Stratégies de défense et d'attaque : le cas des consoles de jeux

R. BENADJILA, M. RENARD

ANSSI

3 juin 2015

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Contexte

- Consoles de jeux :
  - Vitrines technologiques sur le plan de la sécurité
- Depuis 20 ans, l'industrie du jeu vidéo investit du temps de R&D pour :
  - Lutter contre la contrefaçon et le piratage
  - Empêcher la prise de contrôle de leur plateforme

Objectifs

- Tour d'horizon de l'évolution de la sécurité
  - Playstation 1 : naissance des modchips
  - Xbox : quelques idées de sécurité
  - Xbox360 et PS3 : mise en œuvre de fonctions de sécurité

Objectifs

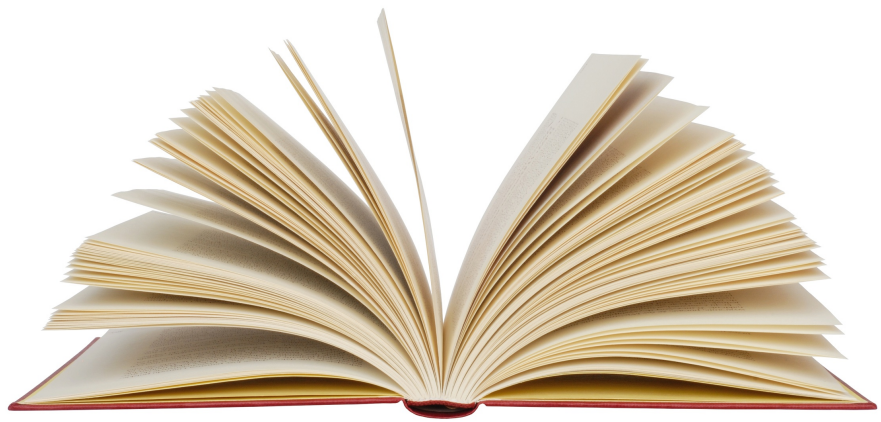
- Tour d'horizon de l'évolution de la sécurité
  - Playstation 1 : naissance des modchips
  - Xbox : quelques idées de sécurité
  - Xbox360 et PS3 : mise en œuvre de fonctions de sécurité
- Comprendre :
  - L'architecture matérielle et logicielle
  - Le choix des chemins d'attaque
  - L'évolution du type d'attaquant
    - Piratage de jeux
    - Prise de contrôle de la plateforme

Objectifs

- Tour d'horizon de l'évolution de la sécurité
  - Playstation 1 : naissance des modchips
  - Xbox : quelques idées de sécurité
  - Xbox360 et PS3 : mise en œuvre de fonctions de sécurité
- Comprendre :
  - L'architecture matérielle et logicielle
  - Le choix des chemins d'attaque
  - L'évolution du type d'attaquant
    - Piratage de jeux
    - Prise de contrôle de la plateforme
- Tirer quelques conclusions des erreurs commises

Avertissement

- Cette présentation est un apreçu :
  - Toutes les attaques ne seront pas présentées
  - Nous disposons de 25 minutes
  - L'article fait plus de 100 pages
- Les actes de 25 Kg dans votre sac, c'est nous ;-)
- Pour faire court : allez lire l'article !



Mise en garde !

Cette présentation décrit des techniques de Jailbreak dans un cadre purement défensif.
L'ANSSI incite les éditeurs à corriger systématiquement toute vulnérabilité identifiée dans les plus brefs délais.
Les utilisateurs sont quant à eux invités à appliquer ces correctifs dès leur publication.

Choose your player

Skill Level

Can I play, Daddy?

Don't hurt me.

Bring 'em on!

I am Death incarnate!

Choose your player

PS1

Skill Level

Can I play, Daddy?

Don't hurt me.

Bring 'em on!

I am Death incarnate!

Playstation 1

- Produite par Sony Computer Entertainment en 1994
- Contrefaçon de masse dès 1995

Playstation 1 : absence de sécurité par conception

- Processeur MIPS R3000 custom
  - Dépourvu d'unité de gestion mémoire (MMU)
  - Les processeurs RS3000E classiques en sont pourvus
- La sécurité semble être bien loin des préoccupations
- Sony semble avoir privilégié les fonctionnalités de DRM

Playsation 1 : zonage des jeux

- Zonage des jeux et des consoles par région
- Code régional
  - Dans le BIOS
  - Sur la piste d'amorçage (Lead-IN) des CD-ROM

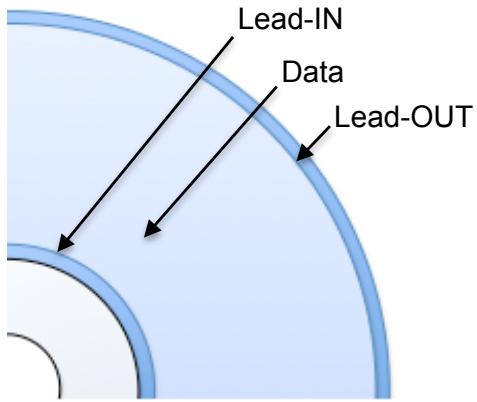
Playsation 1 : zonage des jeux

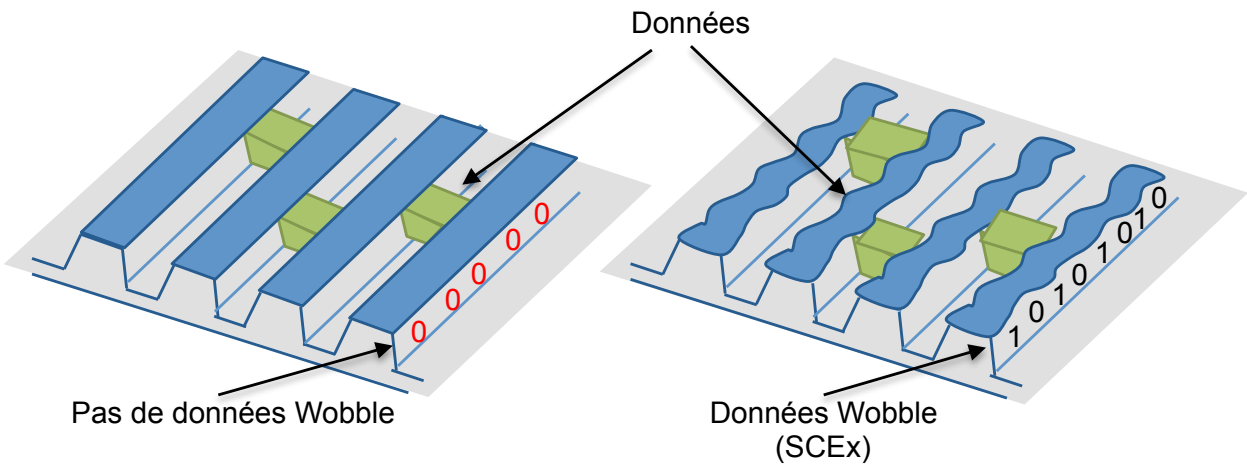
- Zonage des jeux et des consoles par région
- Code régional
  - Dans le BIOS
  - Sur la piste d'amorçage (Lead-IN) des CD-ROM
- Chaîne de caractères ayant la forme : SCEx
  - A pour l'Amérique (SCEA)
  - E pour l'Europe (SCEE)
  - I pour le Japon (SCEI)

Playsation 1 : zonage des jeux

- Zonage des jeux et des consoles par région
- Code régional
  - Dans le BIOS
  - Sur la piste d'amorçage (Lead-IN) des CD-ROM
- Chaîne de caractères ayant la forme : SCEx
  - A pour l'Amérique (SCEA)
  - E pour l'Europe (SCEE)
  - I pour le Japon (SCEI)
- Information stockée en utilisant le DRM Wobble groove
  - Impossible de faire un clone 1:1 de jeu

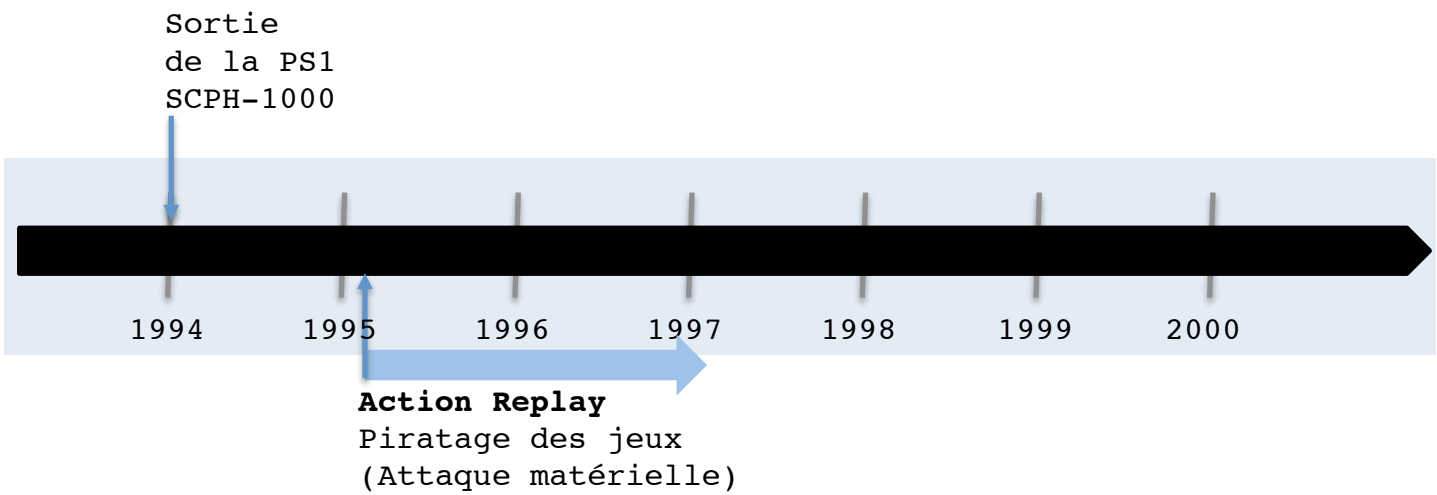
Playsation 1 : wobblegroove





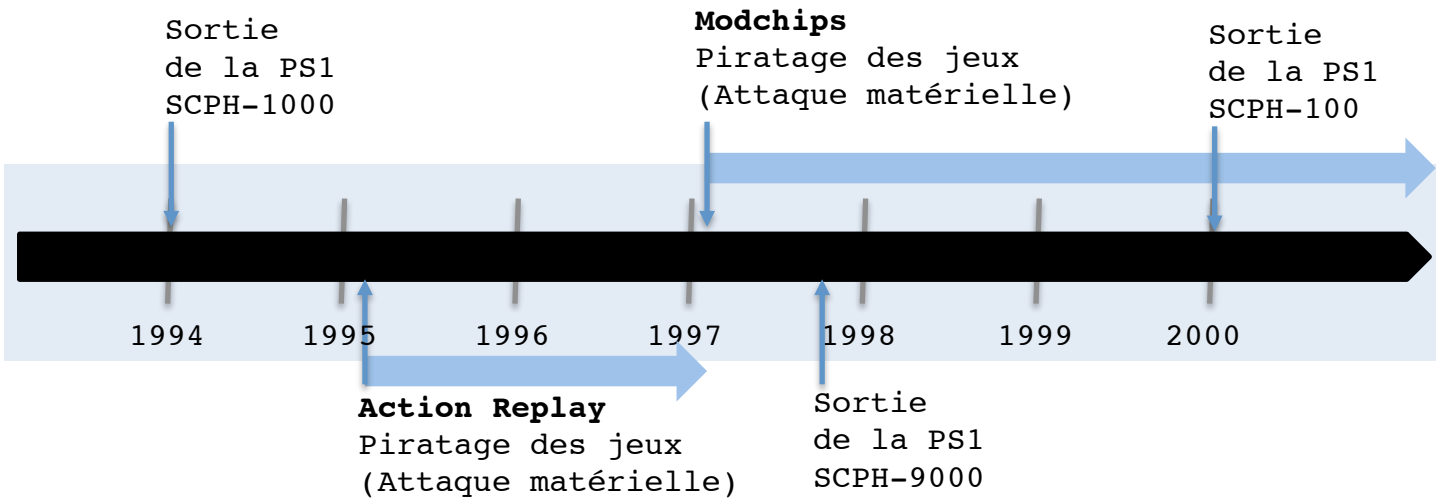
Playsation 1 : attaques

- Absence de fonctions de sécurité
- Objectif : contourner les fonctions de zonage

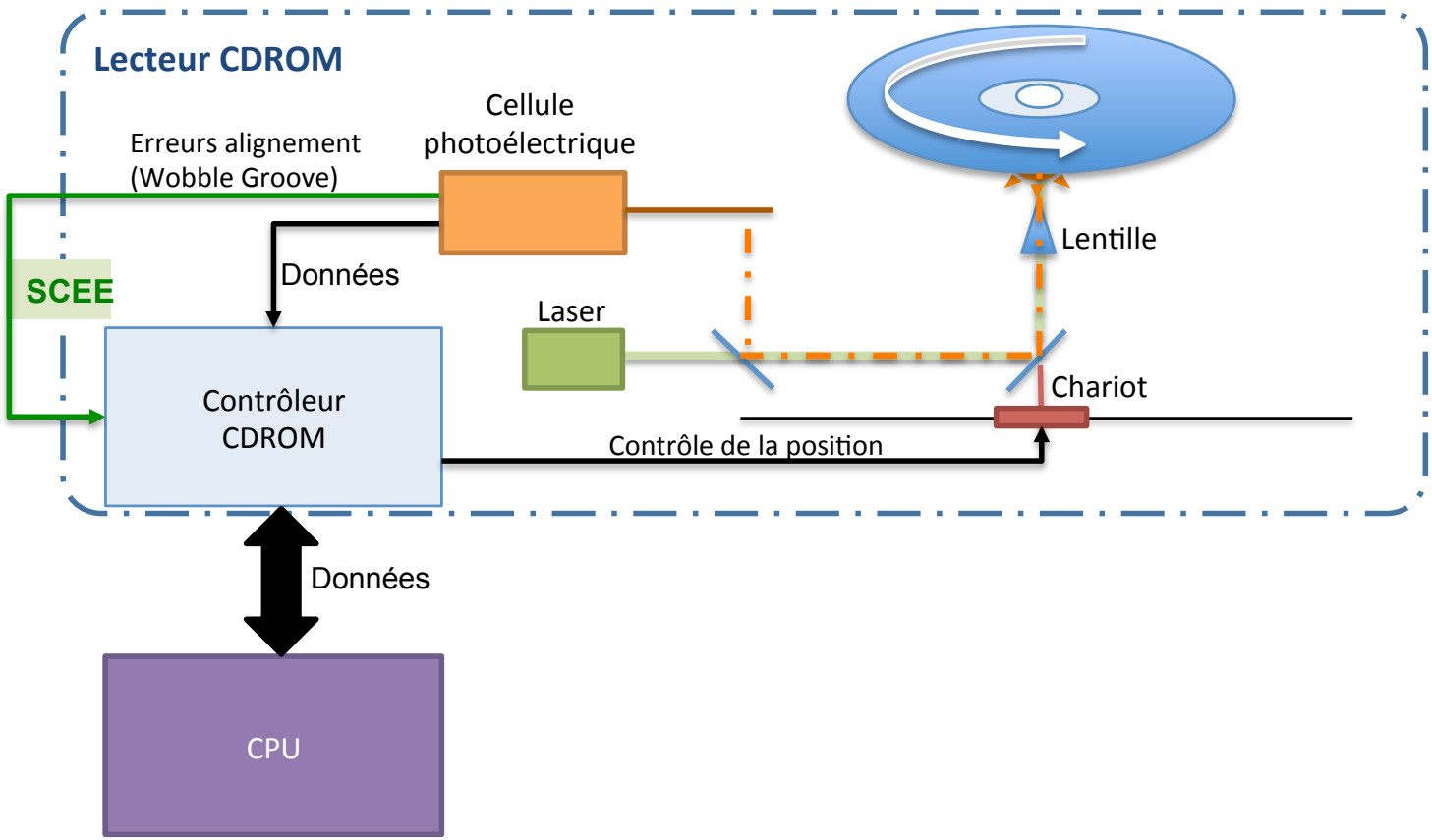


Playsation 1 : attaques

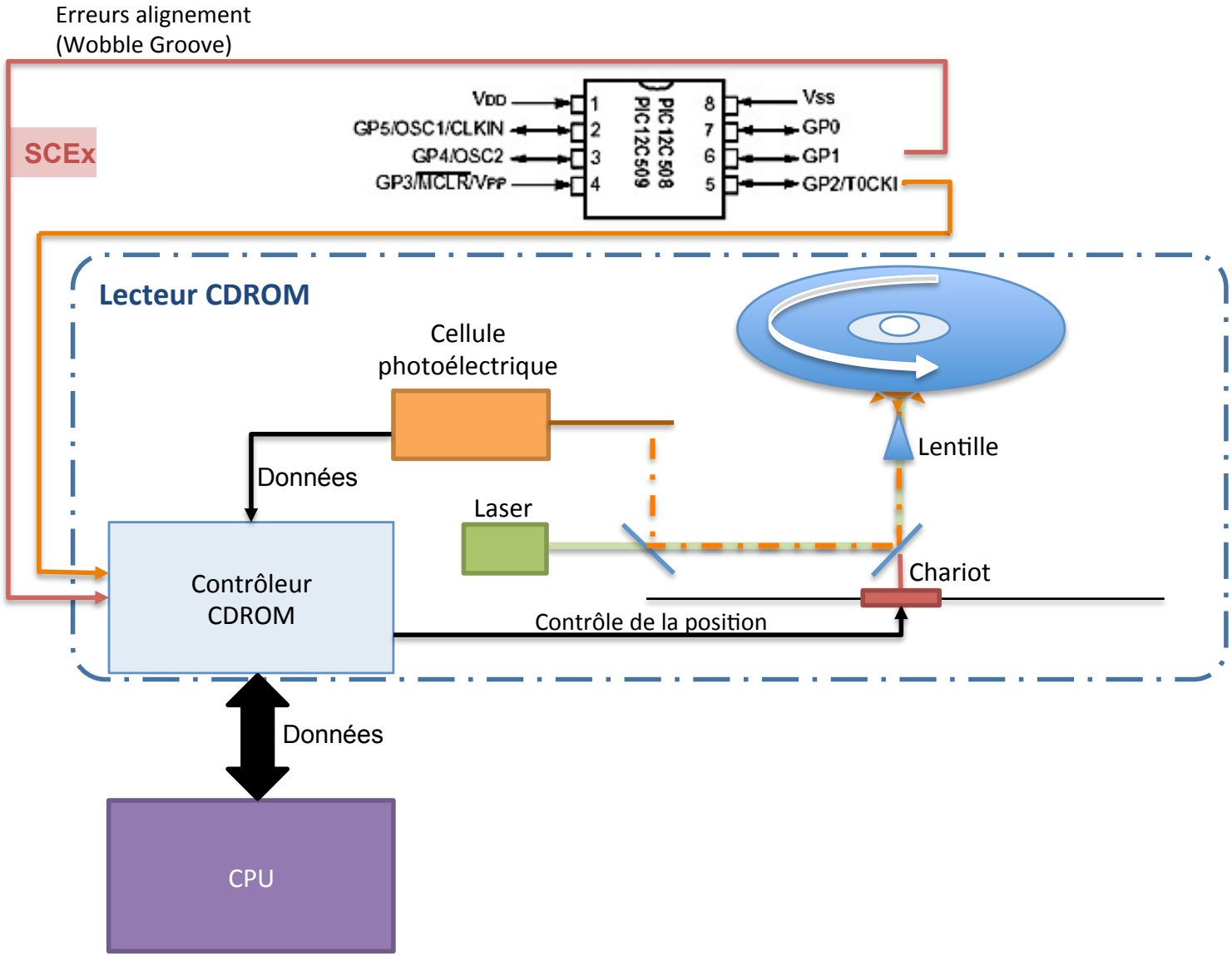
- Absence de fonctions de sécurité
- Objectif : contourner les fonctions de zonage



Playsation 1 : architecture Wobble Groove



Playsation 1 : naissance des Modchips



Playsation 1 : conclusion

- Absence de fonctionnalités de sécurité
- Contournement du DRM
- Généralisation des modchips
- Explosion de l'industrie du piratage

Choose your player

Skill Level

Can I play, Daddy?

Don't hurt me.

Bring 'em on!

I am Death incarnate!

Choose your player

Xbox

Skill Level

Can I play, Daddy?

Don't hurt me.

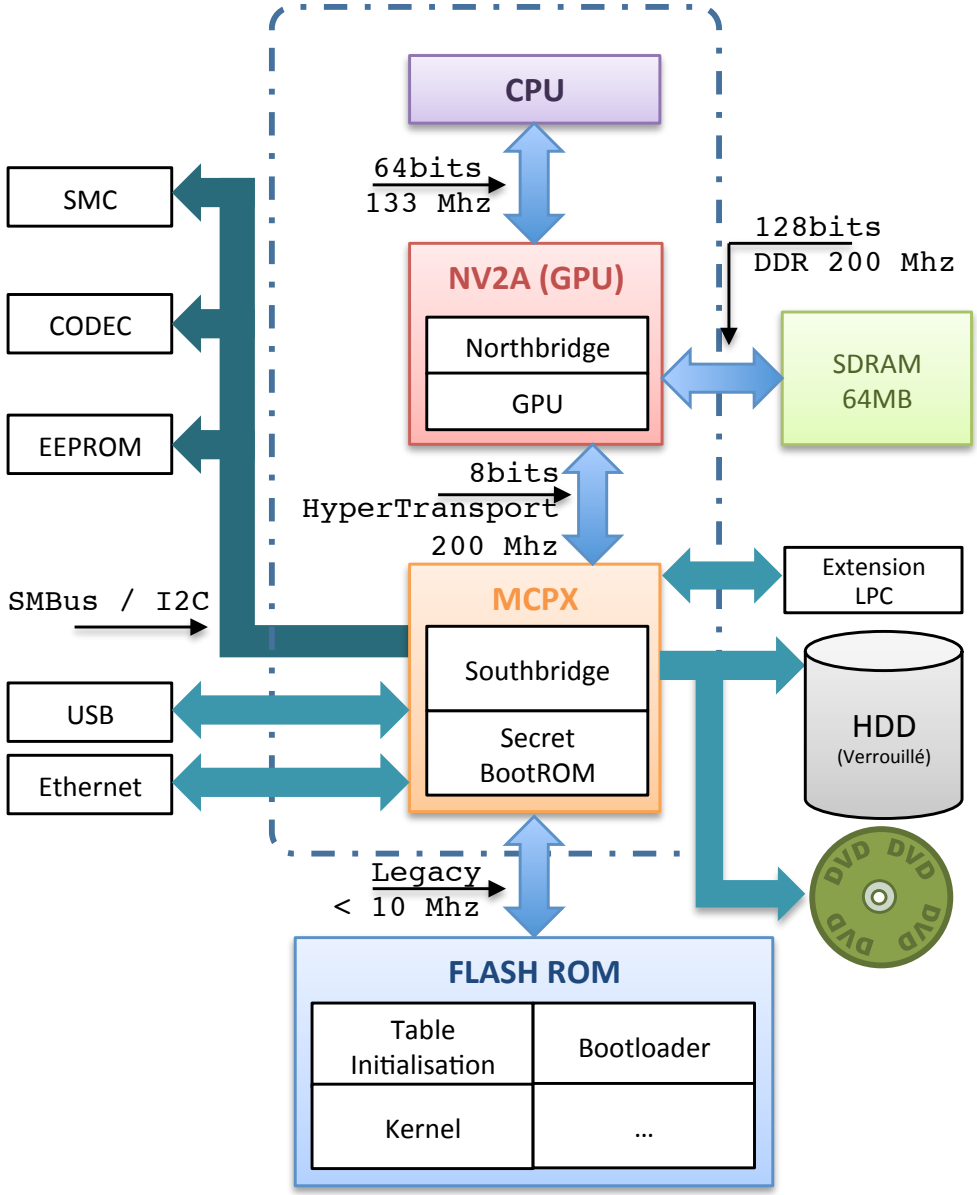
Bring 'em on!

