lire la mémoire de l'enclave en clair.

Composant	Fonction	Vecteur d'attaque
EPC (Enclave Page Cache)	Mémoire chiffrée pour les enclaves (128-256 MB)	Side-channel via les page faults
EPCM	Métadonnées de pages enclave	Mapping manipulation
Attestation	Vérification à distance de l'intégrité	Faking attestation quotes
Sealing	Chiffrement persistant des données	Key extraction si matériel compromis
AEX (Async Enclave Exit)	Interruption de l'enclave	Interrupt-driven side-channel

Controlled-Channel Attacks sur SGX

L'attaque **controlled-channel** (Xu et al., 2015) exploite le fait que l'OS contrôle les tables de pages de l'enclave. L'OS malveillant peut rendre des pages de l'enclave non-présentes (clear le bit Present), puis observer les page faults pour déterminer quelles pages de code et de données l'enclave accède. Cette séquence d'accès aux pages révèle le flux de contrôle et les patterns d'accès aux données — suffisant pour extraire des clés cryptographiques et des données sensibles.

```
// Controlled-channel attack : principe
// L'OS attaquant contrôle les page tables de l'enclave

// 1. Rendre toutes les pages de l'enclave non-présentes
for (each page in enclave) {
    page_table[page].present = 0;
}

// 2. L'enclave exécute son code → page fault sur chaque accès
// 3. Le handler de page fault enregistre l'adresse faultée
// 4. Re-mapper la page, laisser l'enclave continuer
// 5. Recommencer → trace d'accès aux pages complète

// Résultat : l'OS connaît la séquence exacte des pages accédées
// → Reconstruction du flux de contrôle de l'enclave
// → Extraction de secrets si le flux dépend des données
```

Attaques Cache sur les Enclaves SGX

Les enclaves SGX partagent les caches L1/L2/L3 avec le code non-enclave sur le même cœur. Les attaques **Prime+Probe** et **Flush+Reload** s'appliquent directement :

- **SGX-Step** : framework d'attaque permettant l'exécution pas-à-pas d'une enclave (une instruction à la fois) via la manipulation du timer APIC. Chaque instruction peut être suivie d'une mesure cache complète.
- **CacheZoom** : utilise Prime+Probe avec une résolution au niveau de la ligne de cache (64 octets) pour extraire des clés AES depuis une enclave SGX.

- **Plundervolt** : attaque par injection de fautes via la modification du voltage CPU (MSR 0x150). Les sous-voltages provoquent des erreurs de calcul dans l'enclave, corrompant les résultats cryptographiques de manière exploitable.

Foreshadow (L1TF) : Lecture de la Mémoire Enclave

Foreshadow (CVE-2018-3615) est une variante de Meltdown spécifique à SGX. Elle exploite le Terminal Fault dans le cache L1 : quand une adresse dans les tables de pages pointe vers la mémoire EPC (enclave) avec le bit Present à 0, l'exécution spéculative charge quand même les données depuis le cache L1 — **en clair**, avant le chiffrement MEE. Un attaquant peut lire n'importe quelle donnée d'enclave présente dans le cache L1, y compris les clés d'attestation et les données sensibles.

Intel TDX : Confidential VMs

Intel TDX (Trust Domain Extensions) étend les concepts de SGX à des machines virtuelles entières. Un *Trust Domain* (TD) est une VM dont la mémoire est chiffrée par le matériel et isolée de l'hyperviseur. Le **TDX Module** (un firmware Intel exécuté en mode SEAM — Secure Arbitration Mode) gère les transitions entre l'hyperviseur et les TDs. Contrairement à SGX, TDX protège une VM complète (OS + applications) sans modification du code applicatif.

AMD SEV-SNP : Secure Encrypted Virtualization

AMD SEV-SNP (Secure Nested Paging) chiffre la mémoire de chaque VM avec une clé unique gérée par le **PSP** (Platform Security Processor). SNP ajoute l'intégrité mémoire (détection des modifications par l'hyperviseur) et l'attestation à distance. Les attaques publiées incluent :

- **SEVered** : l'hyperviseur manipule les mappings de pages physiques pour rediriger les accès de la VM vers des pages contrôlées, extrayant les données en clair via les opérations I/O de la VM.
- **CipherLeaks** : exploitation des patterns de chiffrement (ciphertext side-channel) pour déduire les données en clair.
- **ÆPIC Leak** : fuite de données via les registres APIC non chiffrés, permettant la lecture de données de VMs SEV depuis l'hyperviseur.

ARM TrustZone : Monde Sécurisé et Normal

ARM TrustZone divise le processeur en deux mondes : le **Secure World** (exécute le TEE OS et les Trusted Applications) et le **Normal World** (exécute Android/Linux et les applications standard). La séparation est matérielle — le bit NS (Non-Secure) dans le bus AXI contrôle l'accès aux périphériques et à la mémoire. Le **Secure Monitor** (EL3) gère les transitions entre les deux mondes via l'instruction `SMC` (Secure Monitor Call).

