Bypassing DMA remapping with DMA

Benoît Morgan, Guillaume Averlant,
Vincent Nicomette, Éric Alata

LAAS-CNRS, INSA Toulouse, Université de Toulouse

3 juin 2016

Plan

Les attaques DMA

Direct Memory Access (DMA)

- Accès des périphériques à la mémoire principale
- Indépendants du CPU

Menaces

- Accès au code et données de logiciels privilégiés
- Les periphériques ne sont pas exempts de vulnérabilités exploitables (carte réseau vulnérable, *Pérez et al.* [**1**])

$\Rightarrow$ Lectures et écritures arbitraires malveillantes

$\Rightarrow$ Contrôles d'accès indispensables

Input Output Memory Management Unit

Services

- DMA Remapping (**DMAR**) : Virtualisation de l'espace d'adressage des périphériques grâce à de la traduction et du filtrage
- Interrupt Remapping

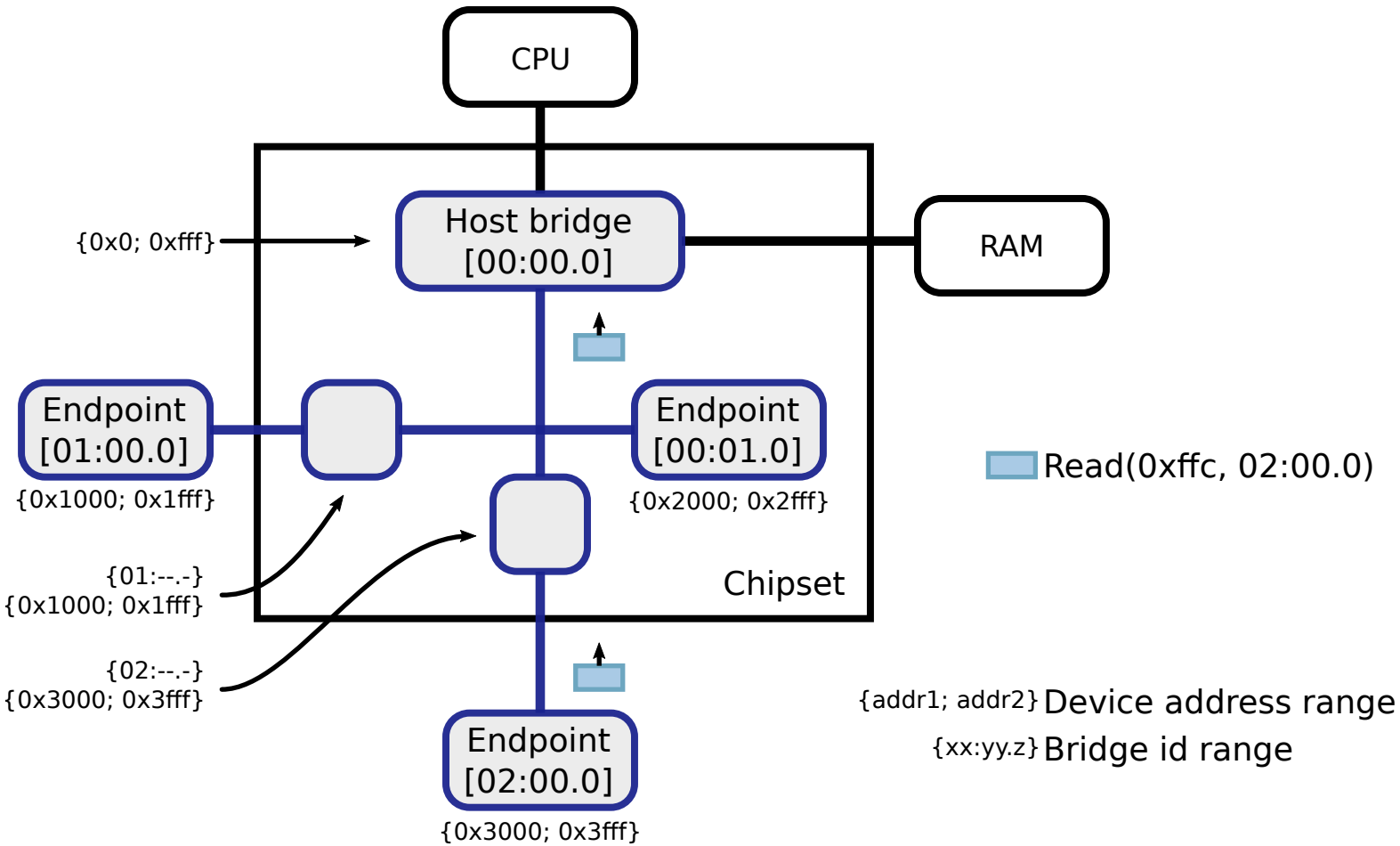
Vulnérabilités ?