I am Death incarnate!

Xbox

- Lancée aux États-Unis le 15 novembre 2001
- Architecture proche de celle d'un PC
- Noyau Windows 2000 simplifié
- Intègre des fonctionnalités de sécurité
  - Mises en défaut par différents attaquants

Xbox : architecture



Xbox : sécurité

- Binaires (XBE) signés
- Contrôle d'accès au contenu du disque dur
- Chaîne de démarrage de confiance

Xbox : bootROM et racine de confiance

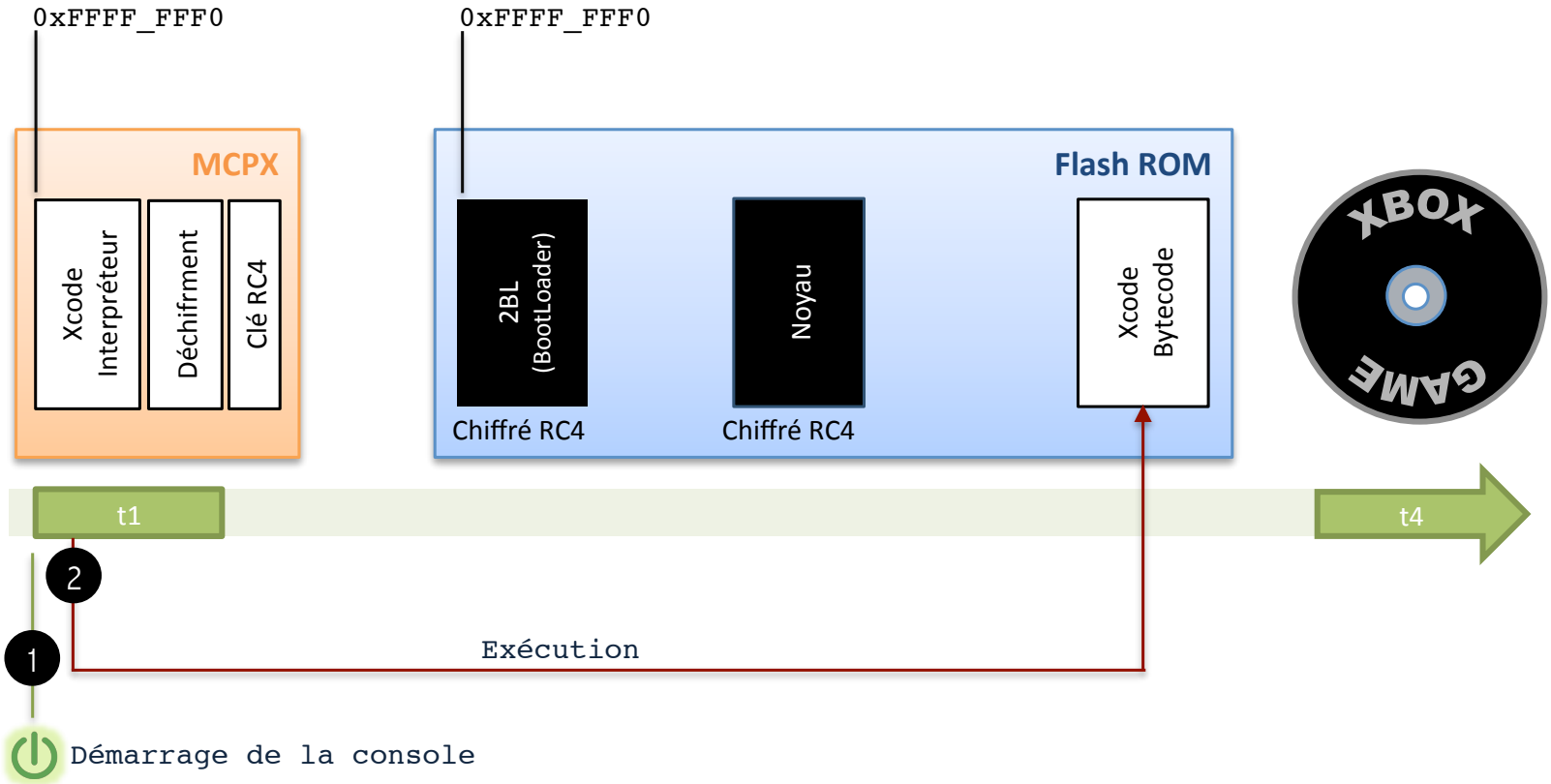
- Tentative de création de sa propre chaîne de confiance
  - Intégration code du bootloader dans le MCPX
  - Zone mémoire dans un composant de type ASIC ⇒ $$$$
  - Zone de stockage de la bootROM à 512 octets
- Pour diverses raisons le code de Training DDR > 1Ko

Xbox : bootROM et racine de confiance

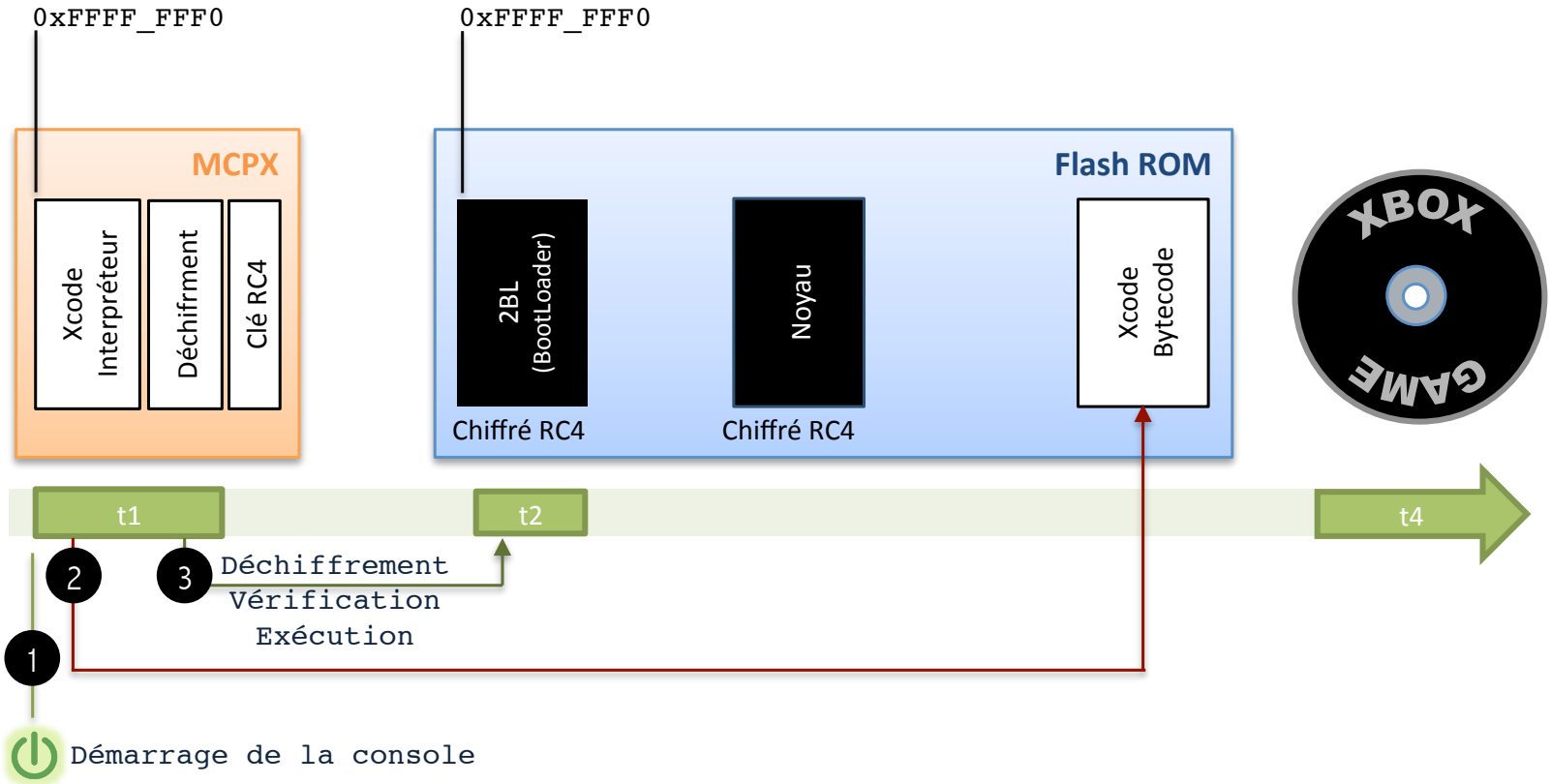
- Tentative de création de sa propre chaîne de confiance
  - Intégration code du bootloader dans le MCPX
  - Zone mémoire dans un composant de type ASIC ⇒ $$$$
  - Zone de stockage de la bootROM à 512 octets
- Pour diverses raisons le code de Training DDR > 1Ko
- Nécessité d'une zone mémoire externe (NAND)
  - Augmentation des risques d'extraction et d'analyse
  - Chiffrement d'une partie du contenu de la NAND (RC4)

Xbox : chaîne de démarrage de confiance

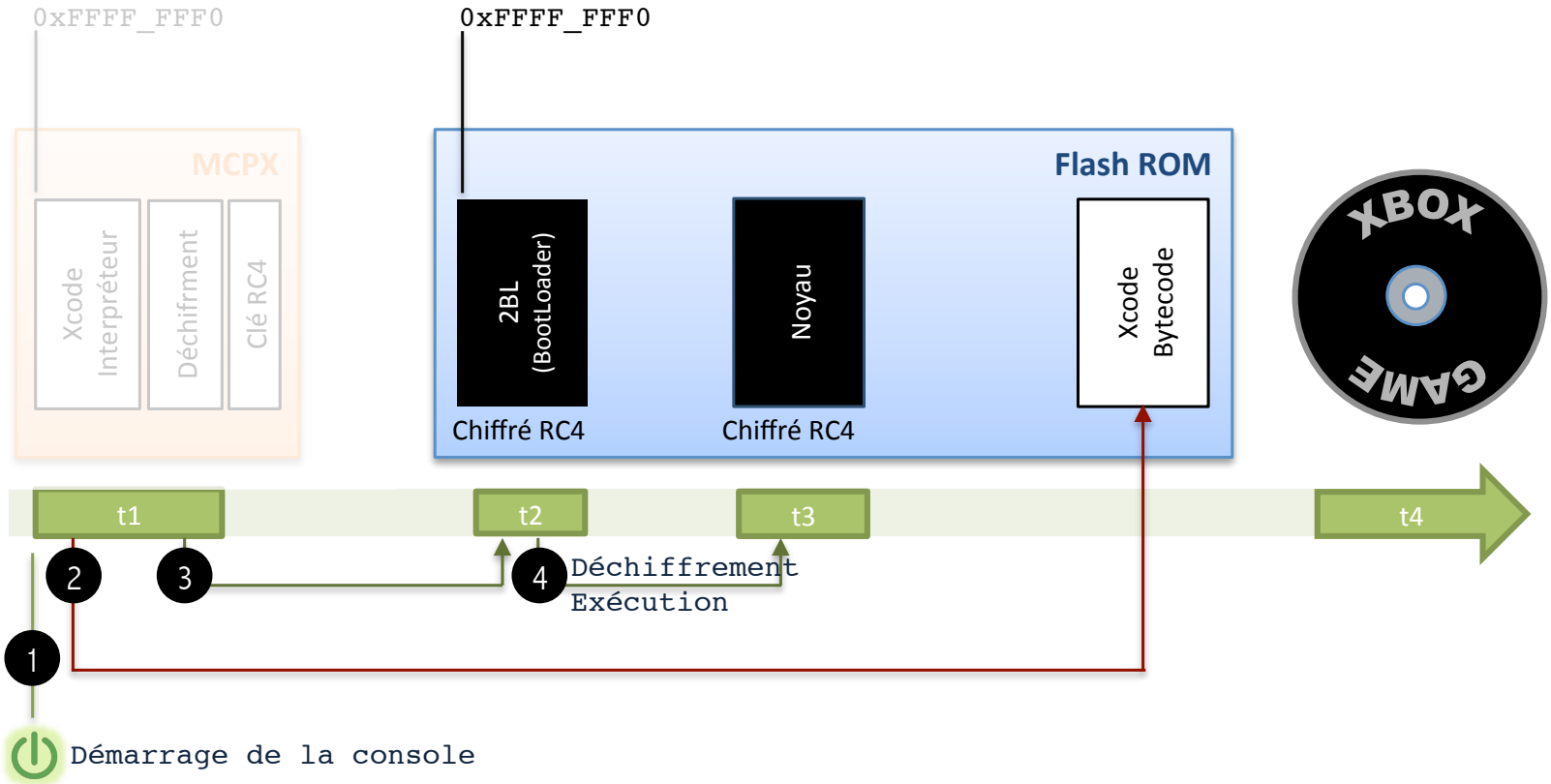
Xbox : chaîne de démarrage de confiance



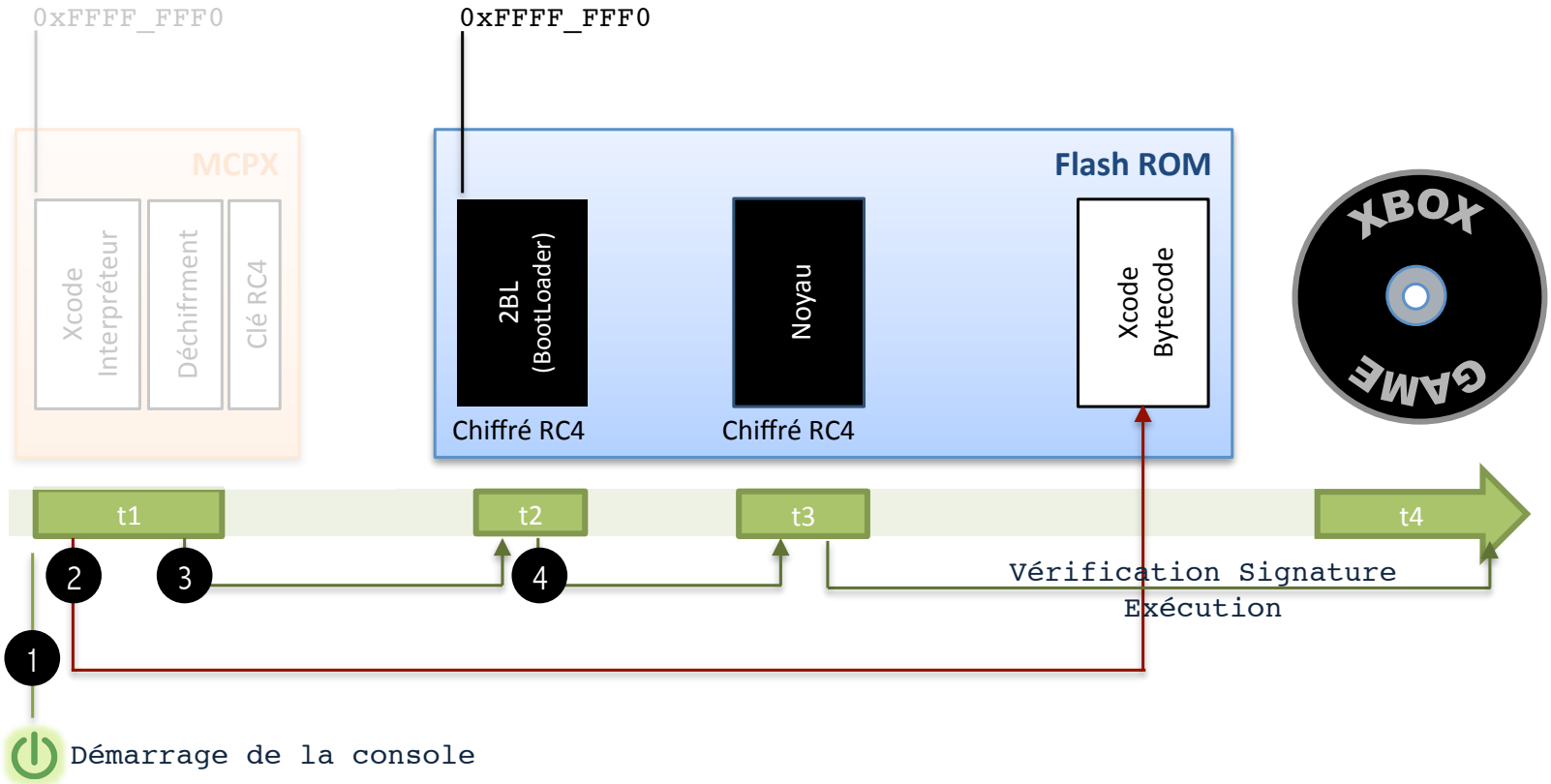
Xbox : chaîne de démarrage de confiance



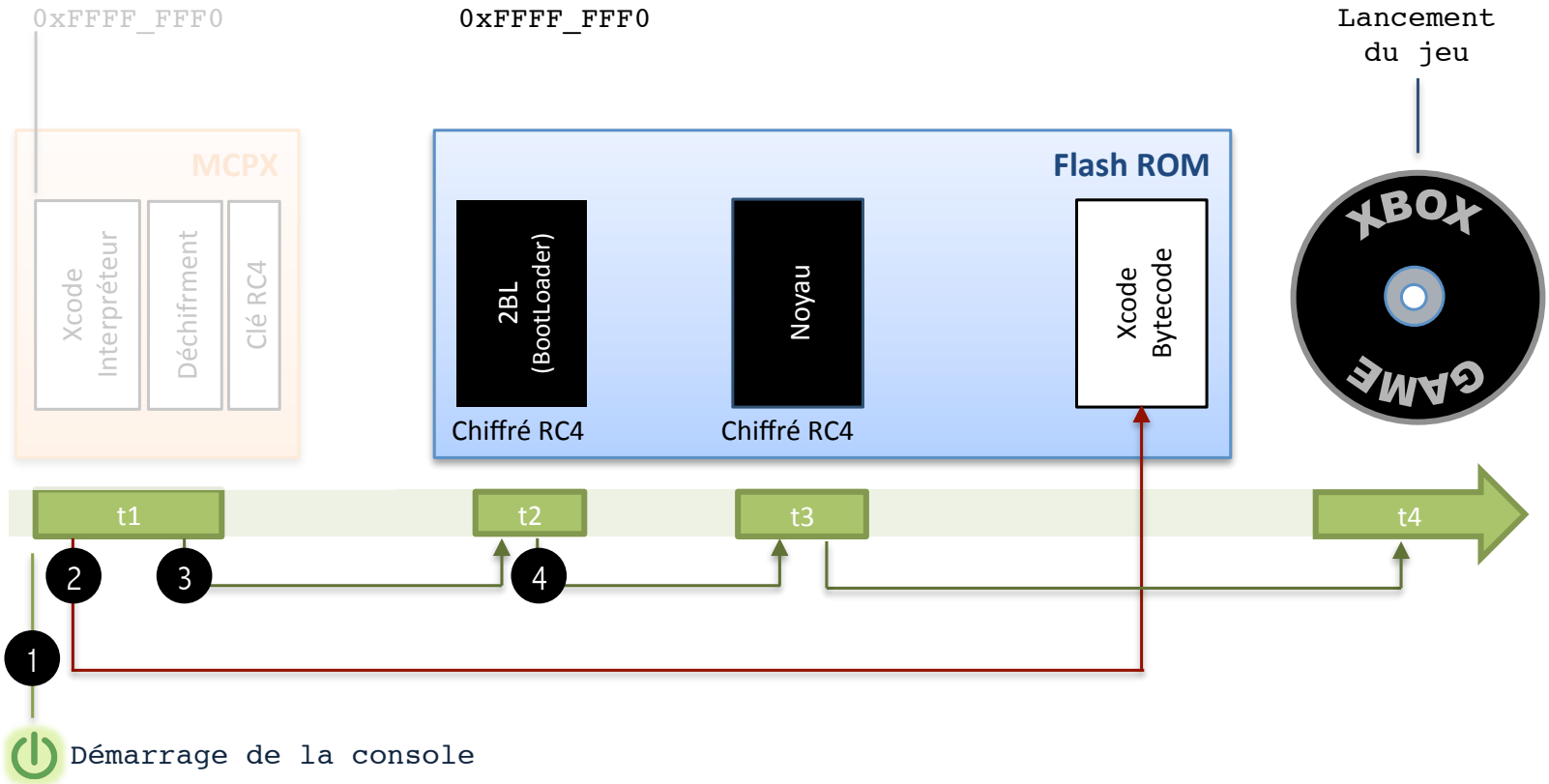
Xbox : chaîne de démarrage de confiance



Xbox : chaîne de démarrage de confiance



Xbox : chaîne de démarrage de confiance



Xbox : attaques

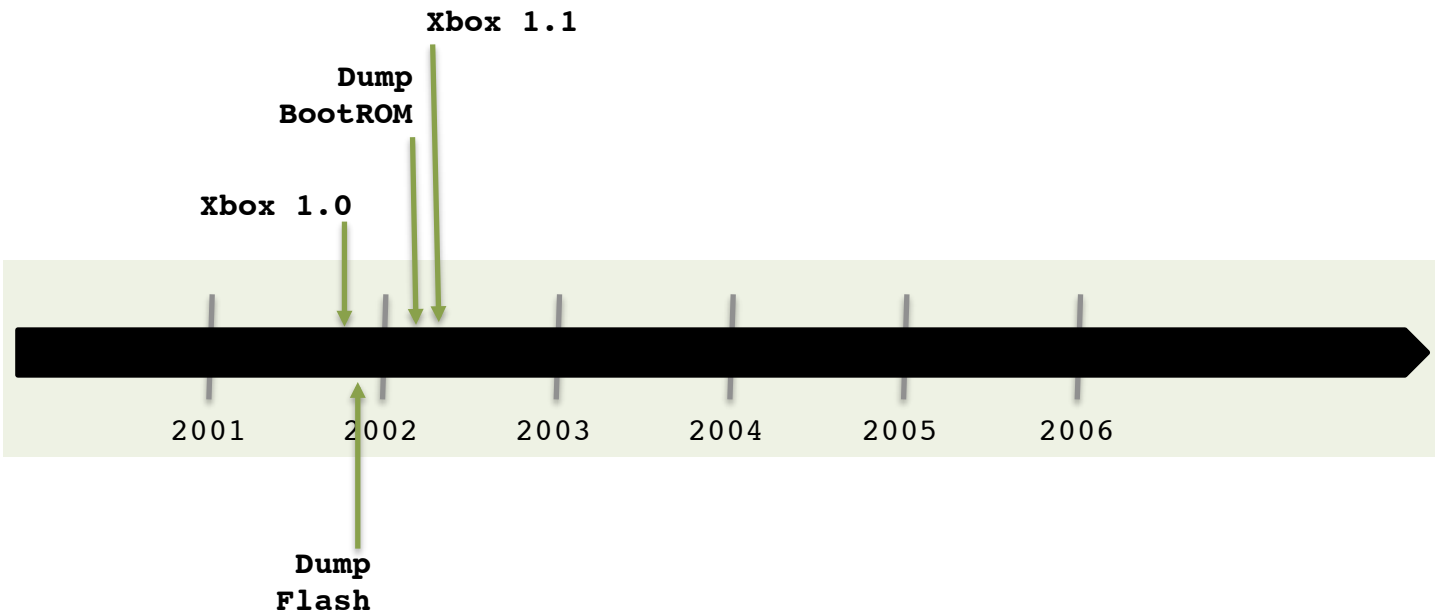
- Sécurité minimum
  - Chaîne de confiance
  - Signature de code
  - DRM