Attaques sur OP-TEE et les Trusted Applications

OP-TEE est l'implémentation TEE open-source la plus déployée (Linaro/ARM). Les Trusted Applications (TAs) s'exécutent dans le Secure World avec des privilèges élevés. Les vulnérabilités typiques :

- **TA buffer overflows** : les TAs parsent les paramètres du Normal World sans validation suffisante → buffer overflows dans le Secure World
- **Shared memory attacks** : la mémoire partagée entre Normal et Secure World peut être modifiée par le Normal World pendant que la TA la traite (TOCTOU)
- **DRM key extraction** : les clés Widevine/PlayReady sont stockées dans les TAs — leur extraction permet le déchiffrement de contenus protégés
- **Secure Boot bypass** : compromettre le TEE permet de modifier la chaîne de boot sécurisée

Confidential Computing : État des Lieux 2026

Le **confidential computing** est déployé en production par les clouds majeurs :

Cloud	Technologie TEE	Service	Maturité
Azure	Intel SGX, TDX, AMD SEV-SNP	Confidential VMs, AKS Confidential	GA
GCP	AMD SEV-SNP, Intel TDX	Confidential VMs, Confidential GKE	GA
AWS	AWS Nitro Enclaves	Nitro Enclaves (pas SGX/TDX)	GA

Contre-mesures et Durcissement des TEE

Les contre-mesures pour protéger les applications TEE :

- **Oblivious RAM (ORAM)** : masque les patterns d'accès mémoire pour contrer les controlled-channel attacks — mais coût de performance 10-100x
- **Constant-time code** : implémenter les opérations cryptographiques en temps constant pour éliminer les timing side-channels
- **Data-oblivious algorithms** : algorithmes dont le flux de contrôle ne dépend pas des données secrètes
- **T-SGX** : utilisation de TSX (Transactional Synchronization Extensions) pour détecter les interruptions anormales pendant l'exécution de l'enclave
- **Partitionnement de cache** : isolation des lignes de cache entre enclave et non-enclave (Intel CAT — Cache Allocation Technology)

⚠️ **Attention** — Intel a déprécié SGX sur les processeurs desktop (12ème gen+) tout en le maintenant sur les Xeon serveur. TDX est le successeur pour le confidential computing cloud. Les applications SGX existantes doivent planifier leur migration vers TDX ou des alternatives (AMD SEV-SNP, ARM CCA).

💡 **Conseil pratique** — Pour développer des applications TEE sécurisées, utilisez les SDKs officiels (Intel SGX SDK, Open Enclave SDK, Gramine) et suivez les guidelines de codage sécurisé : minimisez la surface d'attaque de l'enclave, validez tous les inputs du monde non-sécurisé (ECALL/OCALL), et utilisez des implémentations cryptographiques constant-time.

> **À retenir**
>
> - SGX protège le code et les données contre l'OS et l'hyperviseur — mais les side-channels cache et page-table permettent l'extraction de secrets
> - Foreshadow (L1TF) permettait la lecture directe de la mémoire enclave via l'exécution spéculative — corrigé par microcode
> - TDX étend SGX aux VMs complètes — le TDX Module gère l'isolation entre hyperviseur et Trust Domains
> - AMD SEV-SNP chiffre la mémoire VM avec intégrité — mais des attaques par manipulation de pages (SEVered) existent
> - ARM TrustZone isole Secure/Normal World — les Trusted Applications sont vulnérables aux buffer overflows et TOCTOU
> - Le confidential computing cloud (Azure, GCP) est en production mais les side-channels restent un risque résiduel

FAQ — Questions Fréquentes

SGX est-il déprécié ?

Intel a **retiré SGX des processeurs desktop** à partir de la 12ème génération (Alder Lake). SGX reste disponible sur les **Xeon serveur** (Ice Lake, Sapphire Rapids). Intel pousse **TDX** comme successeur pour le confidential computing cloud. Les applications SGX existantes doivent planifier leur migration.

Quelle est la différence entre SGX et TDX ?

SGX protège des enclaves individuelles (régions de mémoire dans un processus). **TDX** protège des VMs entières (Trust Domains) — le système d'exploitation guest et toutes ses applications sont protégés sans modification du code. TDX est plus adapté au cloud car il ne nécessite pas de réécriture des applications.

Le confidential computing est-il vraiment sécurisé ?

Le confidential computing offre une protection significative contre les attaquants logiciels (hyperviseur compromis, admin cloud malveillant), mais il ne résout pas les **attaques side-channel matérielles** (cache timing, power analysis). Le modèle de menace doit être évalué au cas par cas. Pour les données les plus sensibles, combinez le TEE avec du chiffrement homomorphe ou du calcul multipartite sécurisé.

Article recommandé : Cryptanalyse Pratique : Attaques sur AES, RSA et ECC

📚 Articles connexes

- Side-Channel Attacks : Spectre et Meltdown
- Intel ME et AMD PSP : Exploitation Firmware
- Cryptanalyse Pratique : AES, RSA et ECC
- GPU Side-Channels : CUDA et OpenCL

🔗 Références externes

- SGX.fail — Intel SGX Attack Database
- Intel SGX Documentation officielle

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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