- Est-ce que les systèmes opératoires utilisent aujourd'hui ce composant ?
- Comment et quand est-il configuré ?
- Quelles interactions existent entre le noyau et le firmware vis-à-vis des IOMMU ?

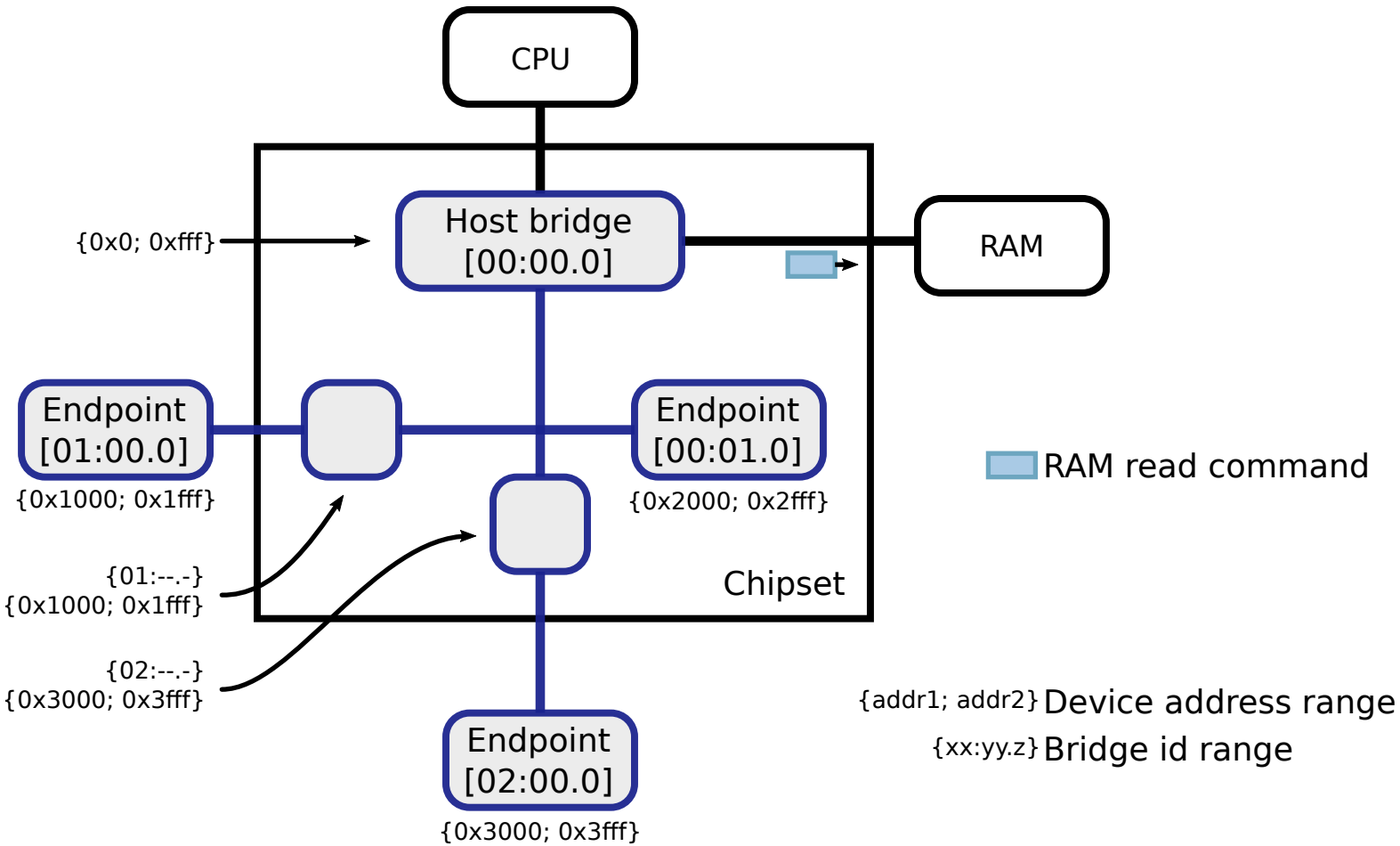
DMA et PCI Express

- Bus d'interconnexion des périphériques et du CPU via le host bridge
- Modèle orienté message
  - Memory Read / Write
  - Configuration Read / Write
- Adressage mémoire
  - Chaque périphérique peut exposer un range mémoire : ex. `[0x1000, 0x1fff]`
- Adressage des devices par identifiant : `[bus:dev.fun]`
  - Host bridge : `[00:00.0]`
  - Devices internes : `[00:x.y]`