Xbox : attaques

- Sécurité minimum
  - Chaîne de confiance
  - Signature de code
  - DRM
- Objectif :
  - Prendre le contrôle de la plateforme
  - Briser la chaîne de confiance

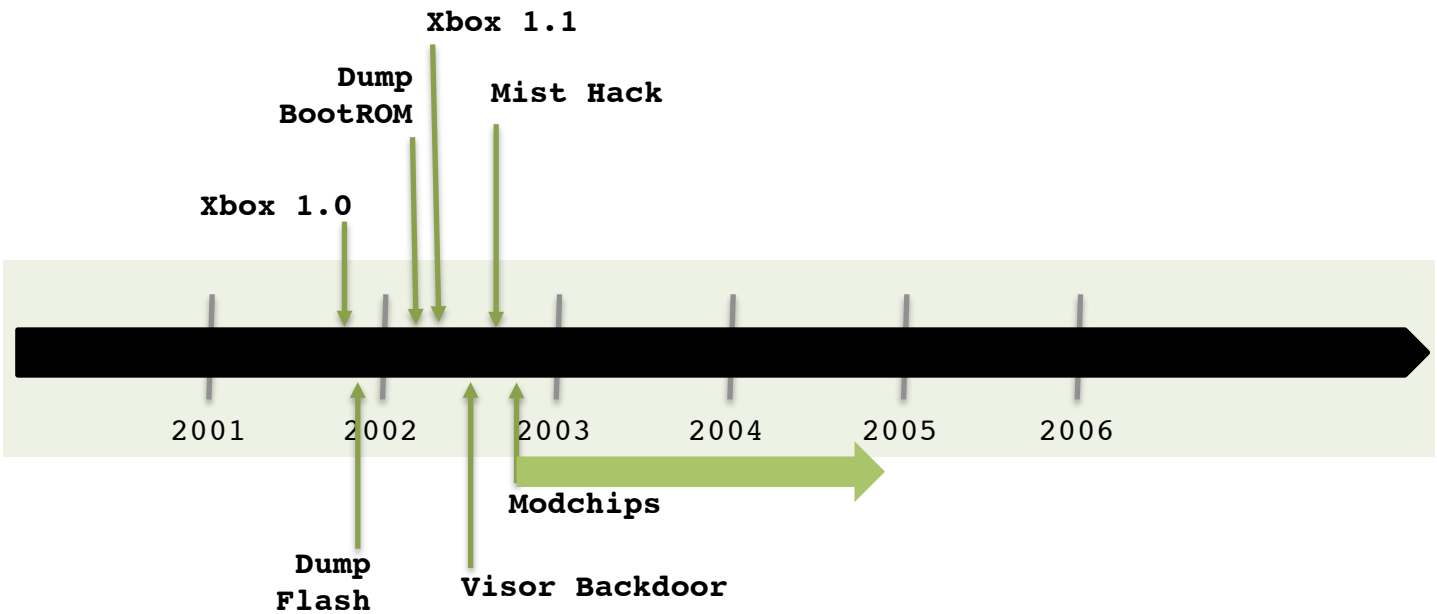
Xbox : attaques

- Sécurité minimum
  - Chaîne de confiance
  - Signature de code
  - DRM
- Objectif :
  - Prendre le contrôle de la plateforme
  - Briser la chaîne de confiance



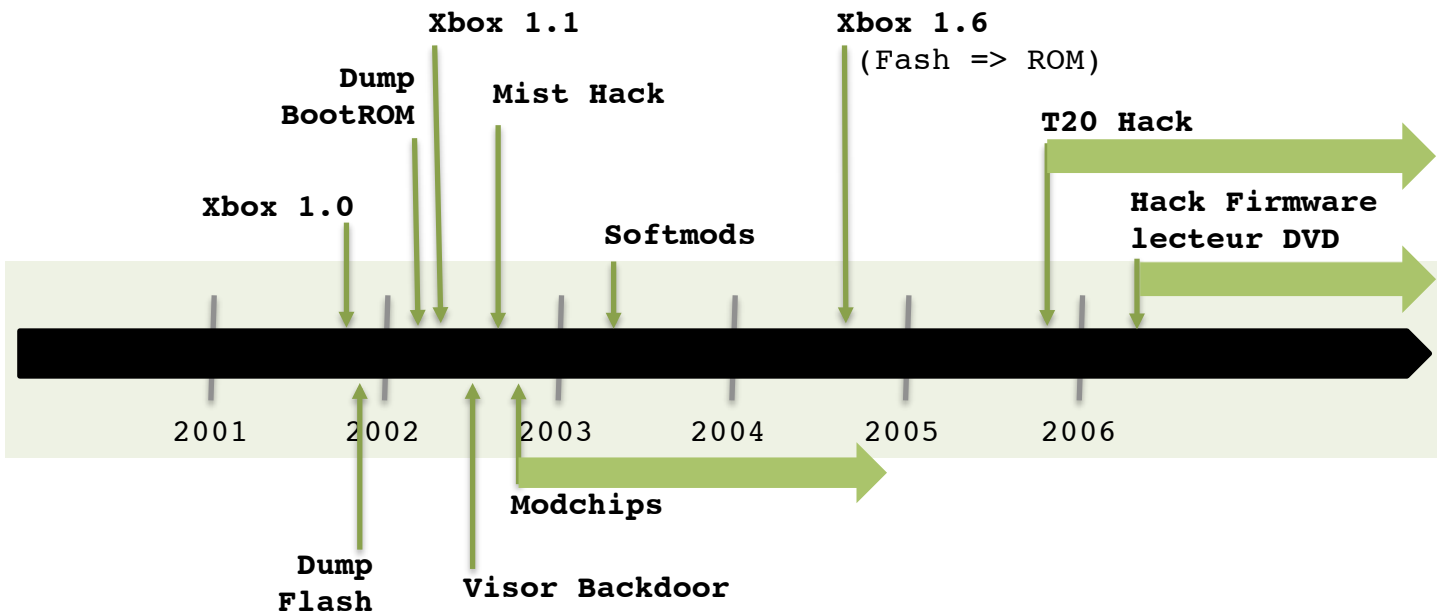
Xbox : attaques

- Sécurité minimum
  - Chaîne de confiance
  - Signature de code
  - DRM
- Objectif :
  - Prendre le contrôle de la plateforme
  - Briser la chaîne de confiance

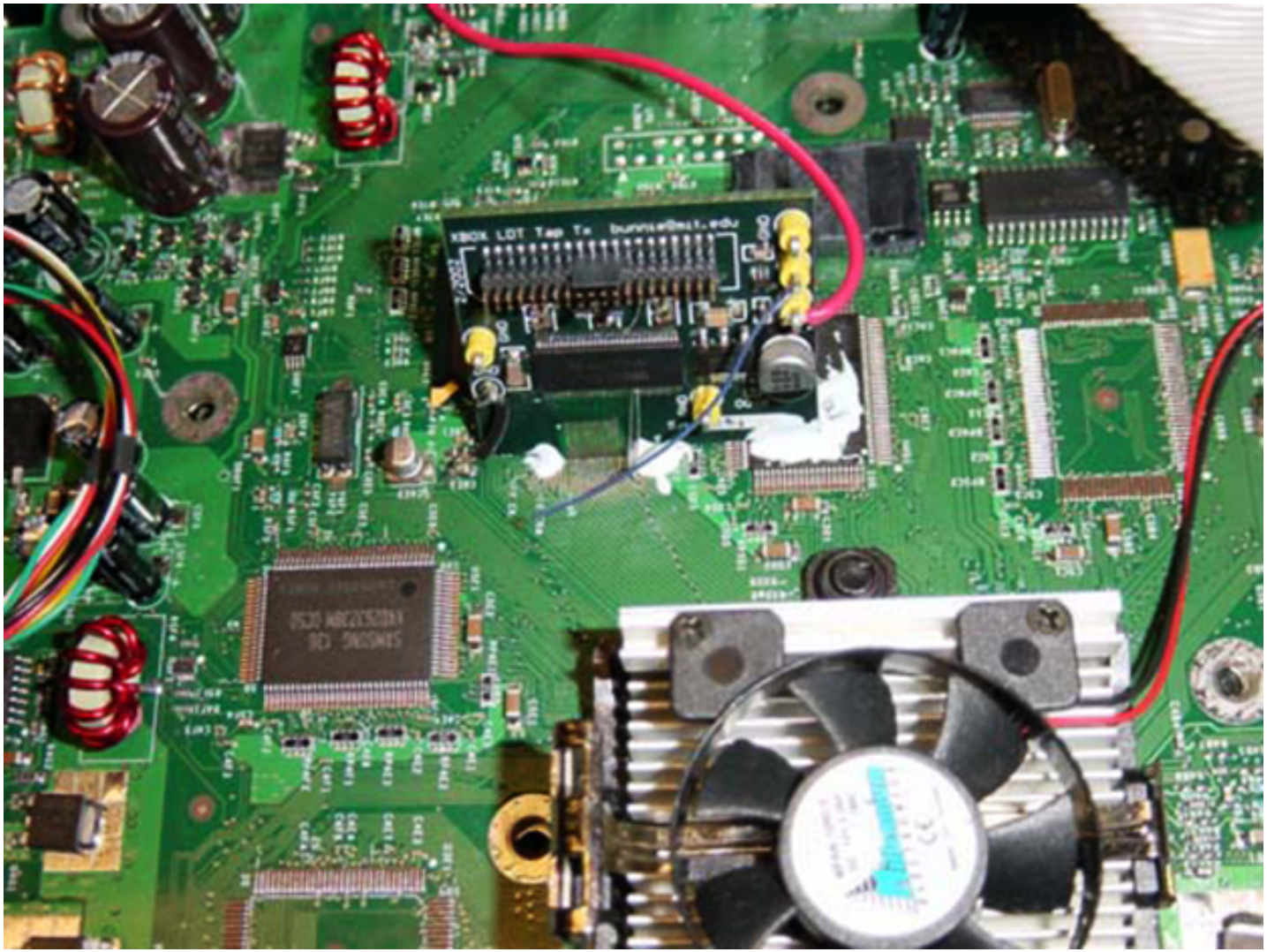


Xbox : attaques

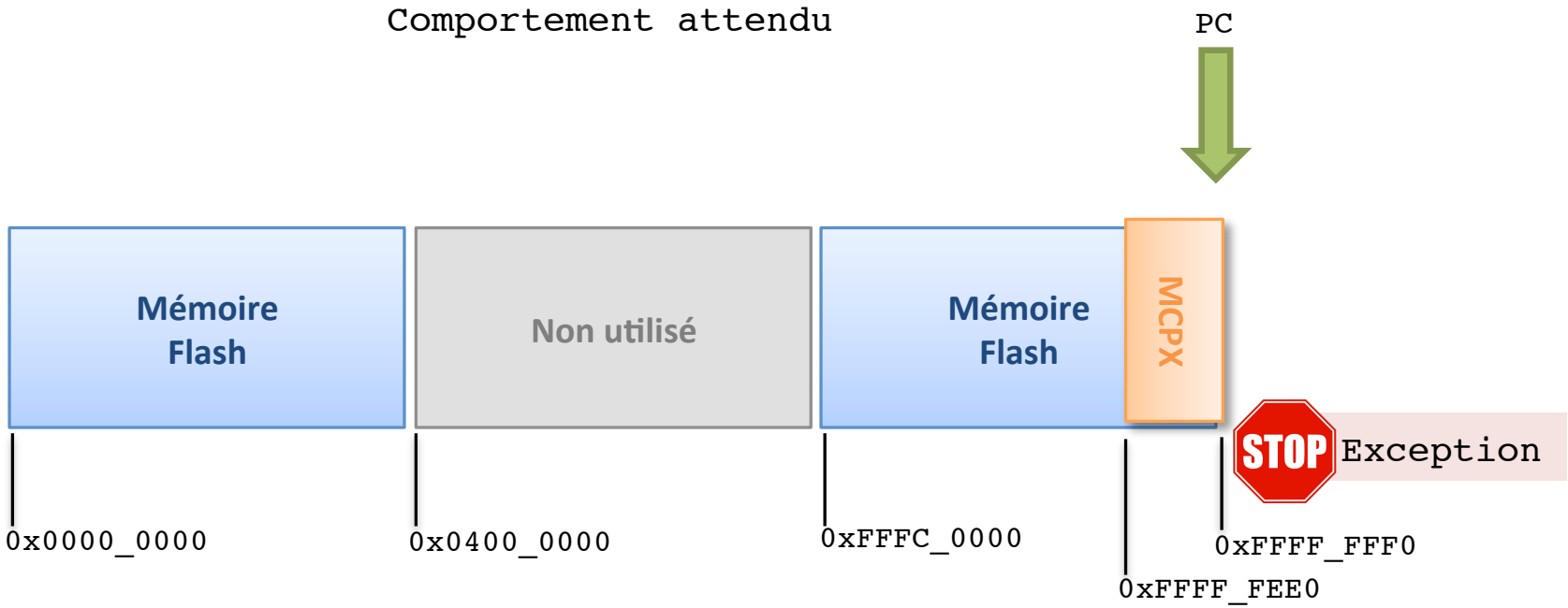
- Sécurité minimum
  - Chaîne de confiance
  - Signature de code
  - DRM
- Objectif :
  - Prendre le contrôle de la plateforme
  - Briser la chaîne de confiance



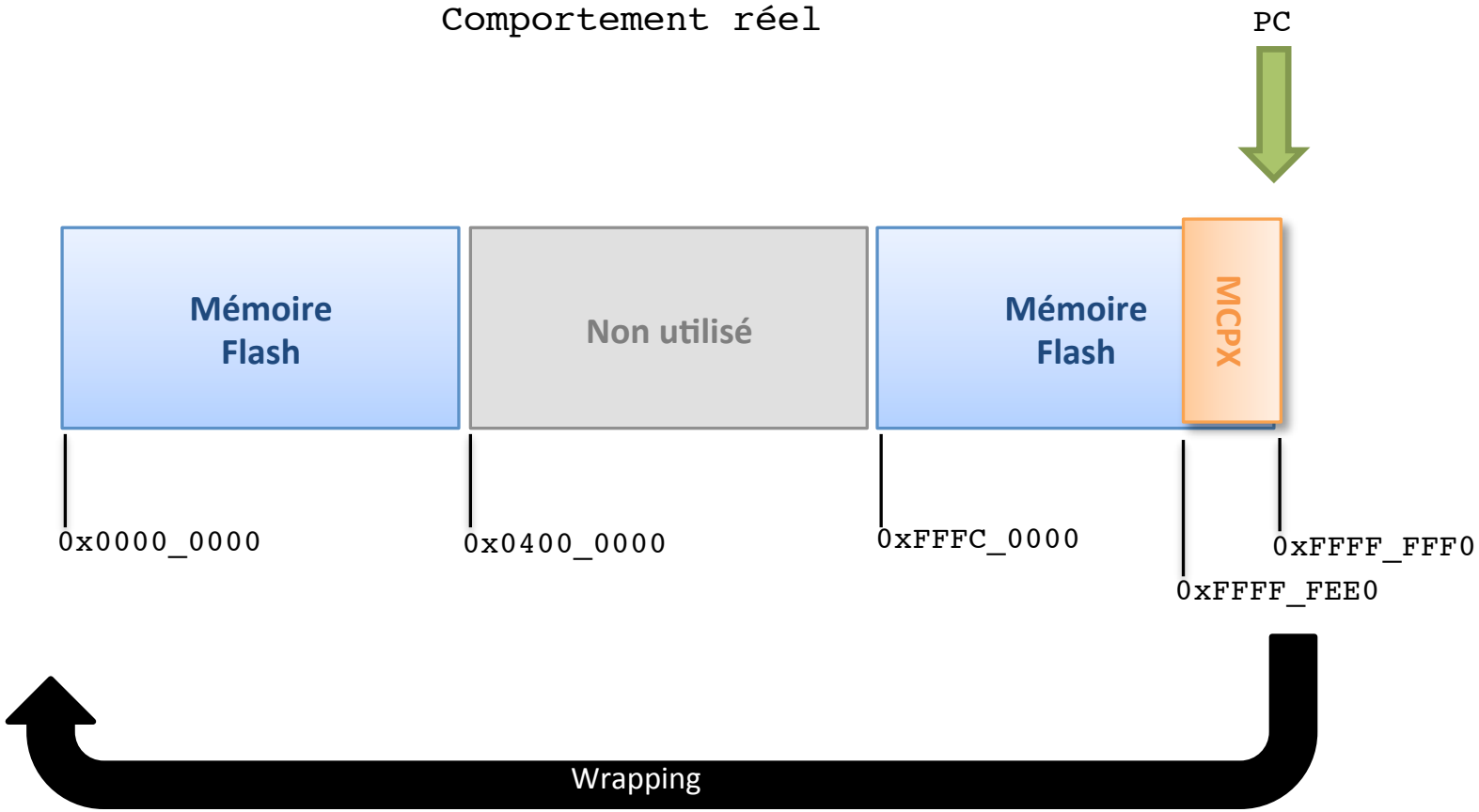
Xbox : écoute du bus hypertransport



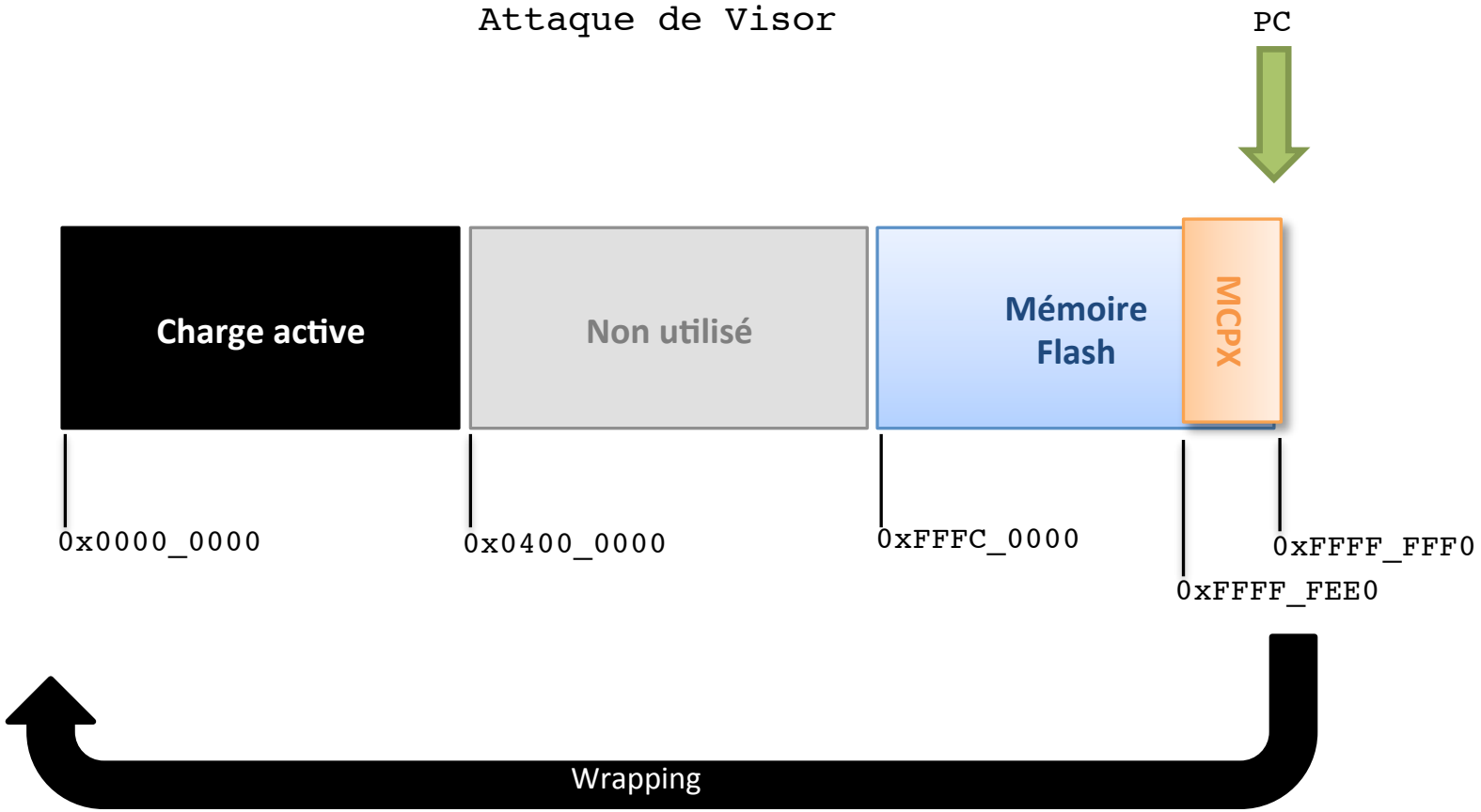
Xbox : Visor backdoor - vulnérabilité



Xbox : Visor backdoor - vulnérabilité



Xbox : Visor backdoor - vulnérabilité



Xbox : conclusion

- Tentative d'intégration d'une racine de confiance

Xbox : conclusion

- Tentative d'intégration d'une racine de confiance
- Limitation de la taille de la ROM
  - Déterminant pour la sécurité
- Plusieurs vulnérabilités dans 512 octets de code
- Sécurité complètement compromise

Choose your player

Skill Level

Can I play, Daddy?

Don't hurt me.

Bring 'em on!

I am Death incarnate!

Choose your player

Xbox 360

Skill Level

Can I play, Daddy?

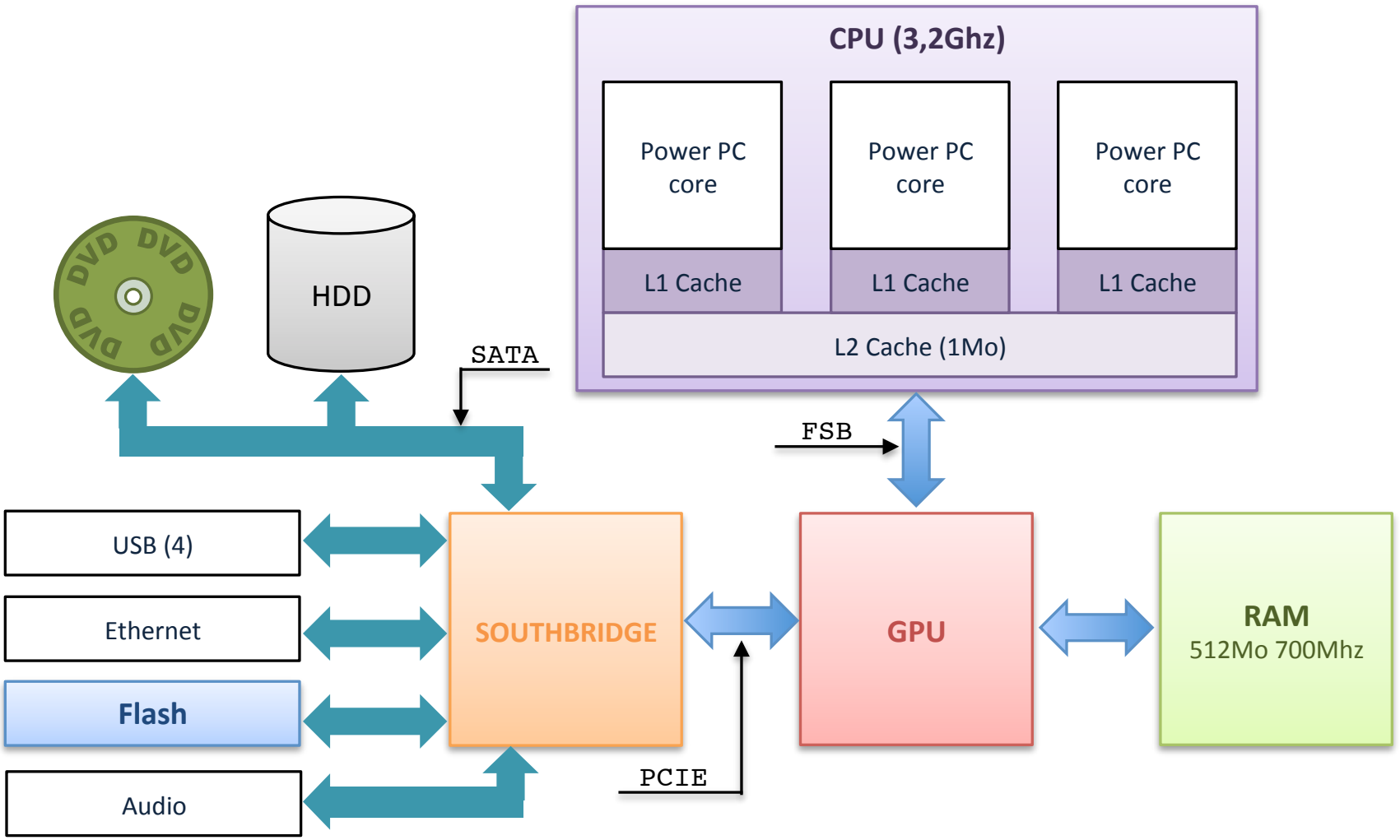
Don't hurt me.

Bring 'em on!

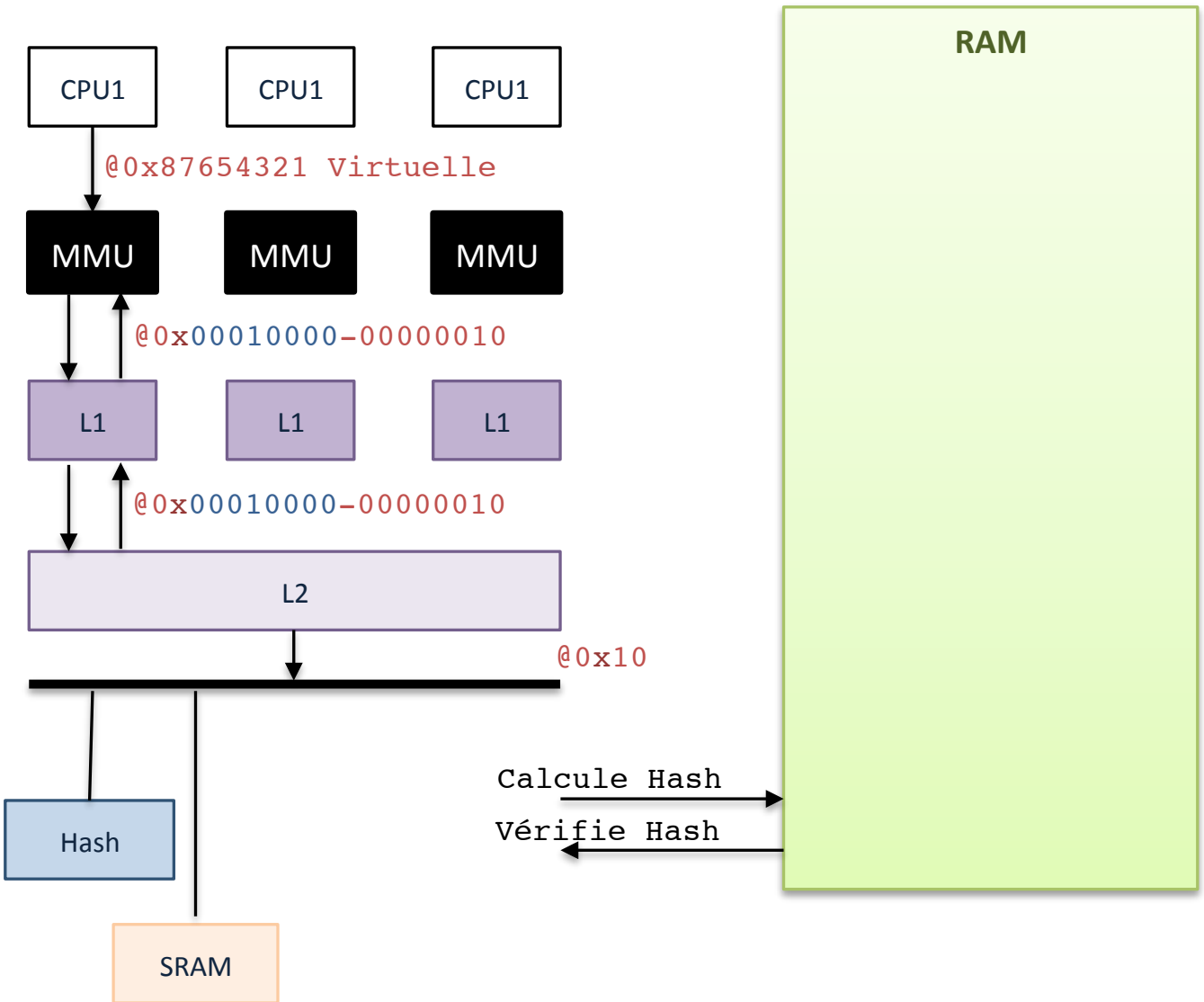
I am Death incarnate!

Xbox 360 : architecture matérielle

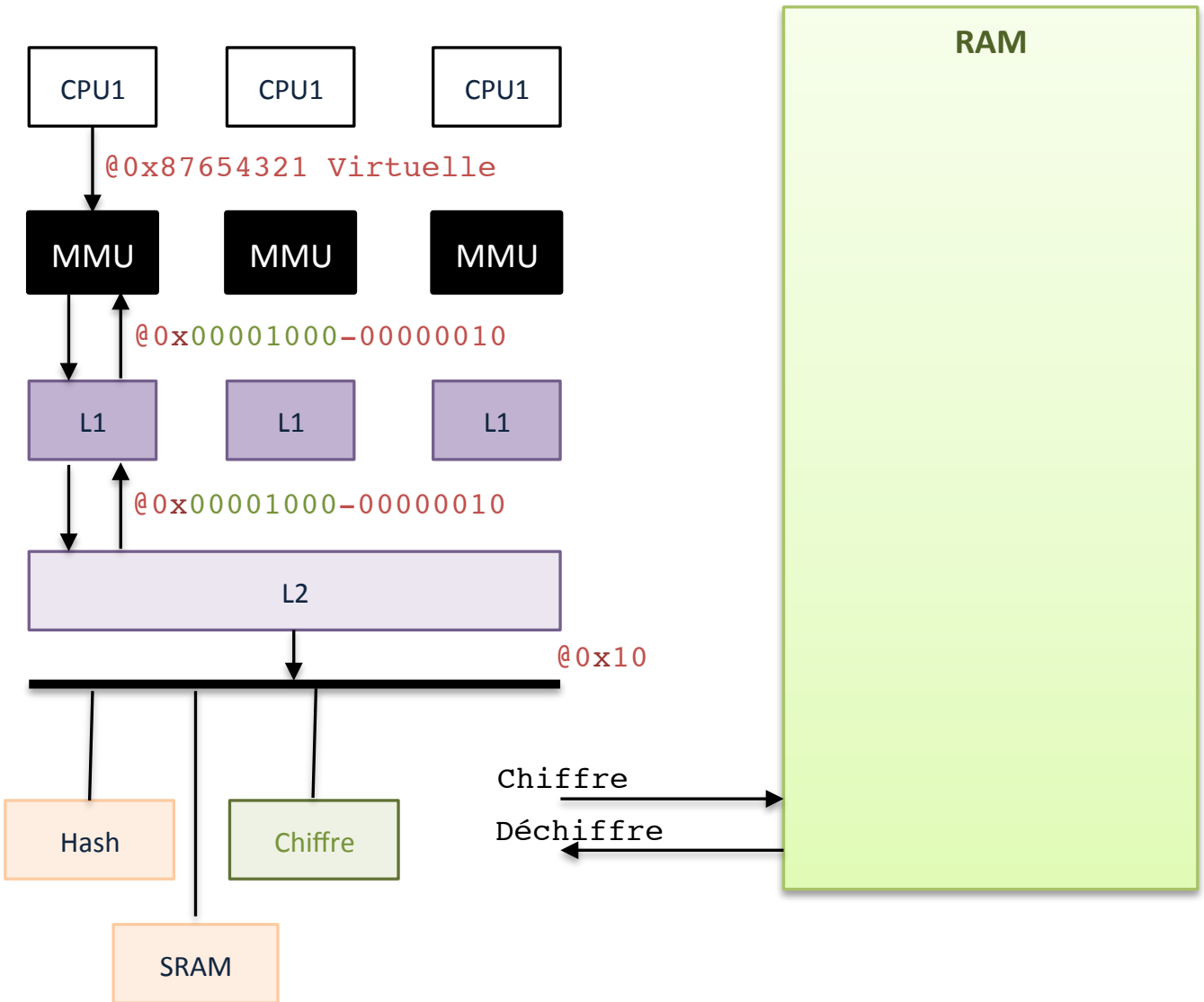
- Architecture PowerPC 64-bit tri-cœur, proche d'un PC



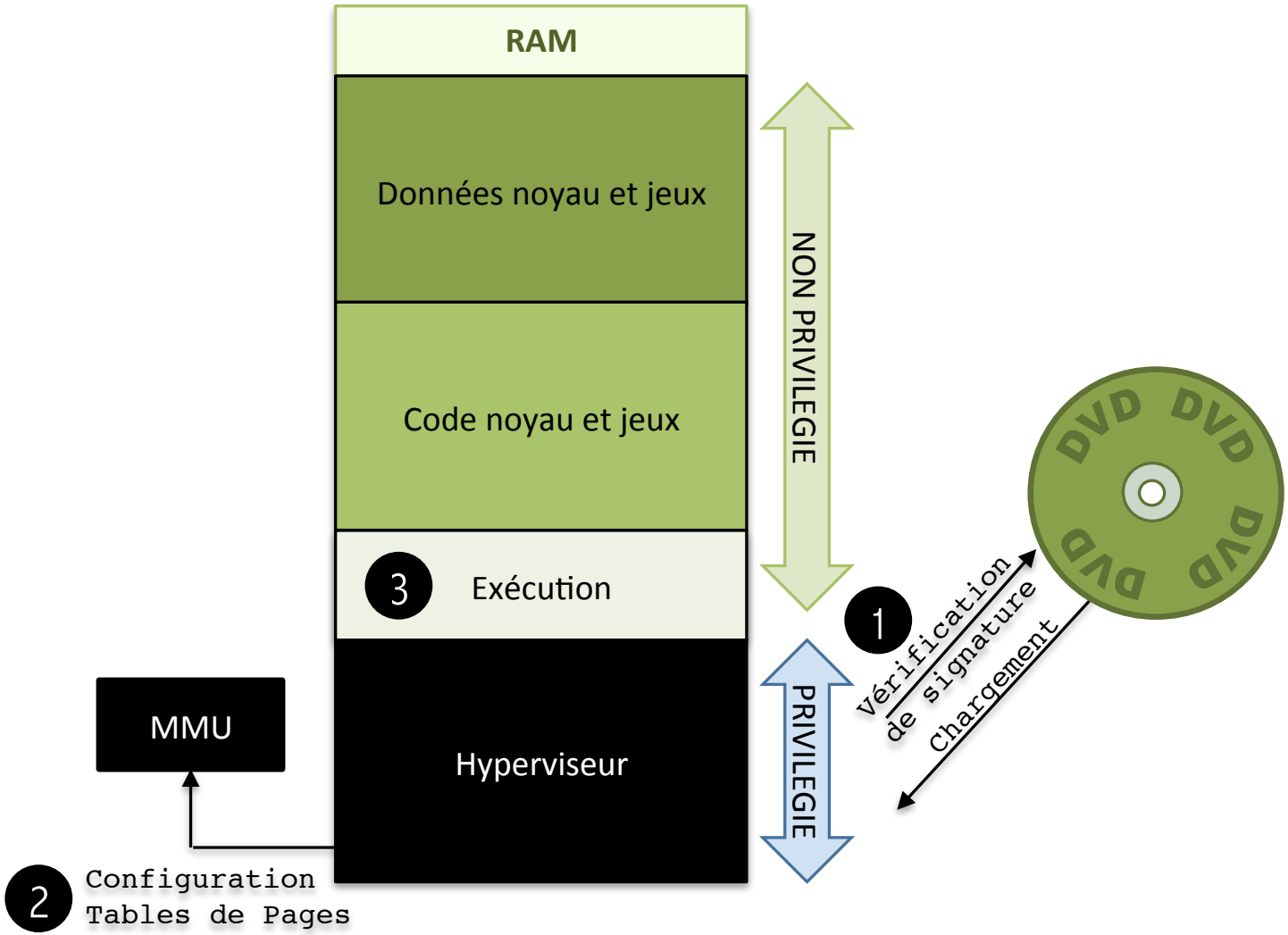
Xbox 360 : coprocesseur cryptographique



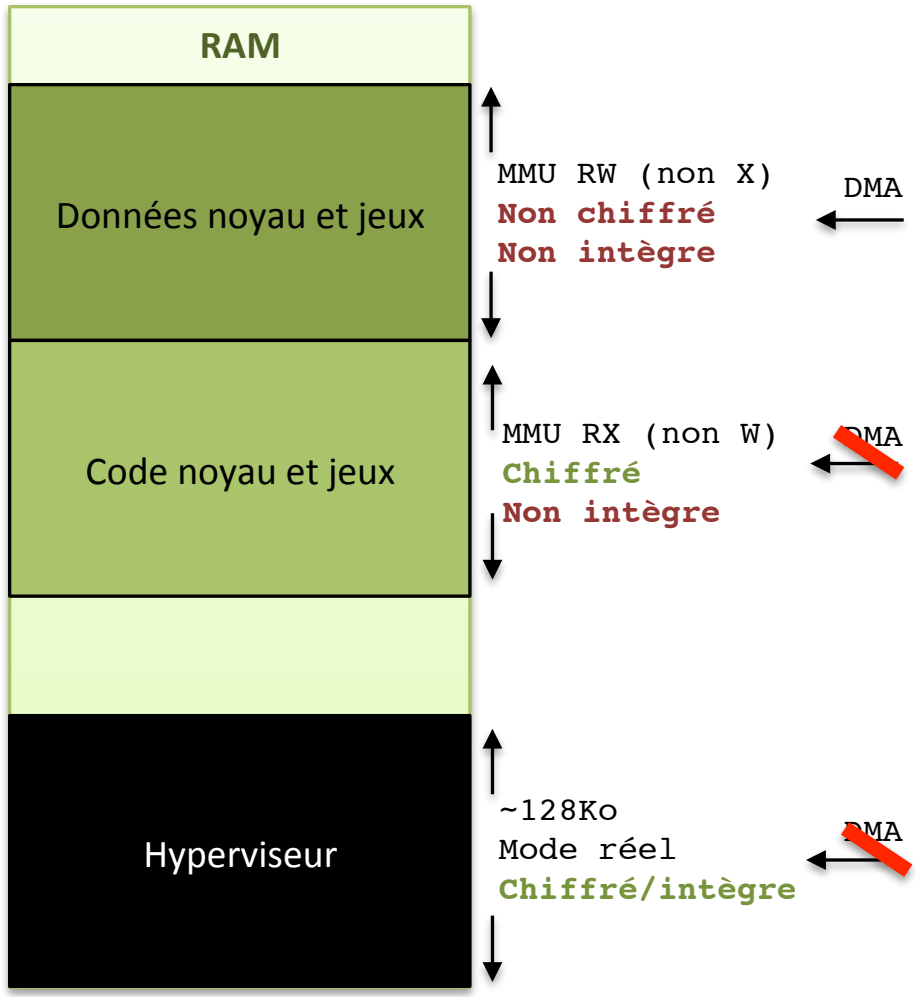
Xbox 360 : coprocesseur cryptographique



Xbox 360 : architecture logicielle

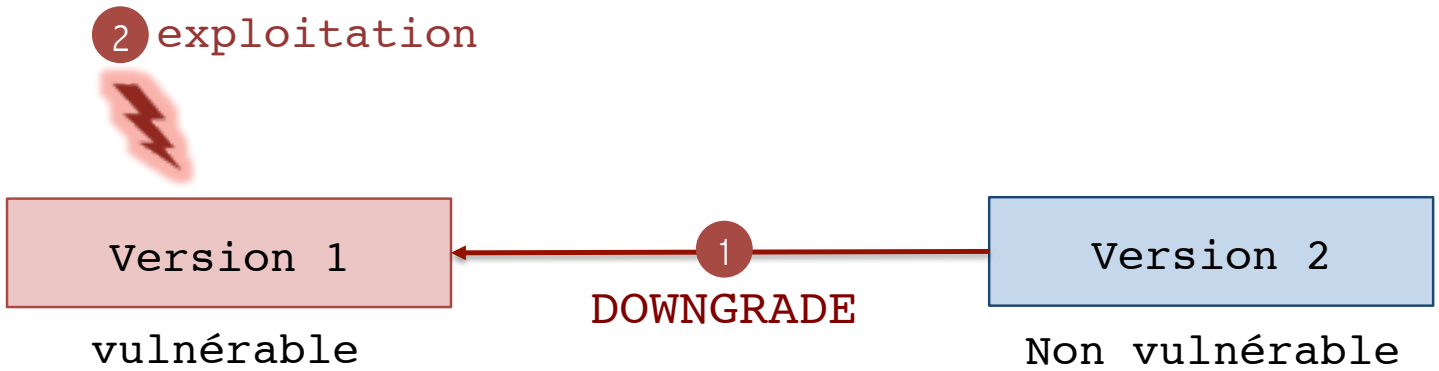


Xbox 360 : modèle de sécurité



Xbox 360 : anti-downgrade

- **Downgrade** : diminuer le niveau de version du système de la console pour exploiter une faille présente dans un ancien firmware



Xbox 360 : anti-downgrade

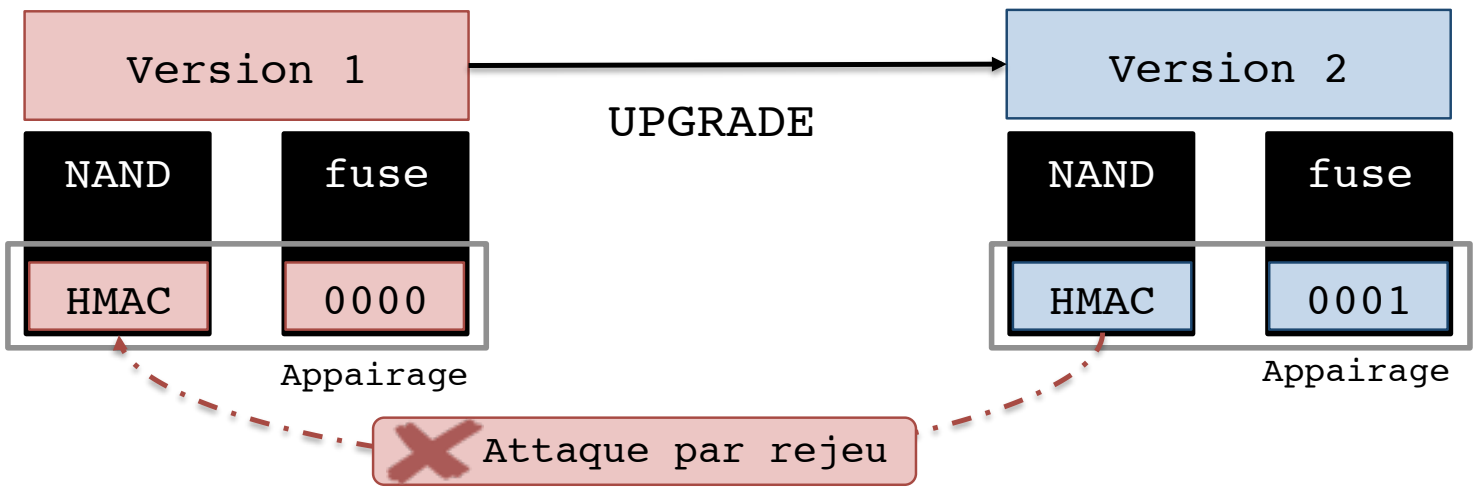
- **Downgrade** : diminuer le niveau de version du système de la console pour exploiter une faille présente dans un ancien firmware
- Nécessité de détecter cela : utilisation de **eFuses** matériels dans le CPU
  - Fonctionnement : 

Xbox 360 : anti-downgrade

- **Downgrade** : diminuer le niveau de version du système de la console pour exploiter une faille présente dans un ancien firmware
- Nécessité de détecter cela : utilisation de **eFuses** matériels dans le CPU
  - Les fuses servent aussi à générer une **clé CPU** de 128 bits propre à chaque console

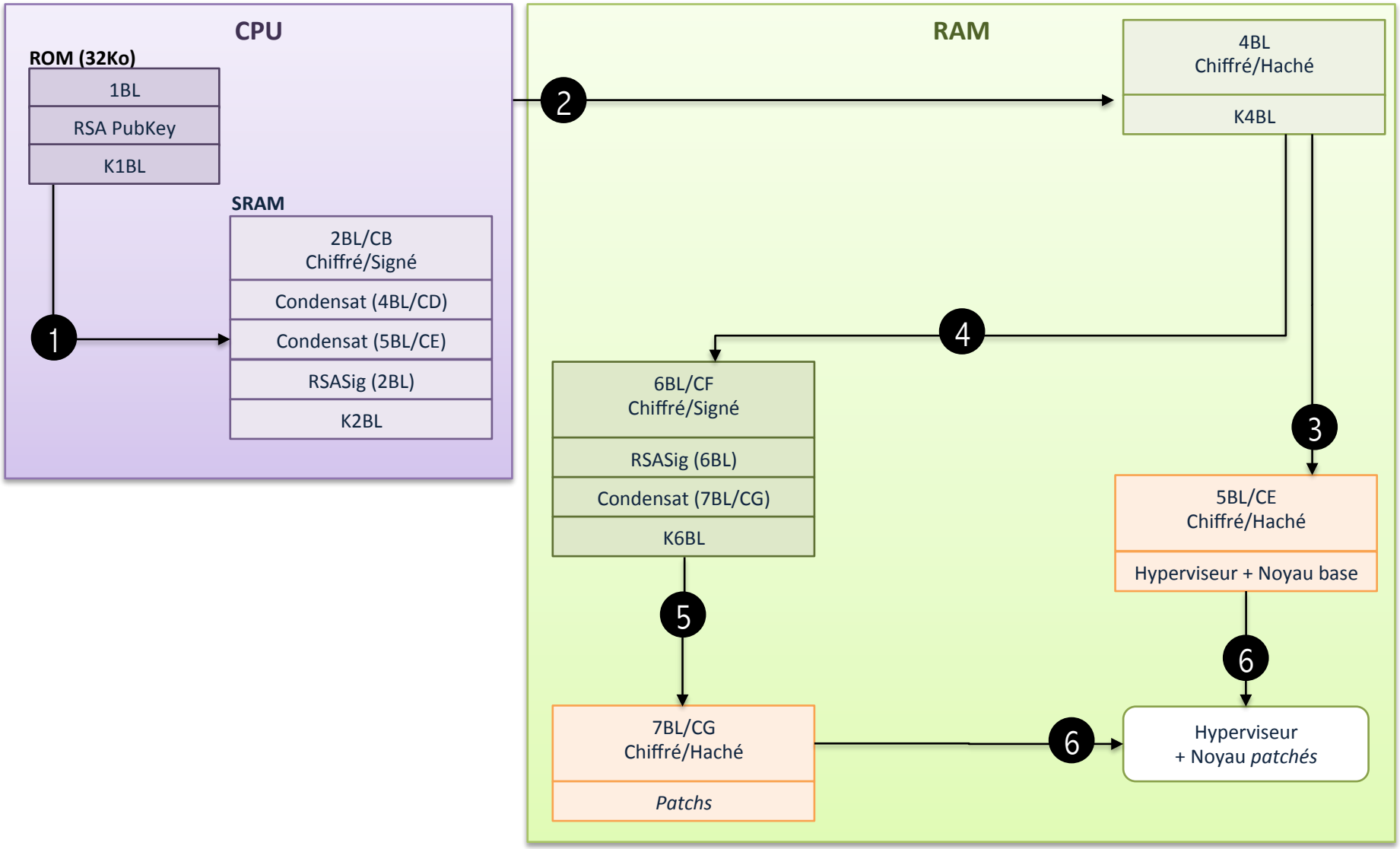
Xbox 360 : anti-downgrade

- **Downgrade** : diminuer le niveau de version du système de la console pour exploiter une faille présente dans un ancien firmware
- Nécessité de détecter cela : utilisation de **eFuses** matériels dans le CPU
  - Fuse grillé à chaque mise à jour
  - Appairage HMAC avec **utilise la clé CPU secrète** en NAND