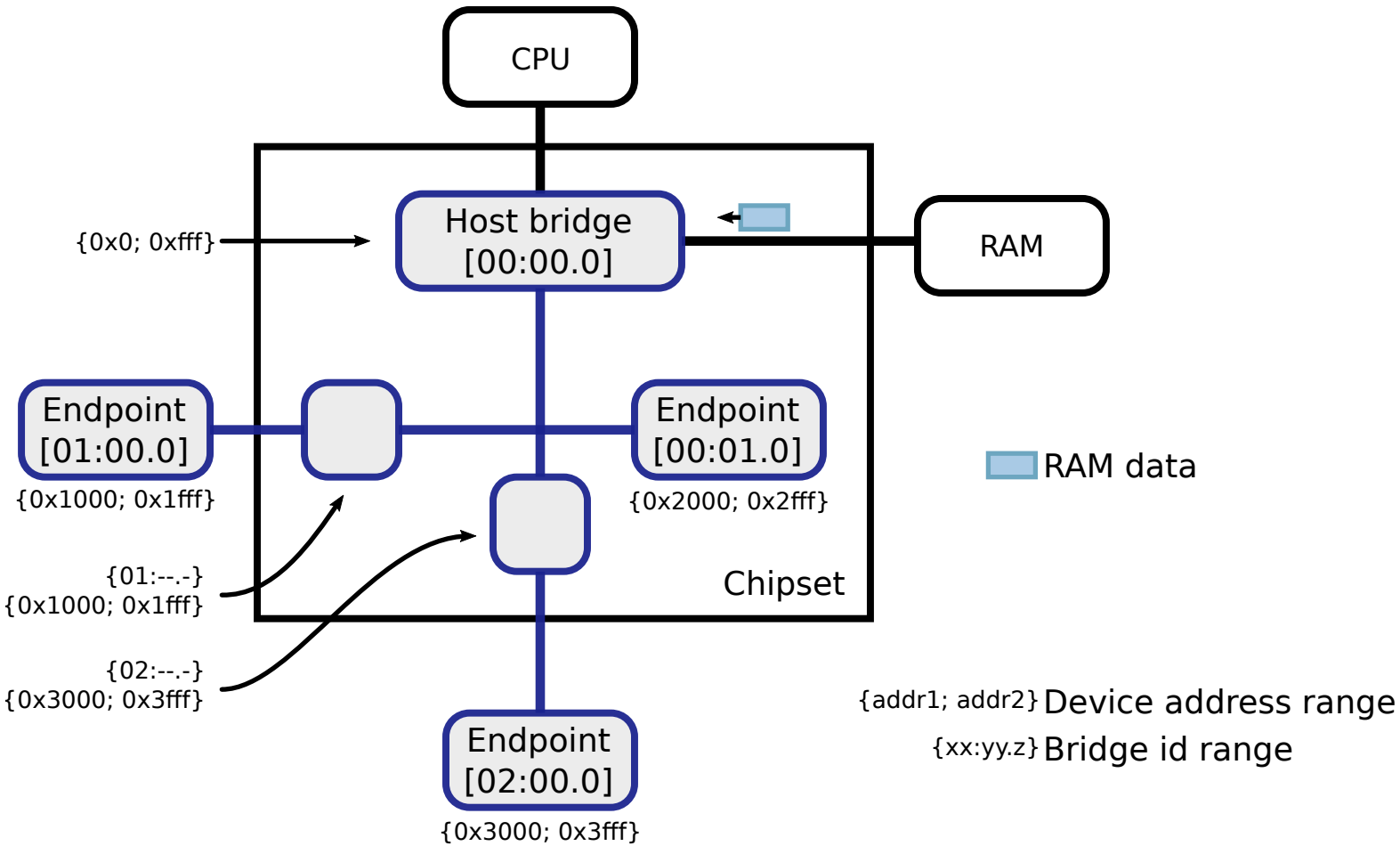
Lecture DMA : PCI Express Memory Read



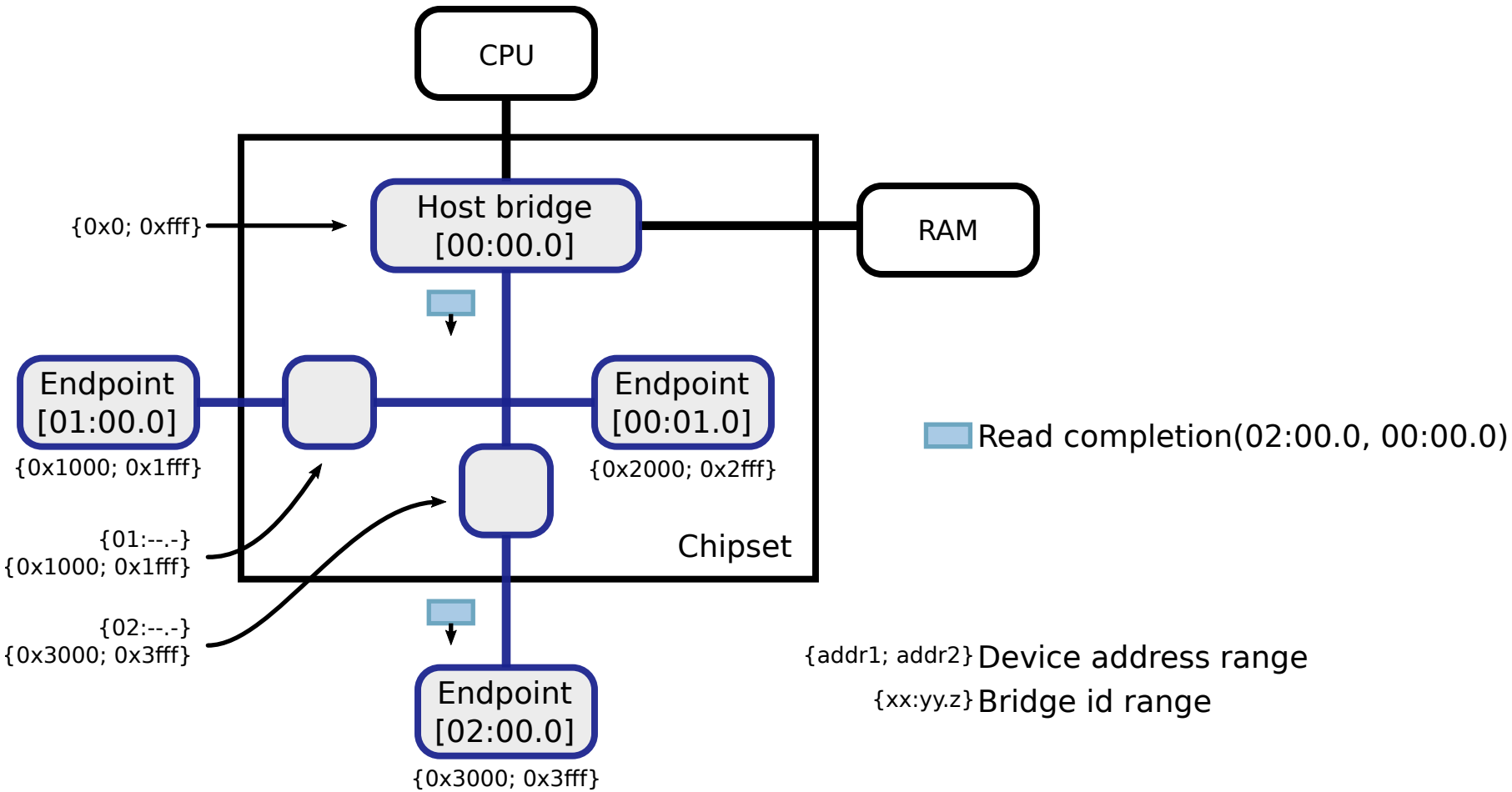
Lecture DMA : PCI Express Memory Read



Lecture DMA : PCI Express Memory Read



Lecture DMA : PCI Express Memory Read



Plan

Configuration du DMAR

- Traduction et filtrage des accès DMA en deux phases avec deux jeux de tables de traduction
  - Device to domain mapping : identification du domaine mémoire associé à un device (root table, context tables)
  - Address translation : traduction de l'adresse pour le domaine mémoire identifié (similaires à la MMU)
- Structures mémoire placées en RAM, lues par l'IOMMU situées au niveau du host bridge.