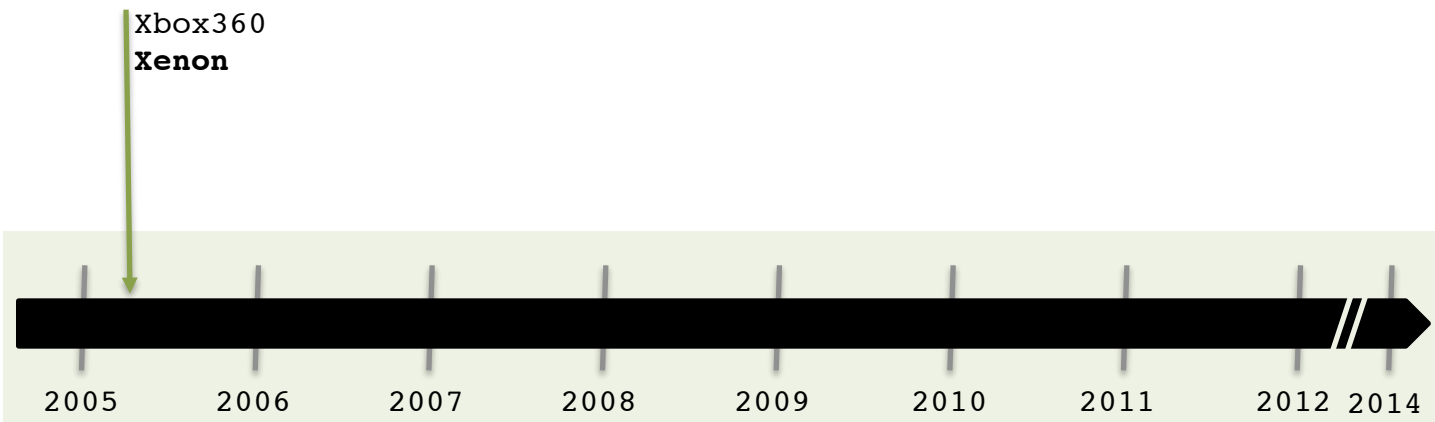
Xbox 360 : démarrage sécurisé

Xbox 360 : démarrage sécurisé



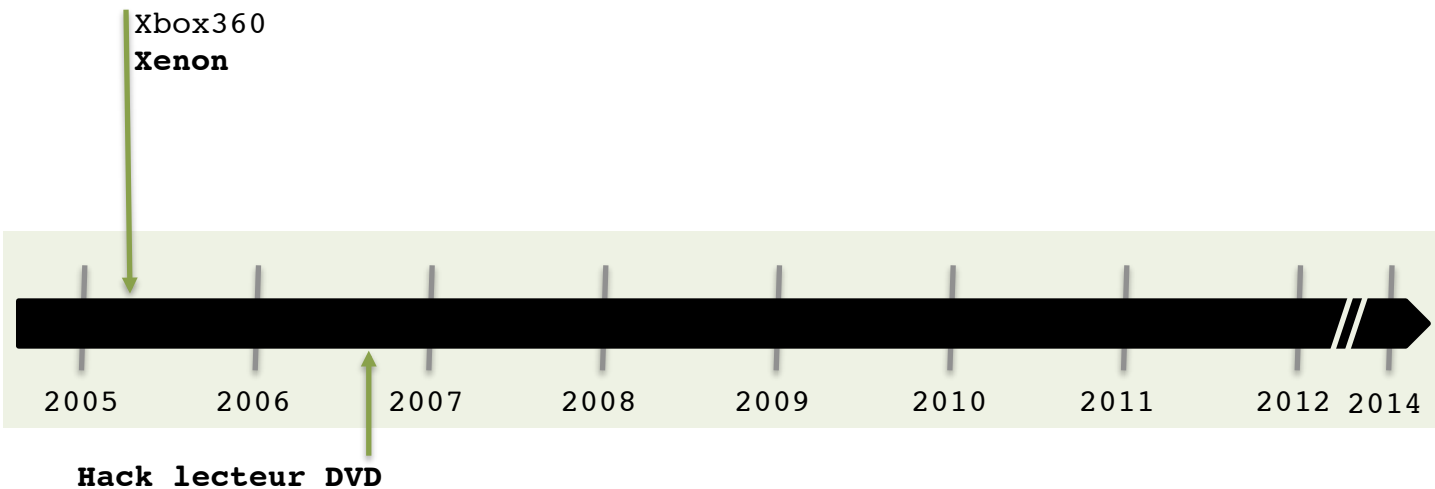
Xbox 360 : historique des attaques

- Sortie de la Xbox 360



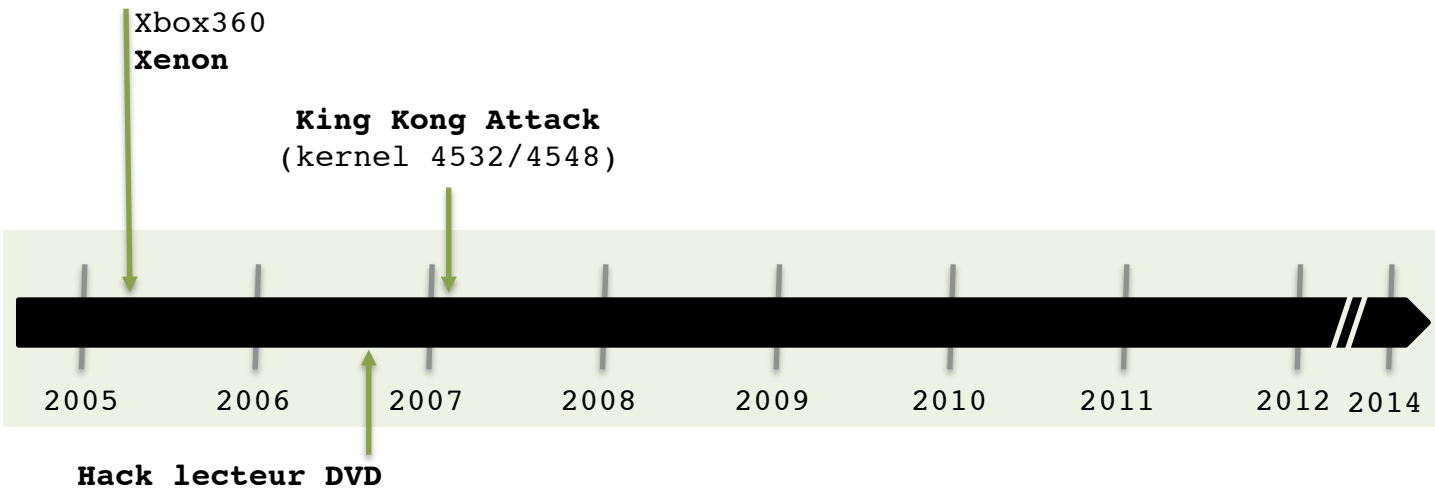
Xbox 360 : historique des attaques

- Piratage des jeux possible



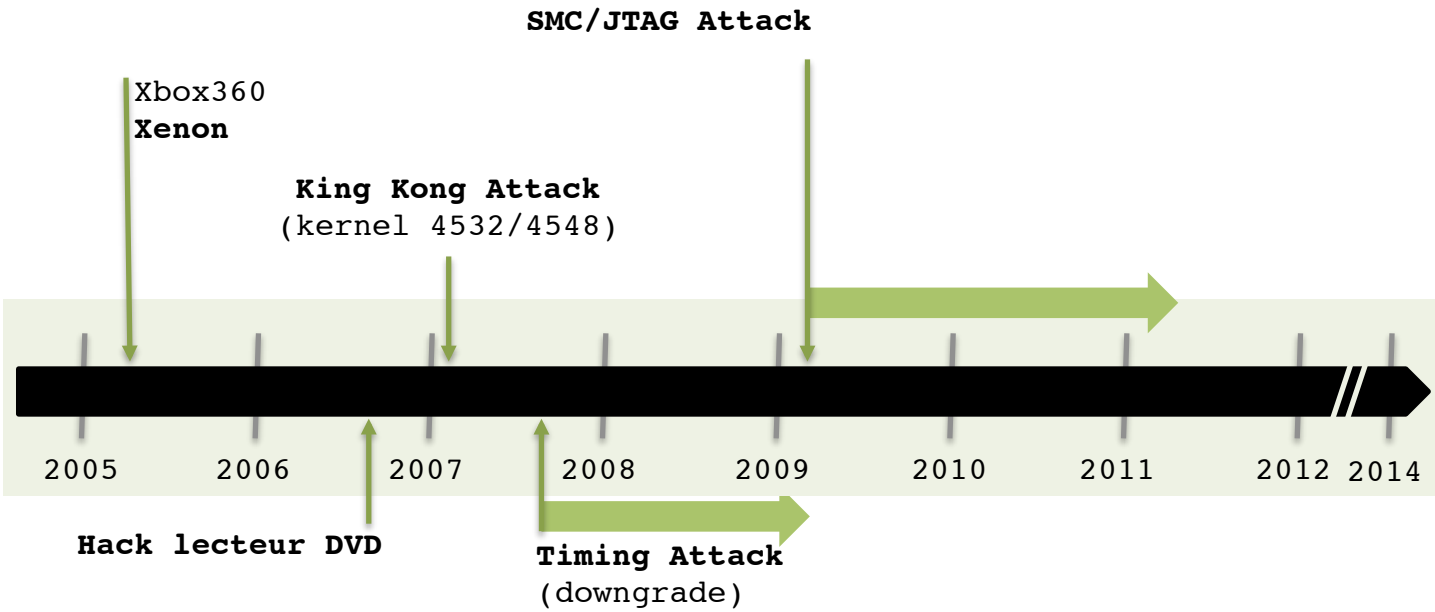
Xbox 360 : historique des attaques

- Première exploitation logicielle (élévation de privilèges hyperviseur)



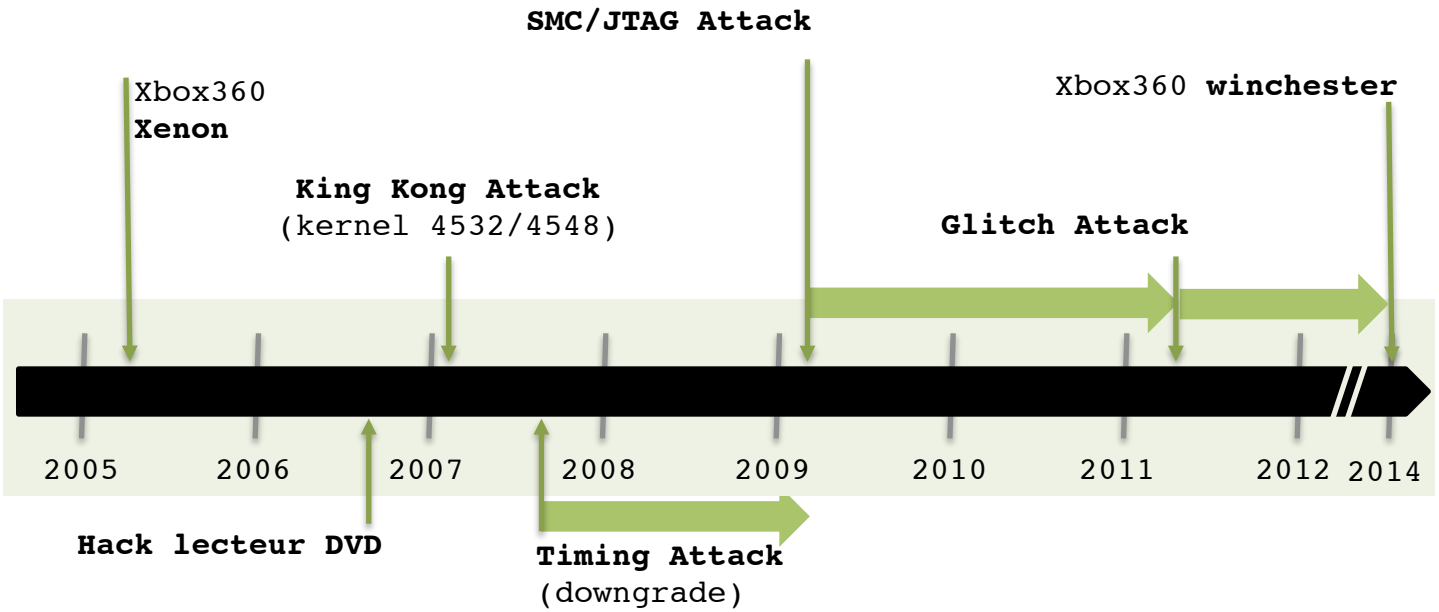
Xbox 360 : historique des attaques

- Downgrade pour exploiter la King Kong attack



Xbox 360 : historique des attaques

- Glitch matériel permettant d'outrepasser le boot sécurisé



Xbox 360 : la King Kong attack

- Première attaque : logicielle, la **King Kong Attack**

Xbox 360 : la King Kong attack

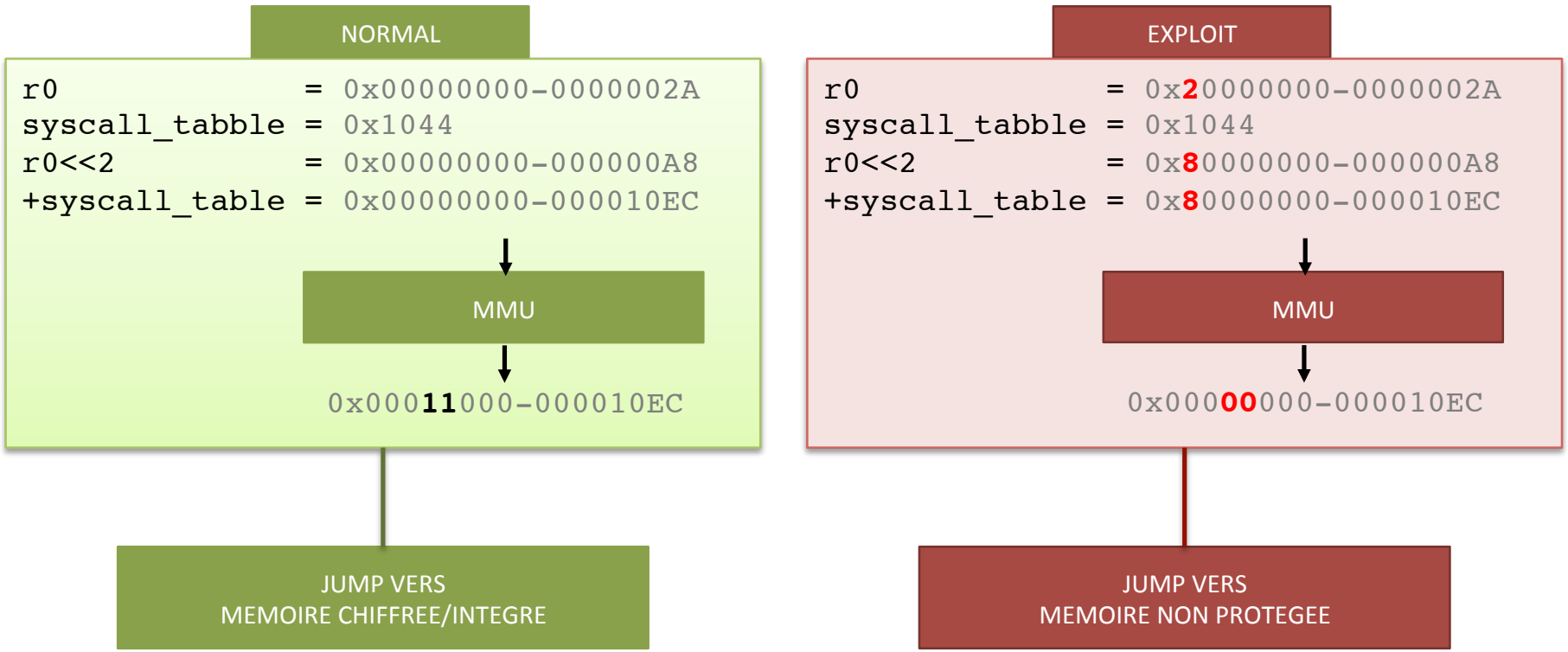
- Première attaque : logicielle, la **King Kong Attack**
- Erreur de comparaison entière dans gestion des appels systèmes (syscalls handler)

PSEUDO CODE C

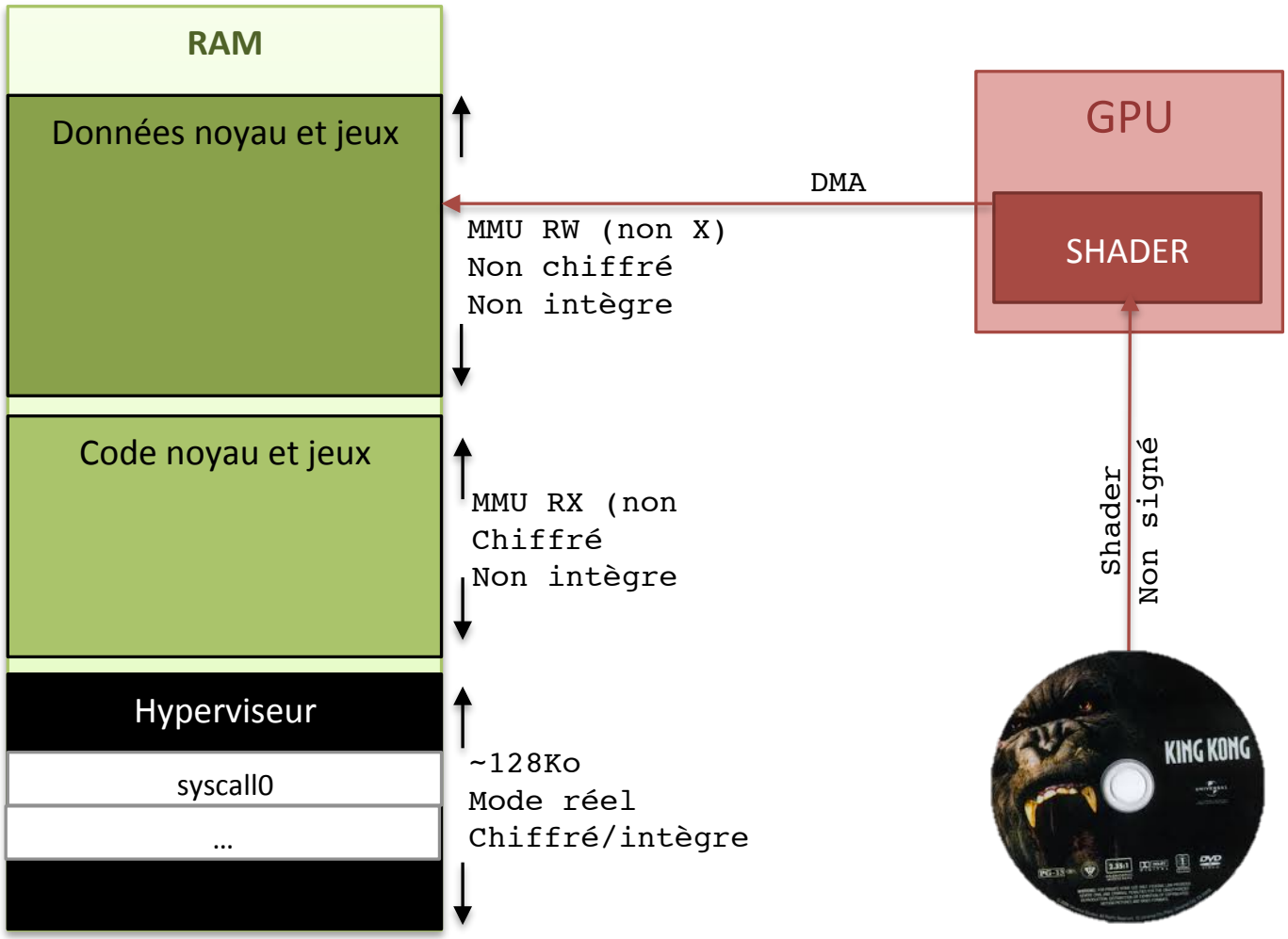
```
extern u32 syscall_table[0x61]

void syscall_handler(r0, r3, r4, …) {

    if((u32)r0 >= 0x61) {
                goto bad_syscall;
    }
    r1 = (void*)syscall_table[(u64)r0];
    r1();
}
```


Xbox 360 : la King Kong attack

- Désactivation de l'intégrité et du chiffrement de RAM



Xbox 360 : la King Kong attack



Xbox 360 : la timing attack

- Problème: la King Kong attack a été patchée avant d'être rendue publique

Xbox 360 : la timing attack

- Problème: la King Kong attack a été patchée avant d'être rendue publique
- Objectif: downgrade vers le noyau vulnérable à la King Kong attack

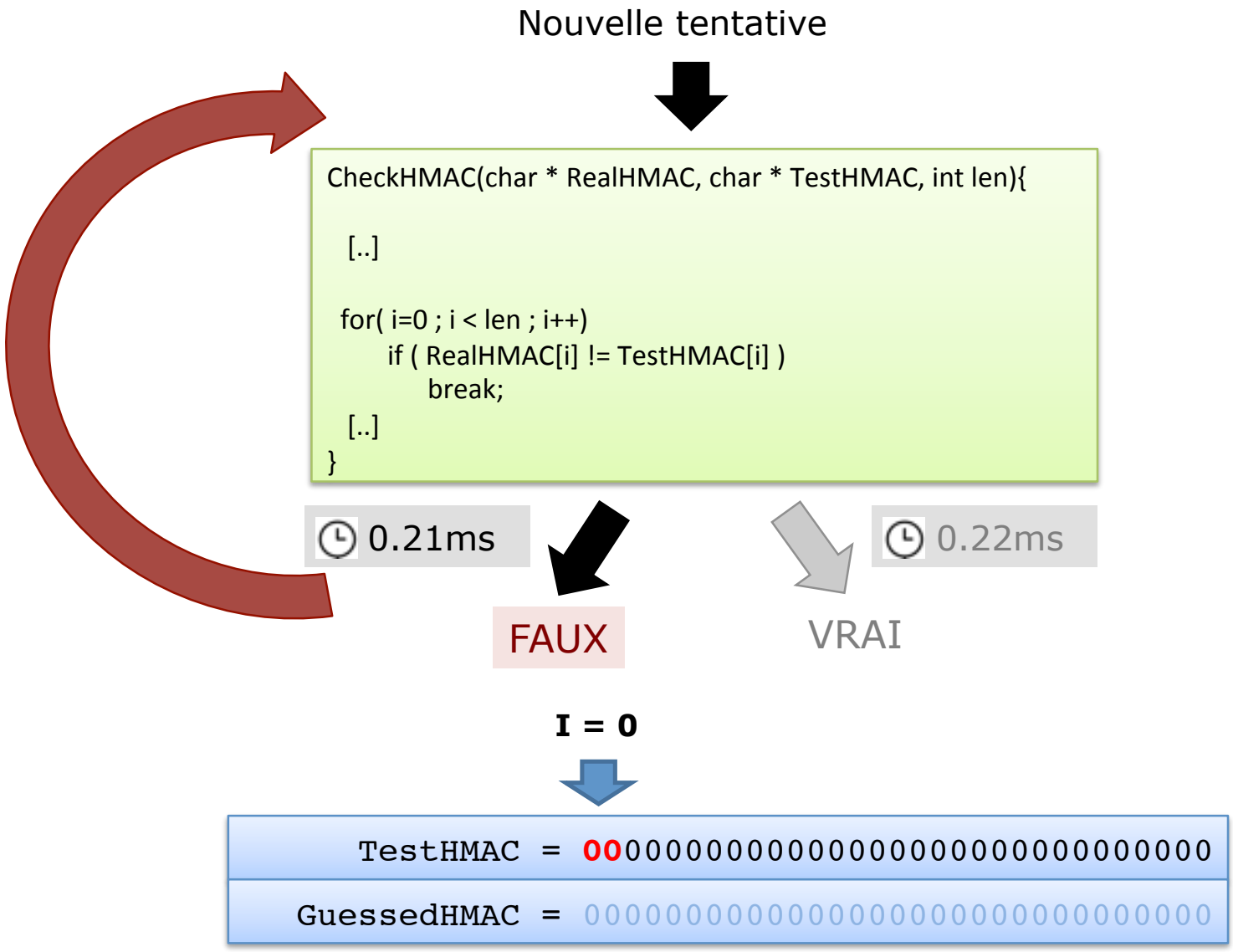
Xbox 360 : la timing attack

- Problème: la King Kong attack a été patchée avant d'être rendue publique
- Objectif: downgrade vers le noyau vulnérable à la King Kong attack
- Utilisation d'un **memcmp** à temps non constant dans le 2BL pour la vérification du HMAC d'appairage

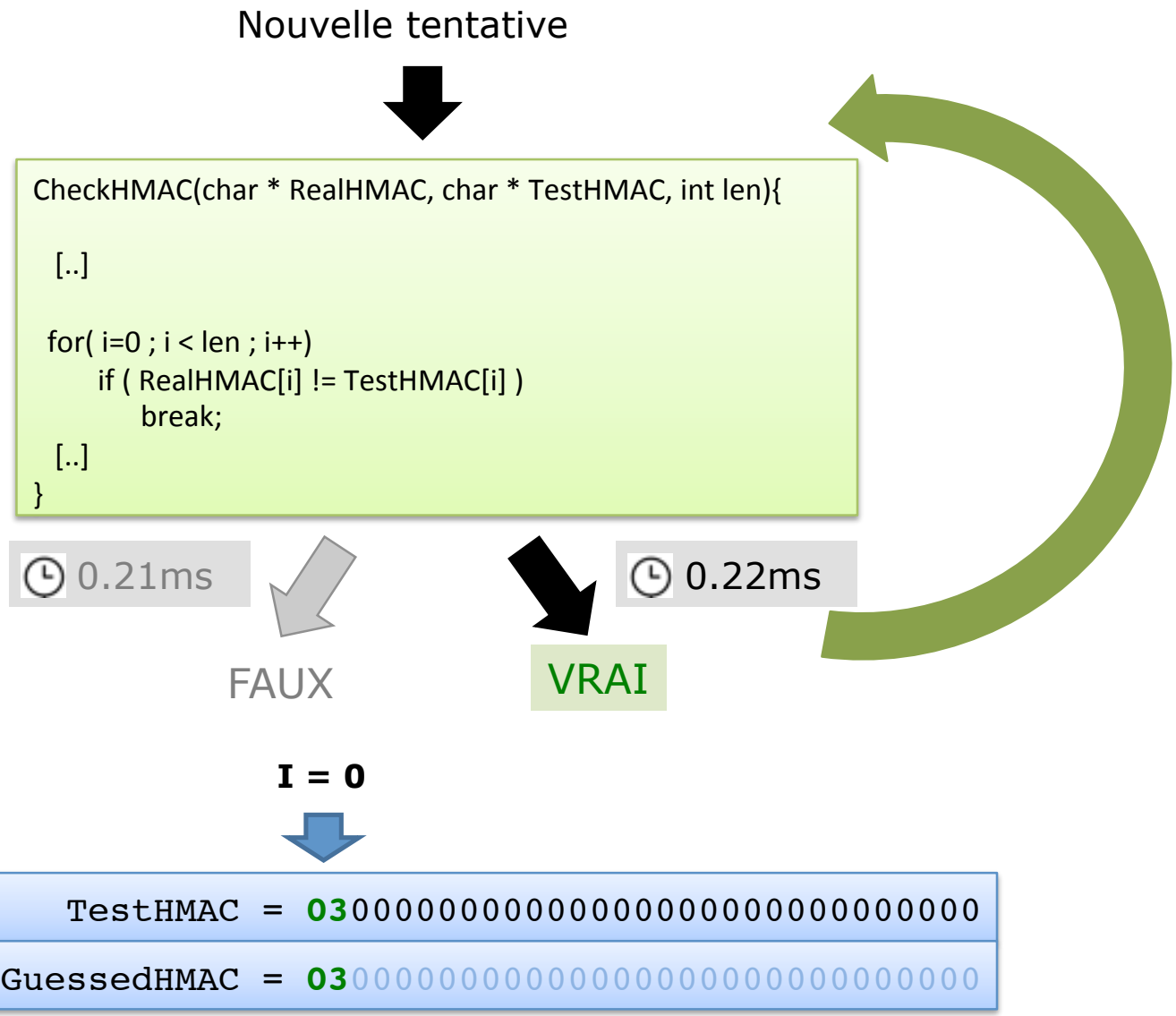
Xbox 360 : la timing attack

- Problème: la King Kong attack a été patchée avant d'être rendue publique
- Objectif: downgrade vers le noyau vulnérable à la King Kong attack
- Utilisation d'un **memcmp** à temps non constant dans le 2BL pour la vérification du HMAC d'appairage
- Possibilité de forger un HMAC valide sans connaître la clé CPU

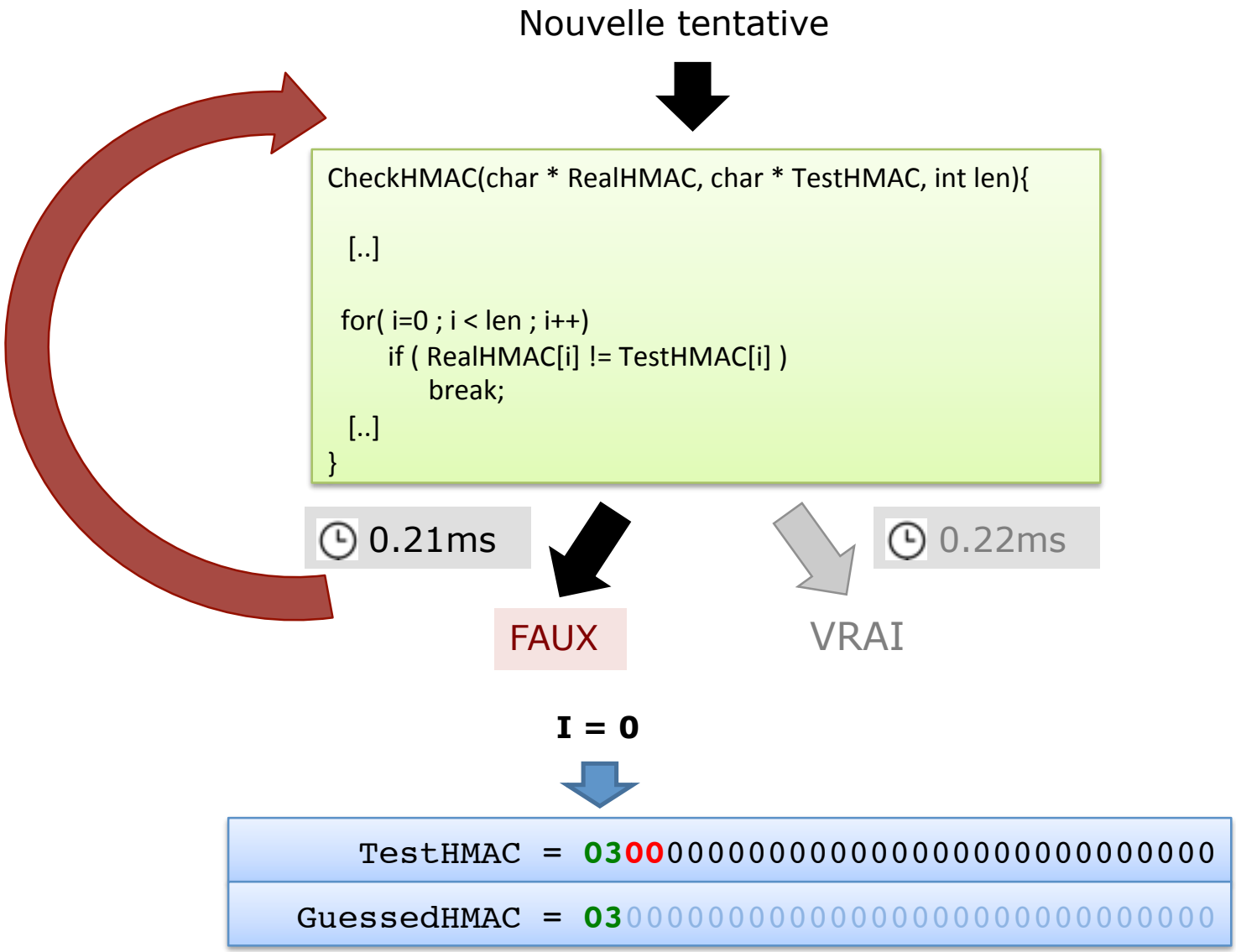
Xbox 360 : la timing attack



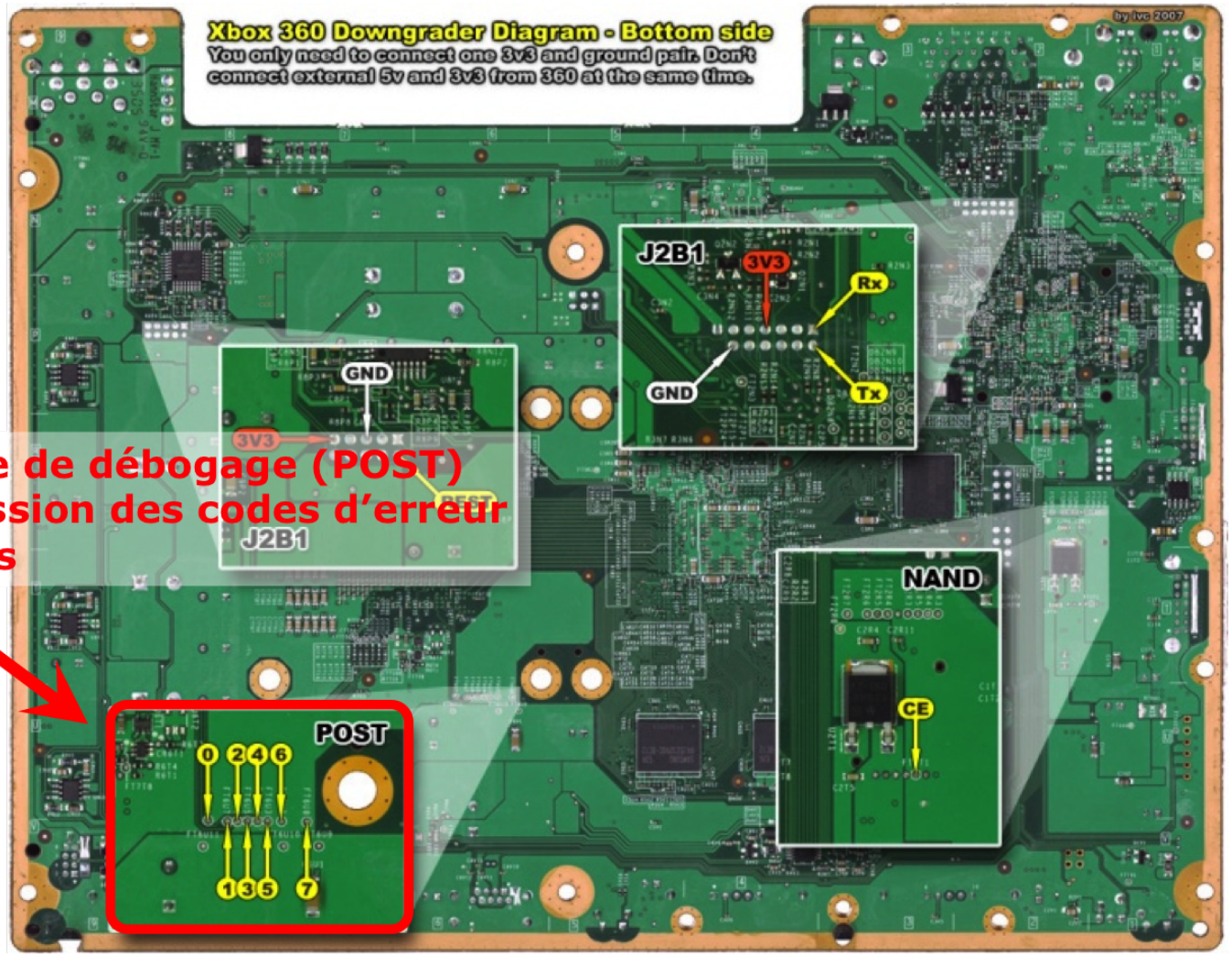
Xbox 360 : la timing attack



Xbox 360 : la timing attack



Xbox 360 : la timing attack

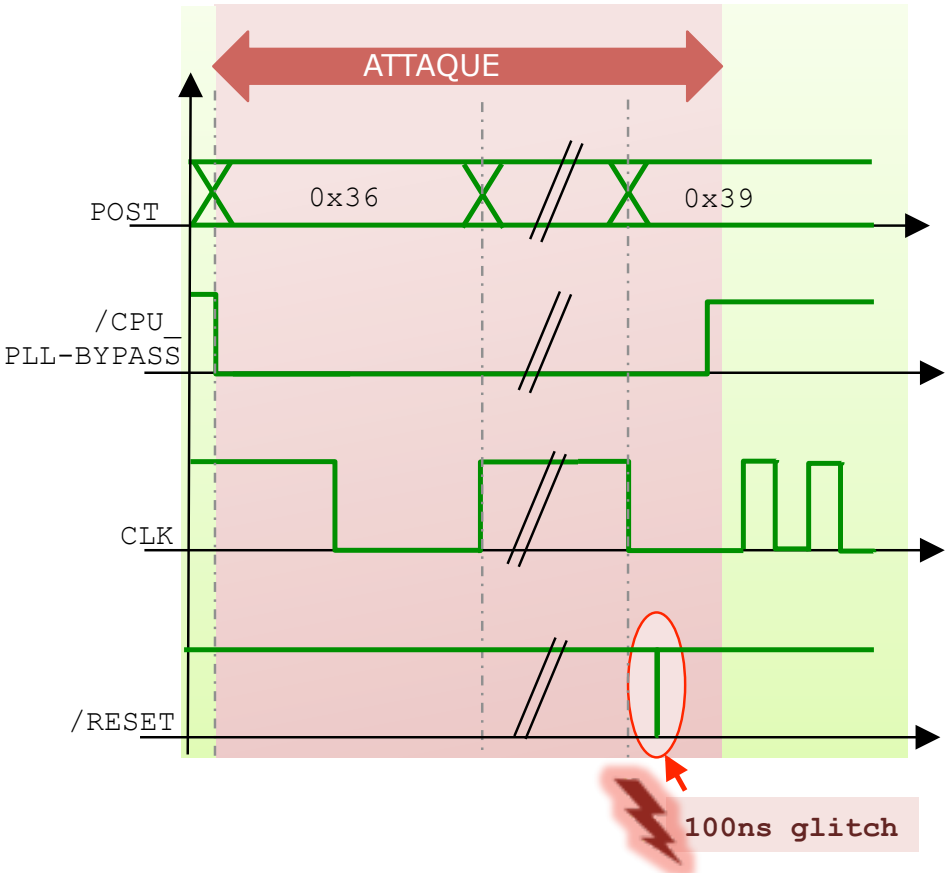


Xbox 360 : la glitch attack

- La vérification d'intégrité du 4BL par le 2BL peut être perturbée par un glitch inséré au moment adéquat

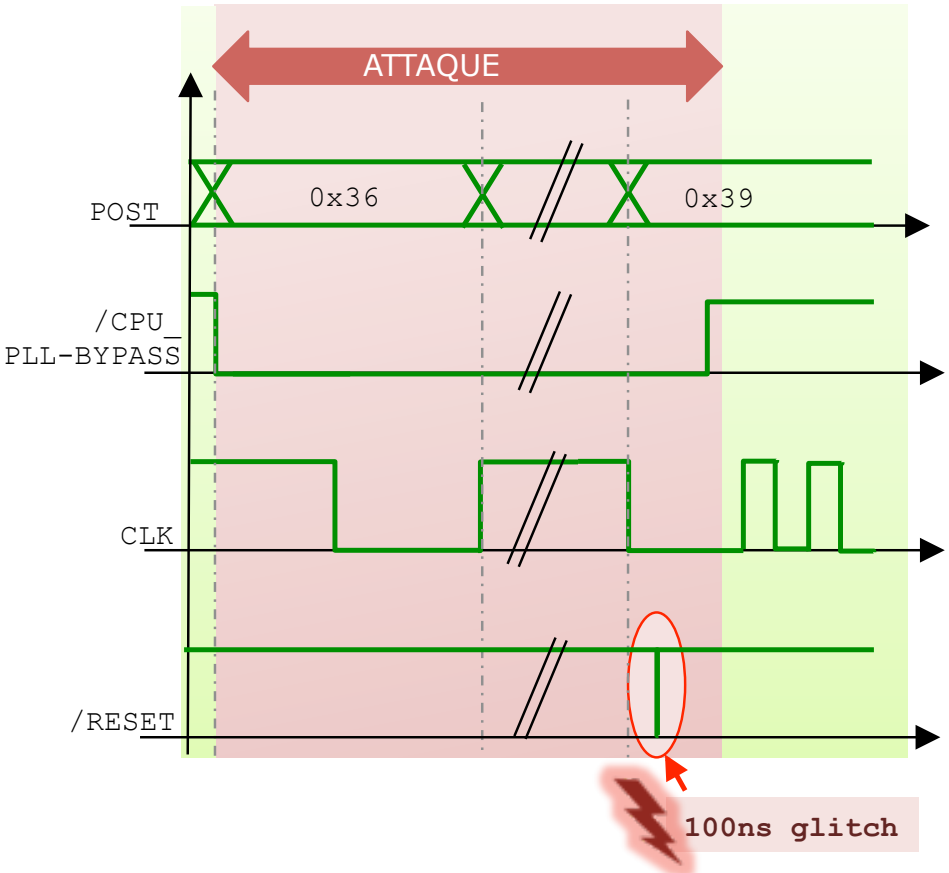
Xbox 360 : la glitch attack

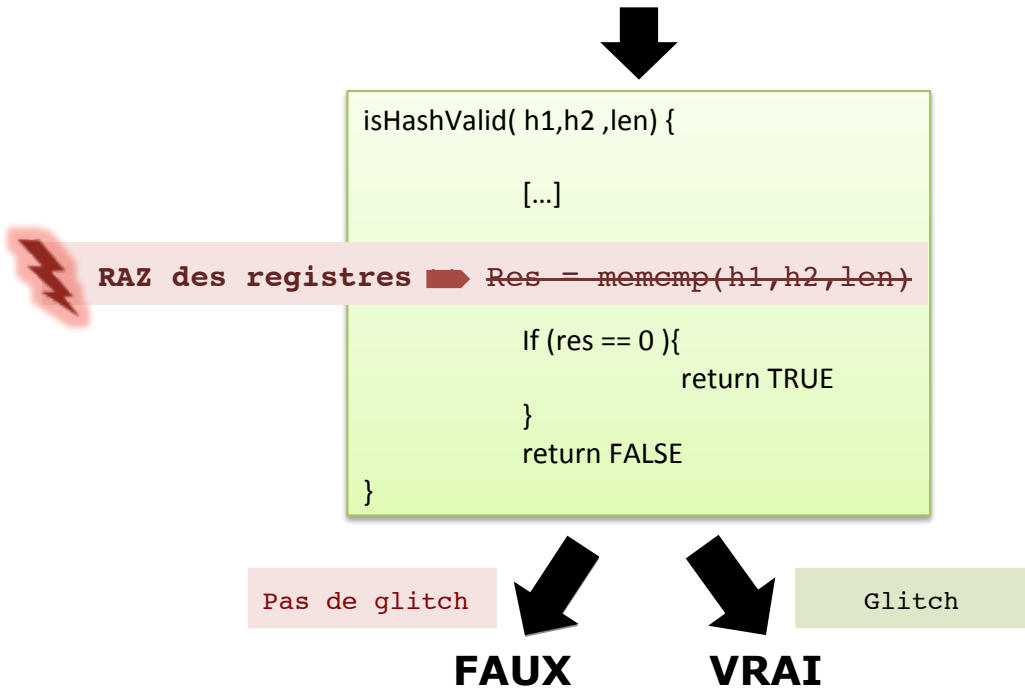
- La vérification d'intégrité du 4BL par le 2BL peut être perturbée par un glitch inséré au moment adéquat



Xbox 360 : la glitch attack

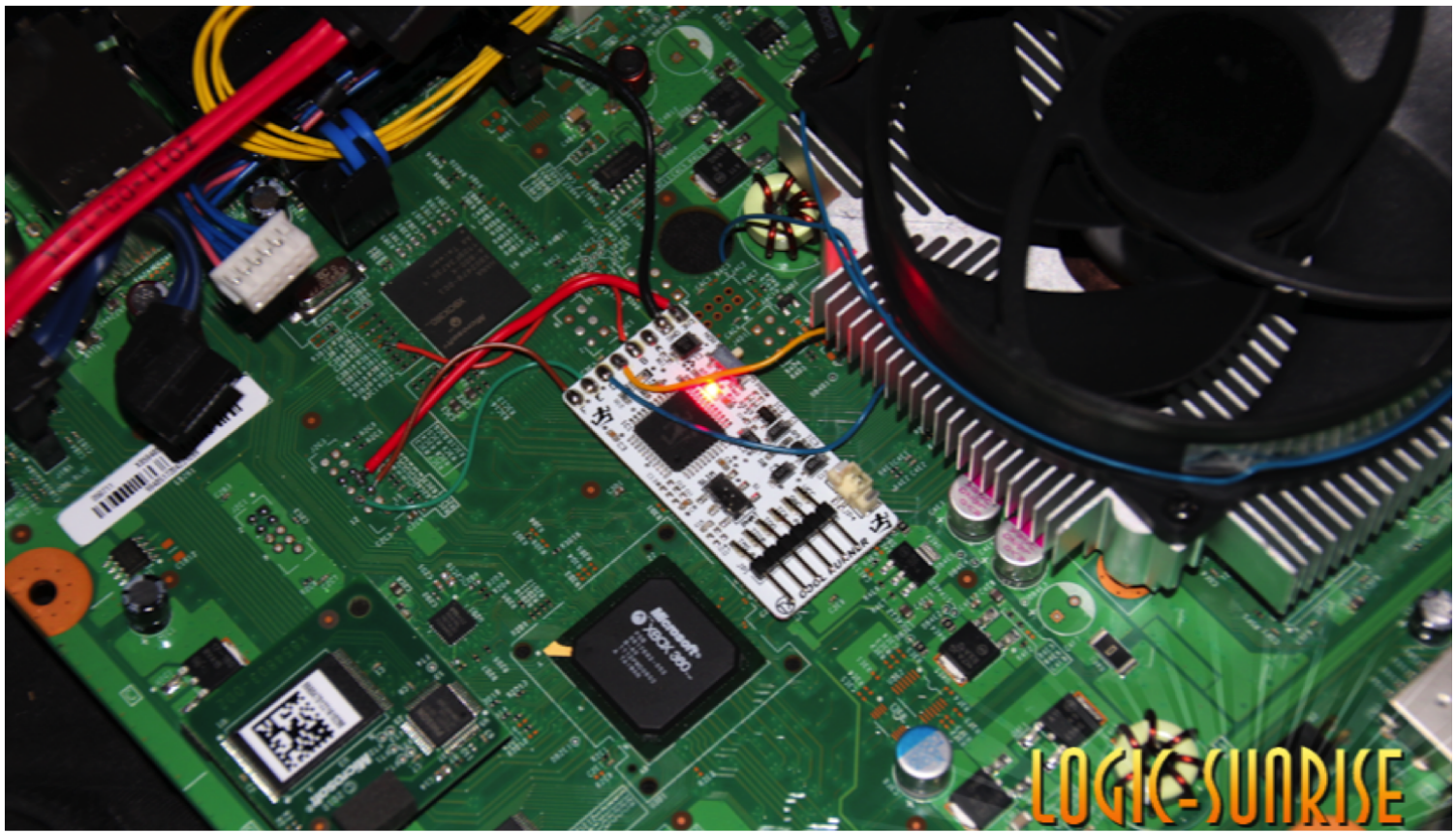
- La vérification d'intégrité du 4BL par le 2BL peut être perturbée par un glitch inséré au moment adéquat





Xbox 360 : la glitch attack

- La vérification d'intégrité du 4BL par le 2BL peut être perturbée par un glitch inséré au moment adéquat



Xbox 360 : conclusion

- Bonne architecture logicielle :
  - Hyperviseur minimaliste
  - W⊕X
  - Authentification de tout code exécuté
- Chaîne de boot bien pensée, eFuses ...

Xbox 360 : conclusion

- Bonne architecture logicielle :
  - Hyperviseur minimaliste
  - W⊕X
  - Authentification de tout code exécuté
- Chaîne de boot bien pensée, eFuses ...

- ... mais attaques DMA (états des threads)
- Certaines données non authentifiées
- Quelques faiblesses cryptographiques exploitées (timing attack, RC4)
- Pas pensée pour les attaques matérielles (glitch)

Choose your player

Skill Level

Can I play, Daddy?

Don't hurt me.

Bring 'em on!

I am Death incarnate!

Choose your player

PS3

Skill Level

Can I play, Daddy?

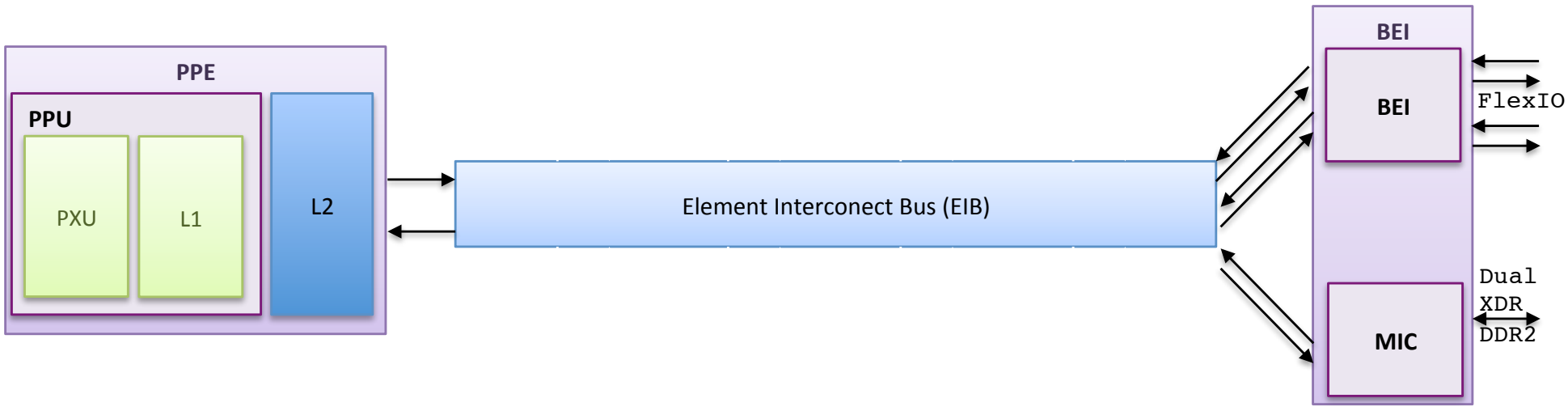
Don't hurt me.

➡ Bring 'em on!

I am Death incarnate!

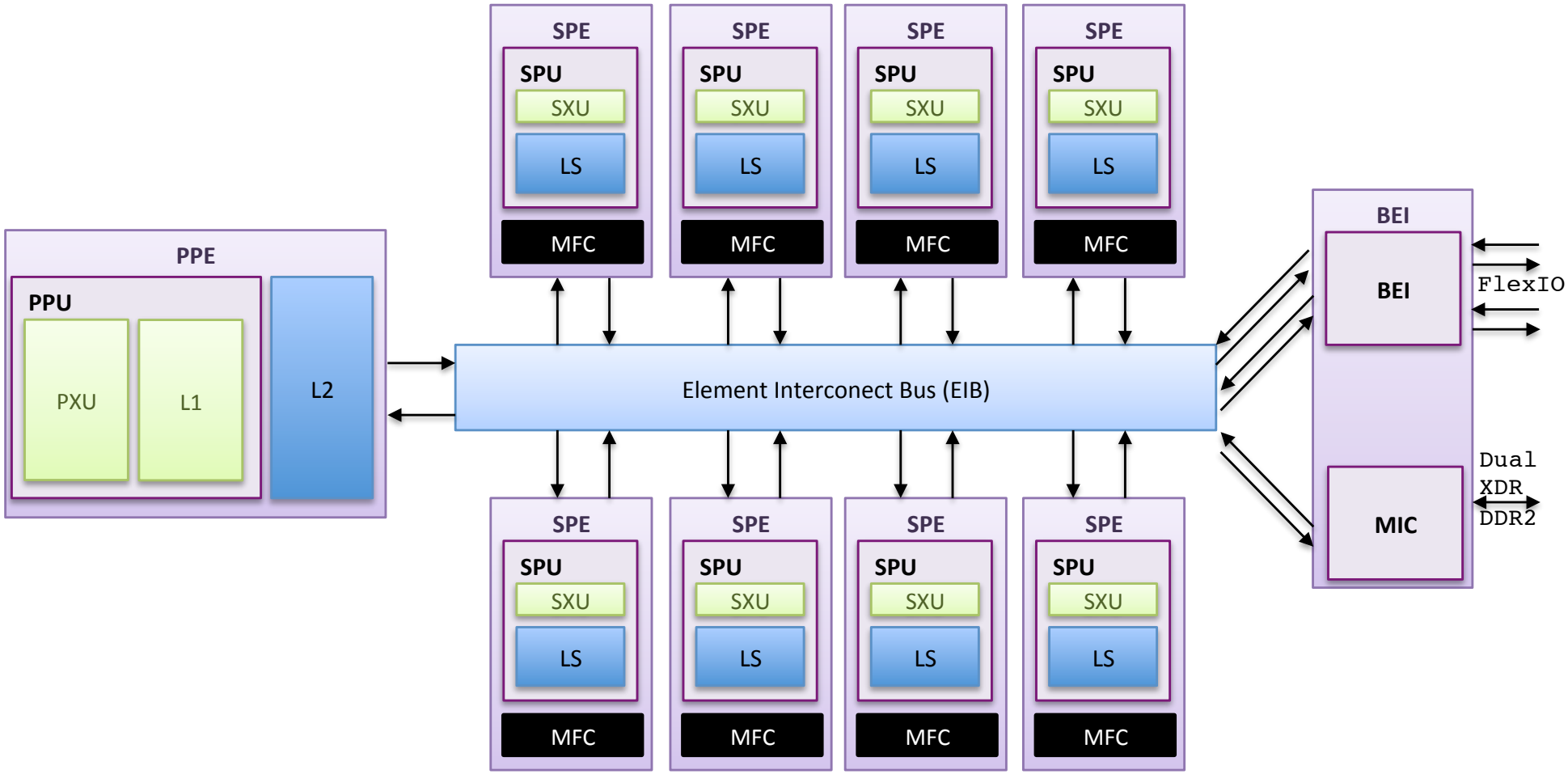
PS3 : architecture

- PPE: architecture PowerPC 64-bit classique




```
SPE — Synergistic Processor Element   PPU — Power Processor Unit
SPU — Synergistic Processor Unit      PXU — Power Execution Unit
SXU — Synergistic Execution Unit      BEI — Broadband Engine Interface
LS  — Local Store                     MIC — Memory Interface Controller
MFC — Memory Flow Controller          XDR/DDR2 — Extreme Data Rate / Double Data Rate 2
```

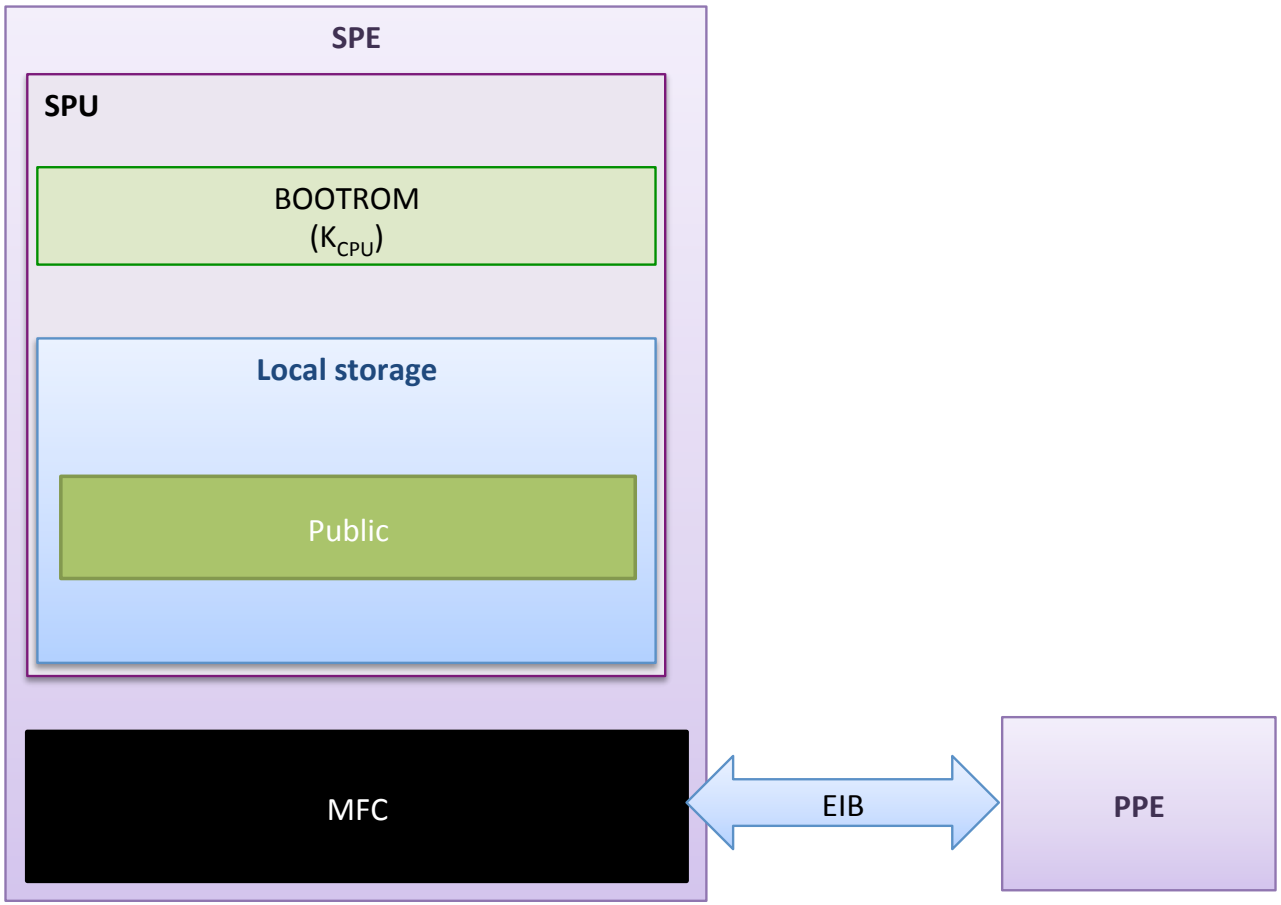
PS3 : architecture




```
SPE — Synergistic Processor Element   PPU — Power Processor Unit
SPU — Synergistic Processor Unit      PXU — Power Execution Unit
SXU — Synergistic Execution Unit      BEI — Broadband Engine Interface
LS  — Local Store                     MIC — Memory Interface Controller
MFC — Memory Flow Controller          XDR/DDR2 — Extreme Data Rate / Double Data Rate 2
```

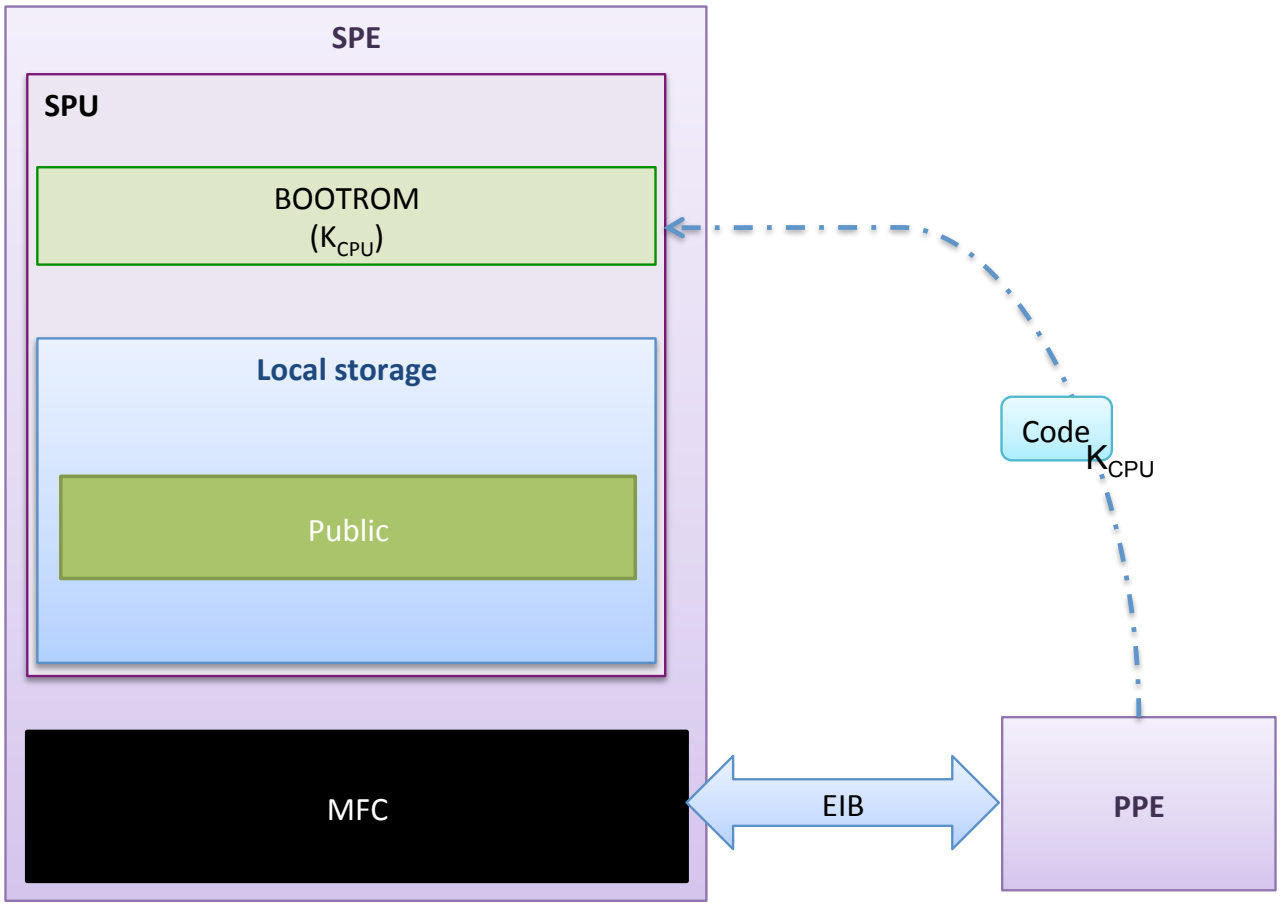
PS3 : mode SPE isolé

- SPE : isolation/bootstrap de code (racine de confiance)



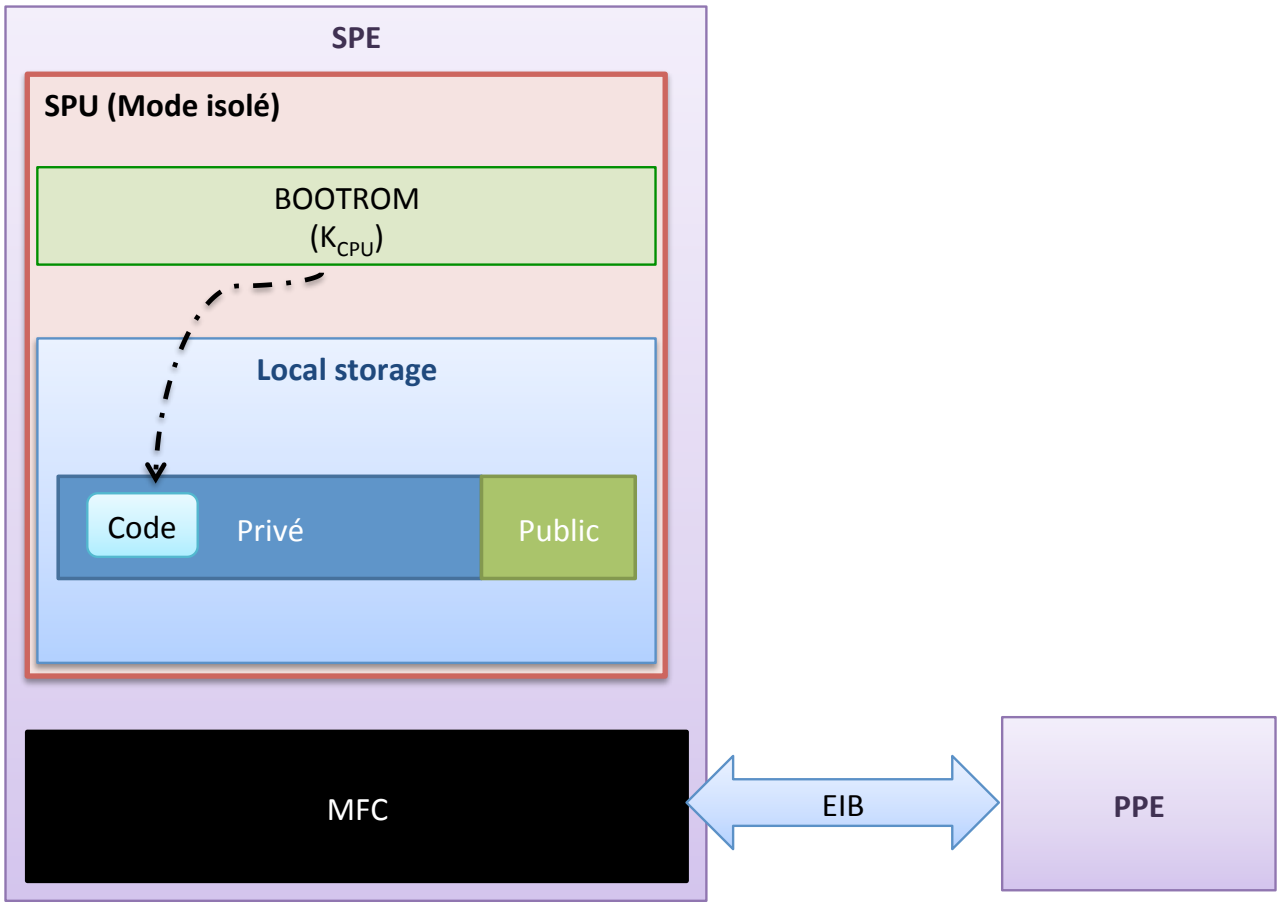
PS3 : mode SPE isolé

- SPE : isolation/bootstrap de code (racine de confiance)



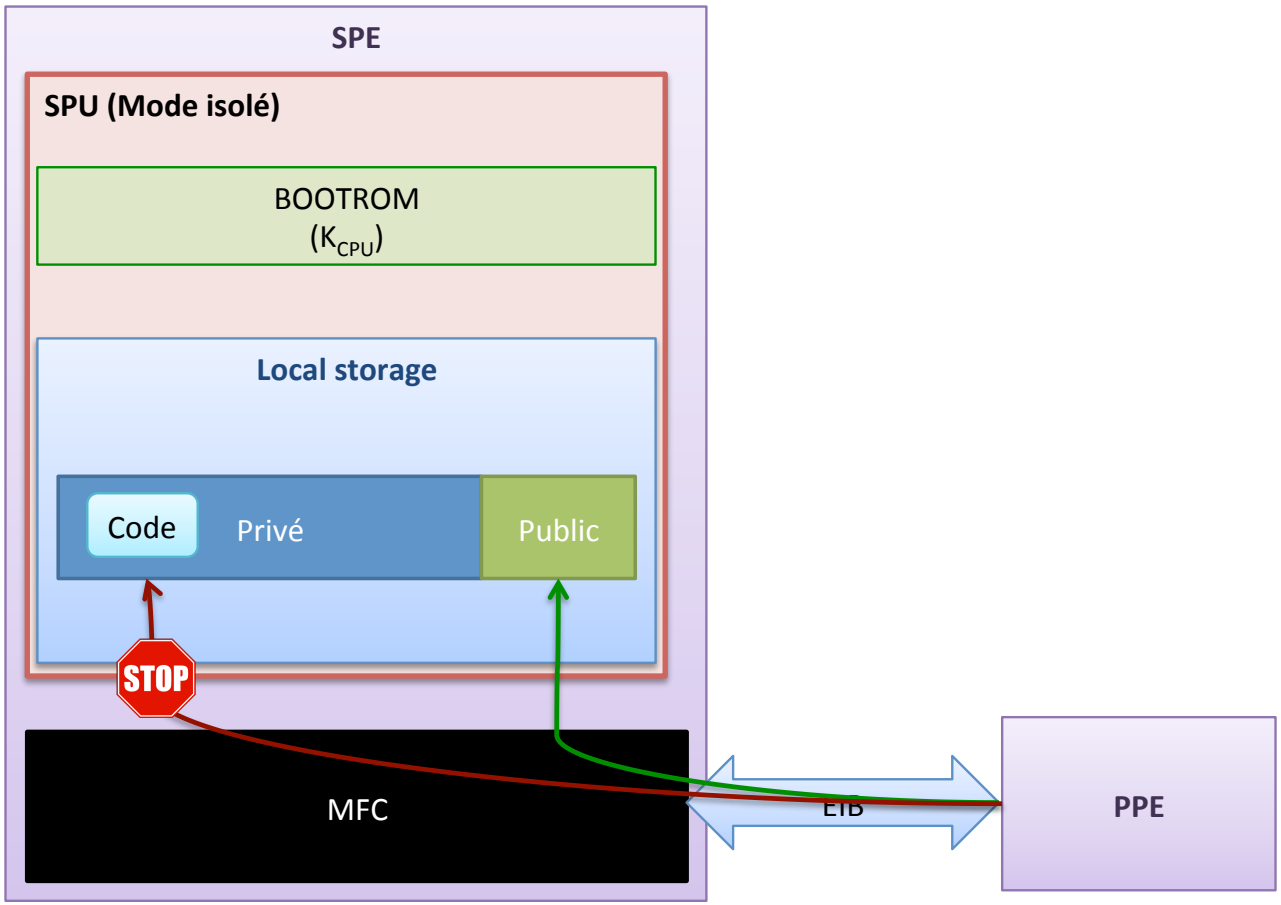
PS3 : mode SPE isolé

- SPE : isolation/bootstrap de code (racine de confiance)



PS3 : mode SPE isolé

- SPE : isolation/bootstrap de code (racine de confiance)



PS3 : architecture logicielle

- **Bootloaders** (ldr*) :
  - De premier niveau : bootstrapent SPE en mode isolé
  - De second niveau : exécutés par les premiers

PS3 : architecture logicielle

- **Bootloaders** (ldr*) :
  - De premier niveau : bootstrapent SPE en mode isolé
  - De second niveau : exécutés par les premiers
- **Hyperviseur** (lv1) : PPE en mode hyperviseur

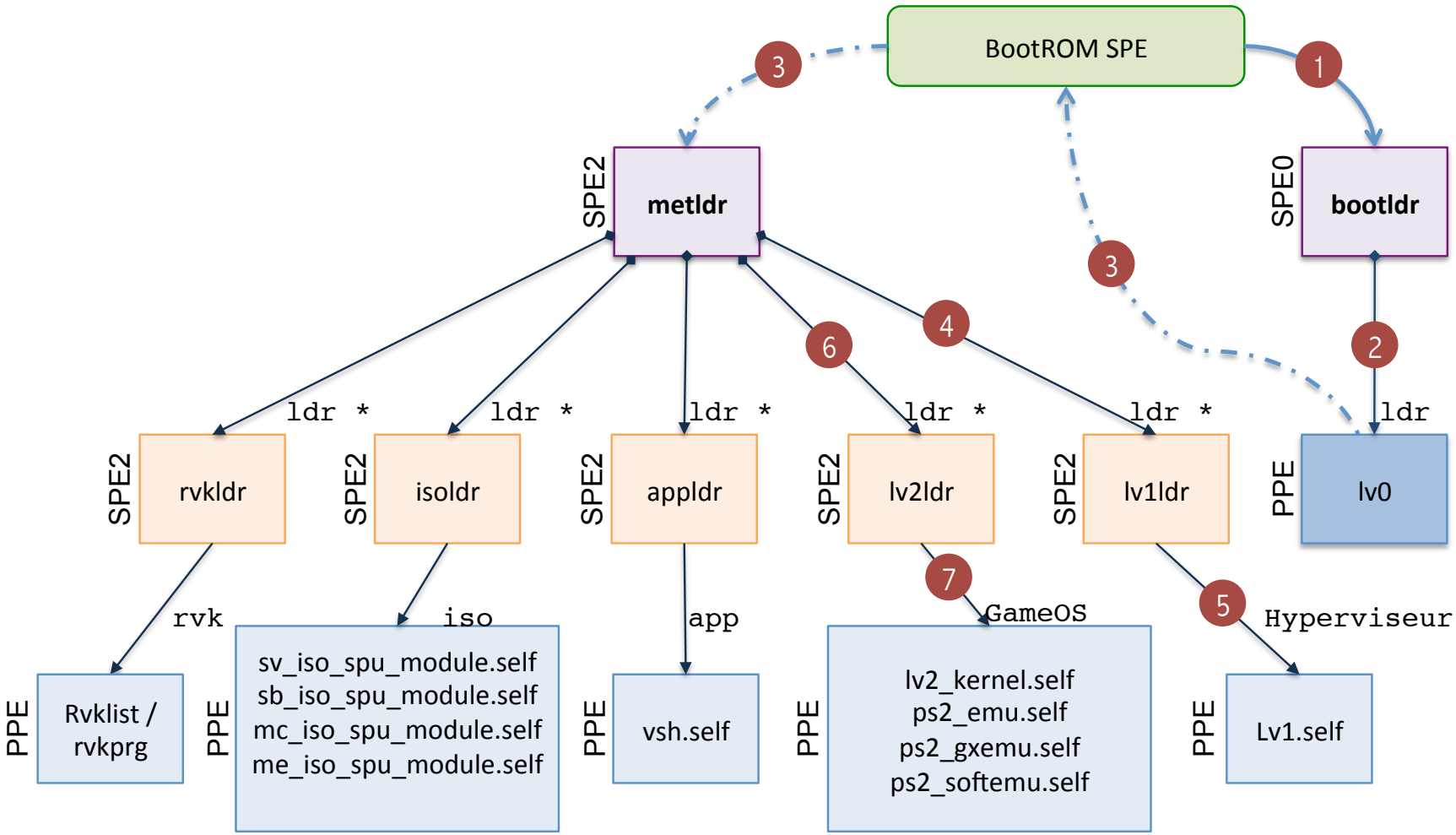
PS3 : architecture logicielle

- **Bootloaders** (ldr*) :
  - De premier niveau : bootstrapent SPE en mode isolé
  - De second niveau : exécutés par les premiers
- **Hyperviseur** (lv1) : PPE en mode hyperviseur
- **GameOS/OtherOS** (lv2/-) : PPE en mode superviseur
  - OtherOS = Linux (supprimé après la première attaque)

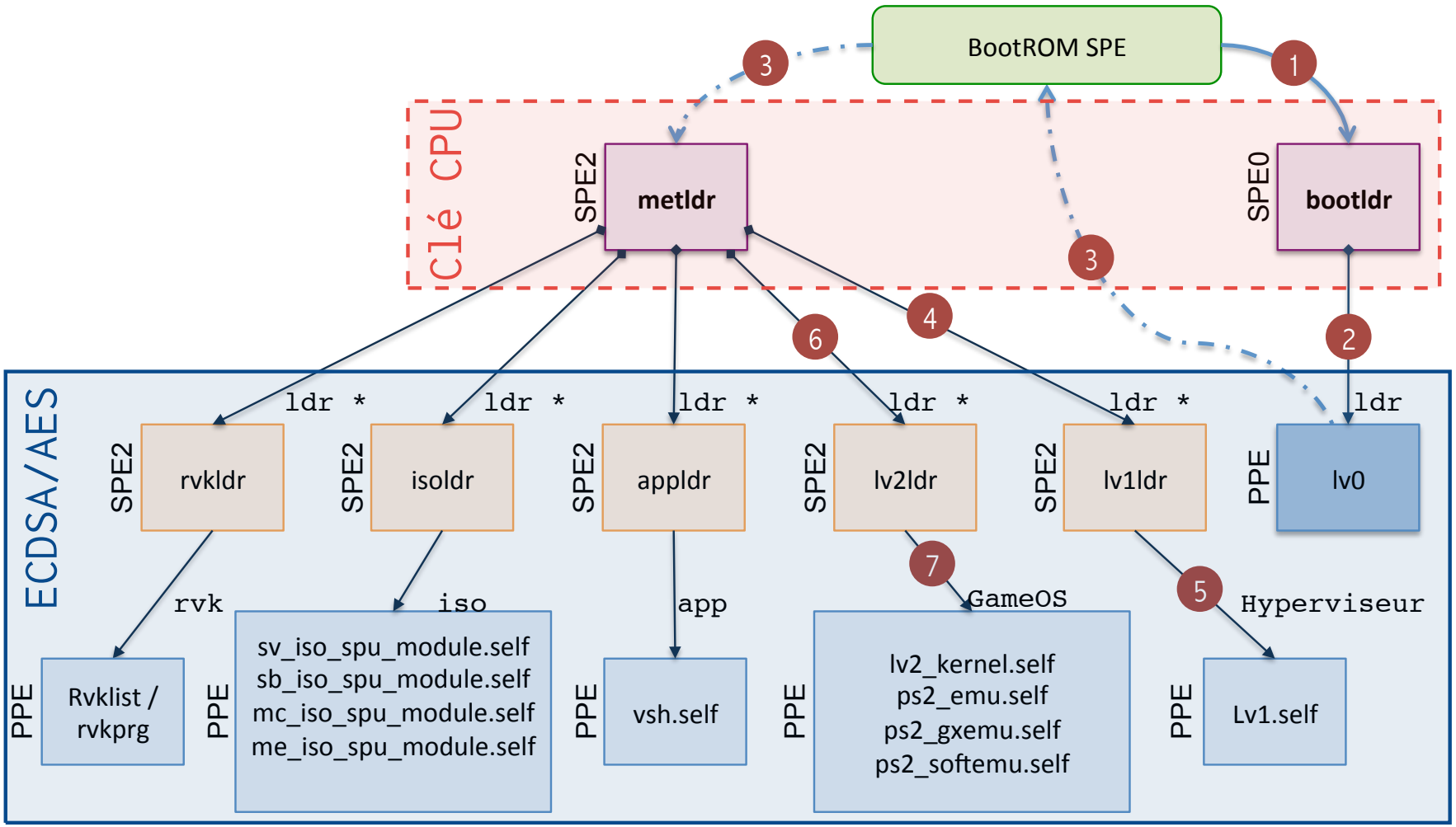
PS3 : architecture logicielle

- **Bootloaders** (ldr*) :
  - De premier niveau : bootstrapent SPE en mode isolé
  - De second niveau : exécutés par les premiers
- **Hyperviseur** (lv1) : PPE en mode hyperviseur
- **GameOS/OtherOS** (lv2/-) : PPE en mode superviseur
  - OtherOS = Linux (supprimé après la première attaque)
- **Applications** : PPE en mode utilisateur

PS3 : boot sécurisé



PS3 : boot sécurisé



PS3 : révocation et anti-downgrade

- Pas d'utilisation d'ancrage matériel via eFuse

	CPU/Mode	MàJ	Révocation
bootROM	Cell	Non	Non
bootldr	SPE0	Non	Non
lv0	PPE/HV	Oui	Non
metldr	SPE2	Non	Non
lv1ldr	SPE2	Oui	Non
lv1	PPE/HV	Oui	Non
lv2ldr	SPE2	Oui	Non
lv2	PPE/SP	Oui	Oui
isoldr	SPE2	Oui	Non
appldr	SPE2	Oui	Oui
jeux/applications	PPE/USR	Oui	Oui

PS3 : modèle de sécurité

- PPE/hyperviseur hors TCB (Trusted Computing Base)
  - Eléments critiques exécutés sur les SPE
  - Tout code est chiffré et signé
  - Sécurité par l'obscurité

PS3 : modèle de sécurité

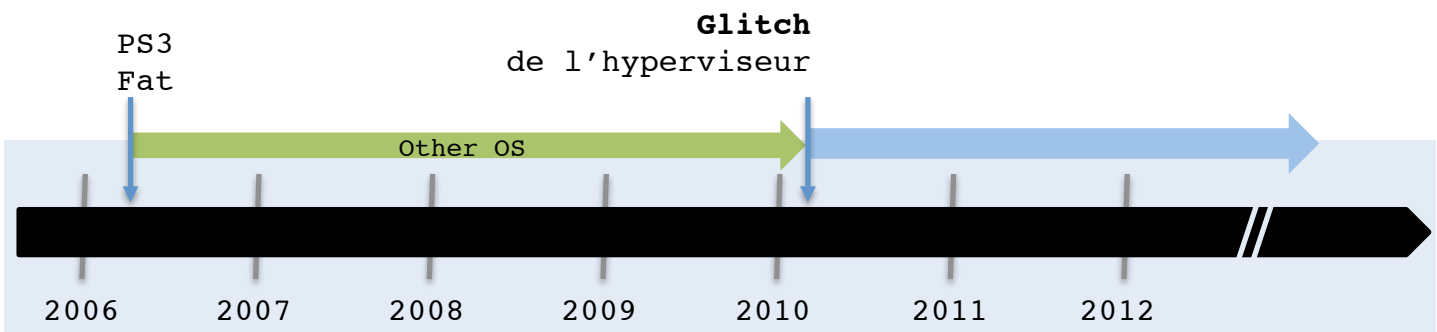
- PPE/hyperviseur hors TCB (Trusted Computing Base)
  - Eléments critiques exécutés sur les SPE
  - Tout code est chiffré et signé
  - Sécurité par l'obscurité
- Chiffrement sur bus EIB (RAM, périphériques)
  - Limitation des attaques via DMA

PS3 : modèle de sécurité

- PPE/hyperviseur hors TCB (Trusted Computing Base)
  - Eléments critiques exécutés sur les SPE
  - Tout code est chiffré et signé
  - Sécurité par l'obscurité
- Chiffrement sur bus EIB (RAM, périphériques)
  - Limitation des attaques via DMA
- Pas de W⊕X, l'hyperviseur ne vérifie rien

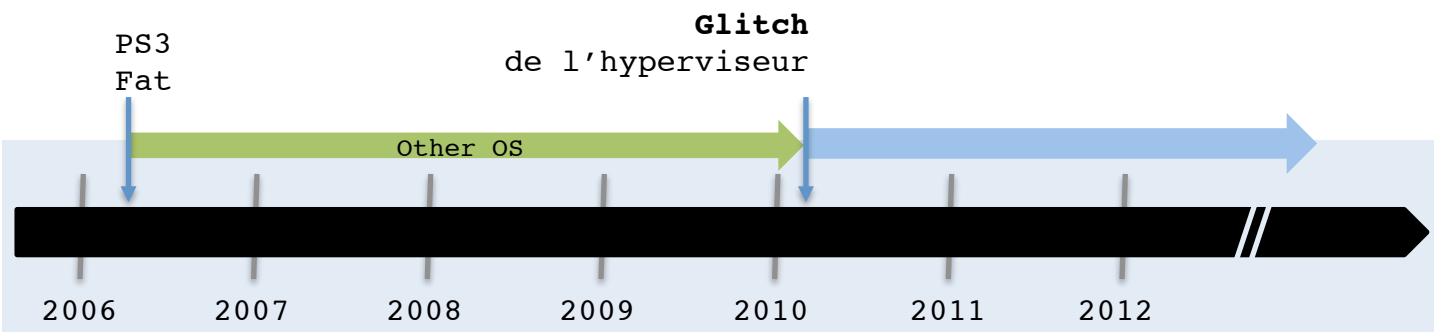
PS3 : hello hypervisor, I'm geohot

- **Glitch** ⇒ contrôle de l'hyperviseur depuis Linux



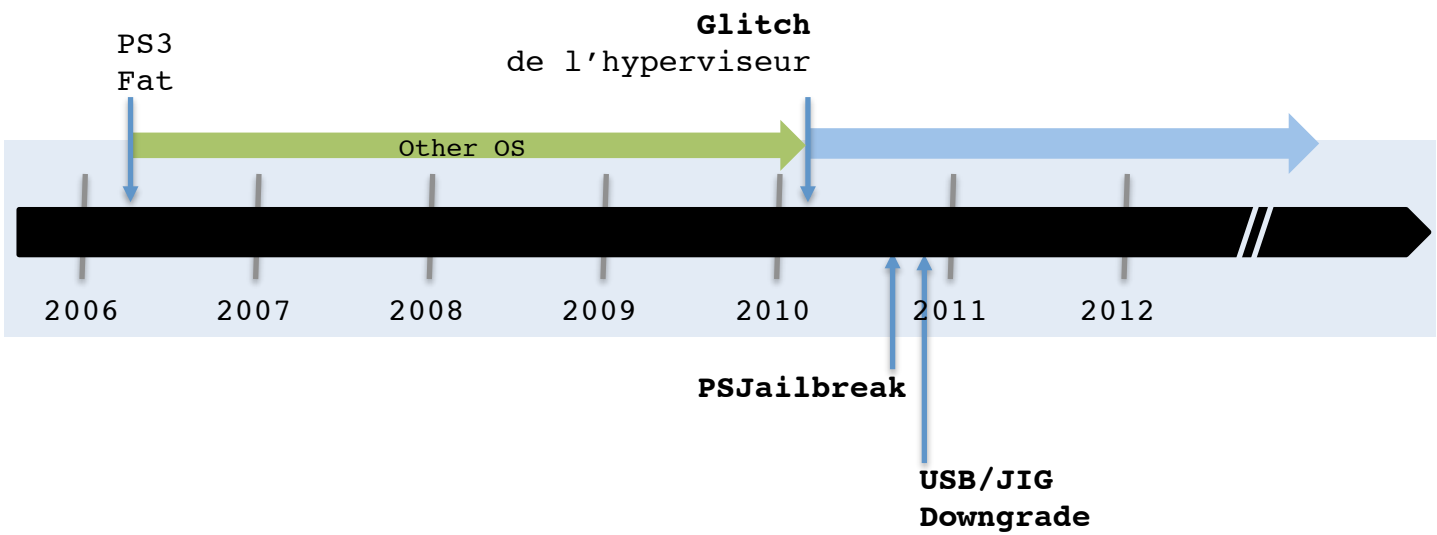
PS3 : hello hypervisor, I'm geohot

- **Glitch** ⇒ contrôle de l'hyperviseur depuis Linux
- Ne permet pas de contrôler les autres éléments
  - Pas de piratage de jeux



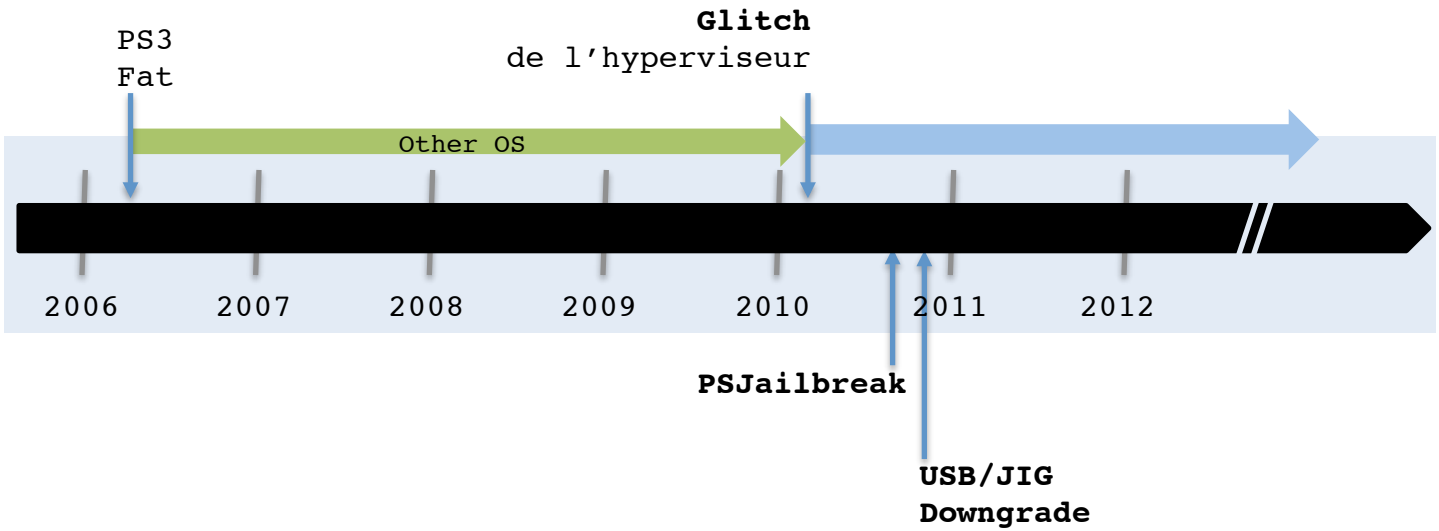
PS3 : PSJailbreak

- Première attaque permettant de pirater les jeux
- Attaque de la pile USB du lv2 (GameOS)
  - Pas de W⊕X : hyperviseur fail



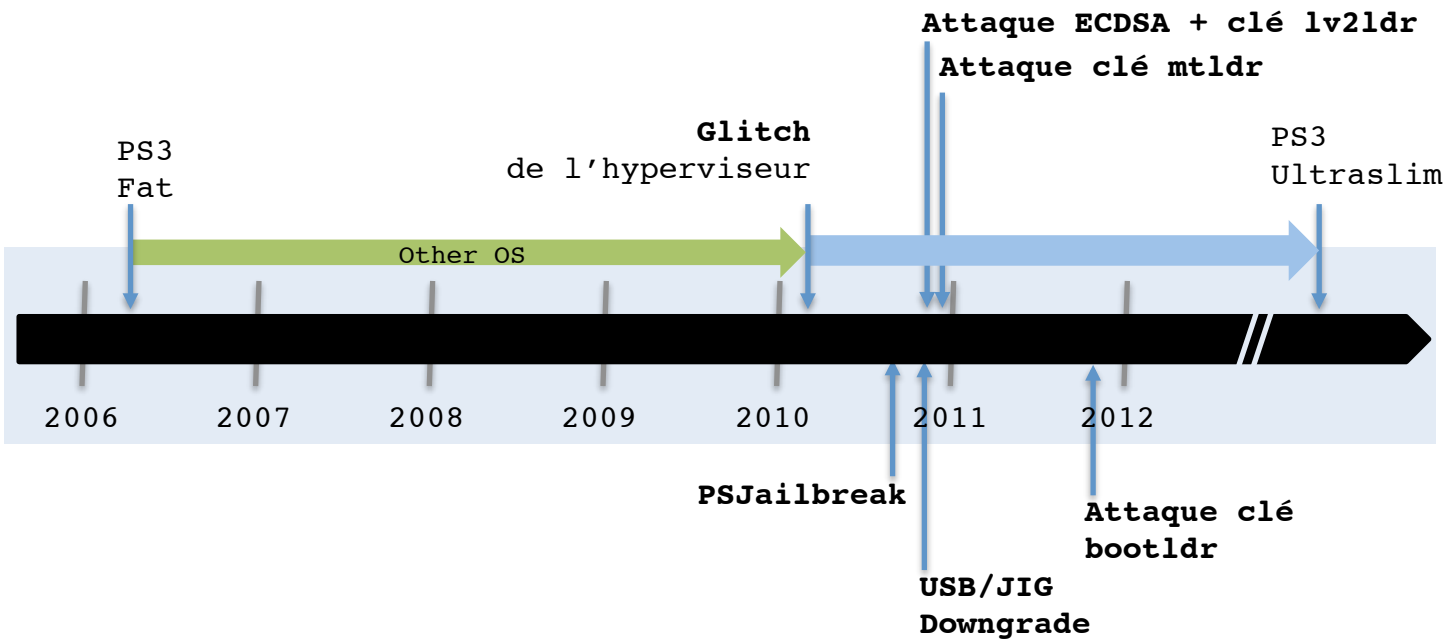
PS3 : attaque des bootloaders

- 2010 : **vulnérabilité majeure** dans l'ECDSA de Sony :
  - **nonces qui sont les mêmes** pour les diverses versions de firmware
  - A partir de deux signatures, calcul de la clé privée !



PS3 : attaque des bootloaders

- 2010 : **vulnérabilité majeure** dans l'ECDSA de Sony :
  - **nonces qui sont les mêmes** pour les diverses versions de firmware
  - A partir de deux signatures, calcul de la clé privée !
  - Chaîne de démarrage définitivement **cassée**



PS3 : conclusion

- Plateforme matérielle exotique intéressante (SPE isolé)
- Contremesures attaques DMA
- BootROM avec clé CPU dédiée

PS3 : conclusion

- Plateforme matérielle exotique intéressante (SPE isolé)
- Contremesures attaques DMA
- BootROM avec clé CPU dédiée

- Hyperviseur limité non pensé pour la sécurité
- Pas de défense en profondeur (pas de W⊕X)
- Fail cryptographique (ECDSA)
- Chaîne de boot avec mise à jour limitée
- Sécurité par l'obscurité (code des SPE)
- Pas pensée contre les attaques matérielles (glitch)

Conclusion

- Il n'y as pas d'économie lorsque l'on parle de sécurité
- Les attaques ciblent toujours le maillon faible
- Les attaquants ne font pas la distinction entre logiciel et matériel
  - La sécurité est un problème d'ensemble
  - Les équipes logicielle et matérielle doivent communiquer

Questions