Constat sur notre machine d'expérimentation

- Configuration standard

Linux 4.3.4 (IOMMU Intel)		Dell Precision t1700
Intel i7-4770	Intel PCH c226	grub 2.02.beta2

- Identifiant PCI connu des périphériques
- Accès DMA disponibles avant le chargement de grub

$\Rightarrow$ Accès DMA autorisés par le firmware

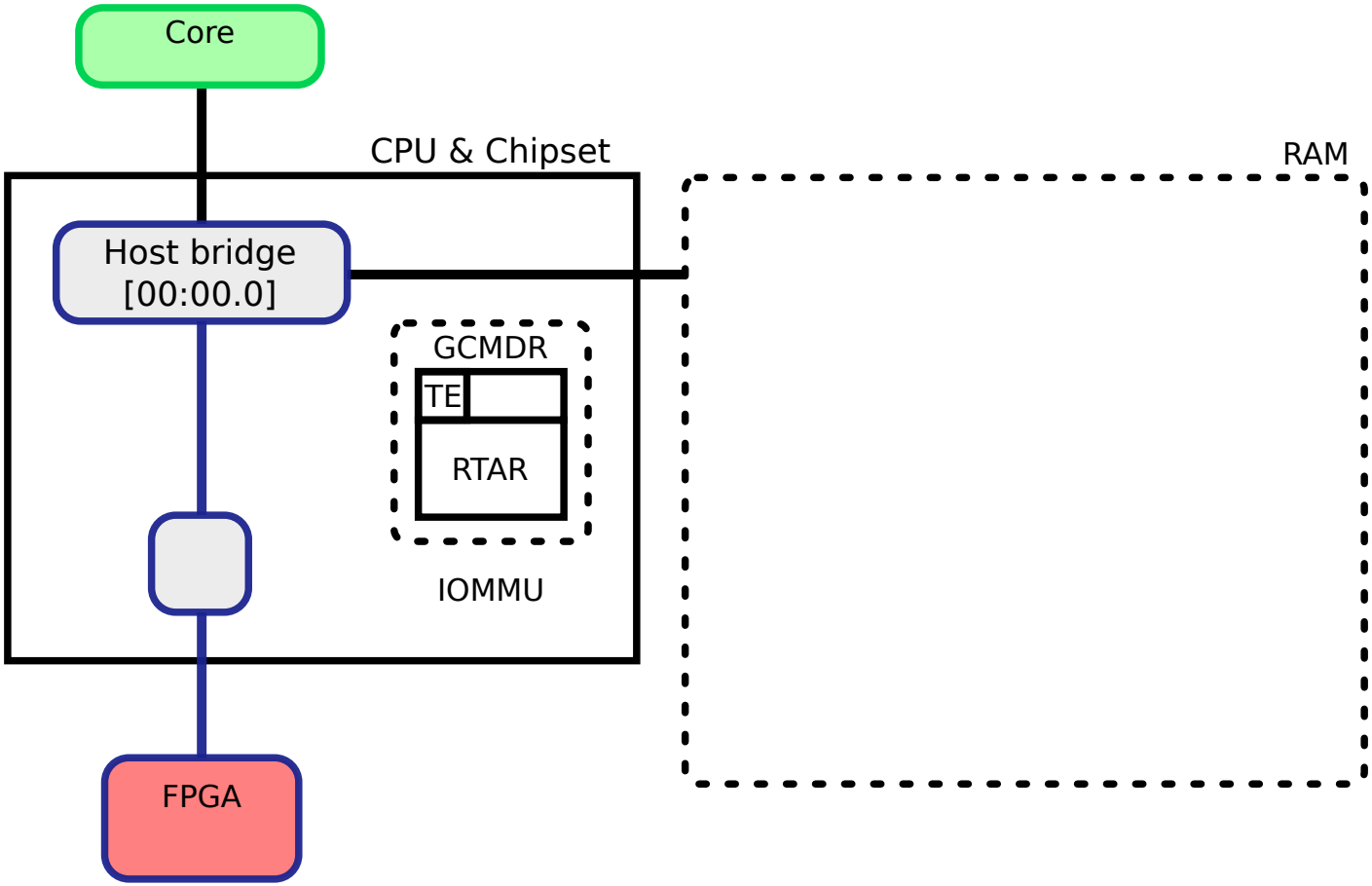
- Structures du DMAR non protégées en RAM, idem pour le code et les données du noyau

$\Rightarrow$ Le noyau est vulnérable aux attaques DMA

Attaque du driver linux `drivers/intel-iommu.c`

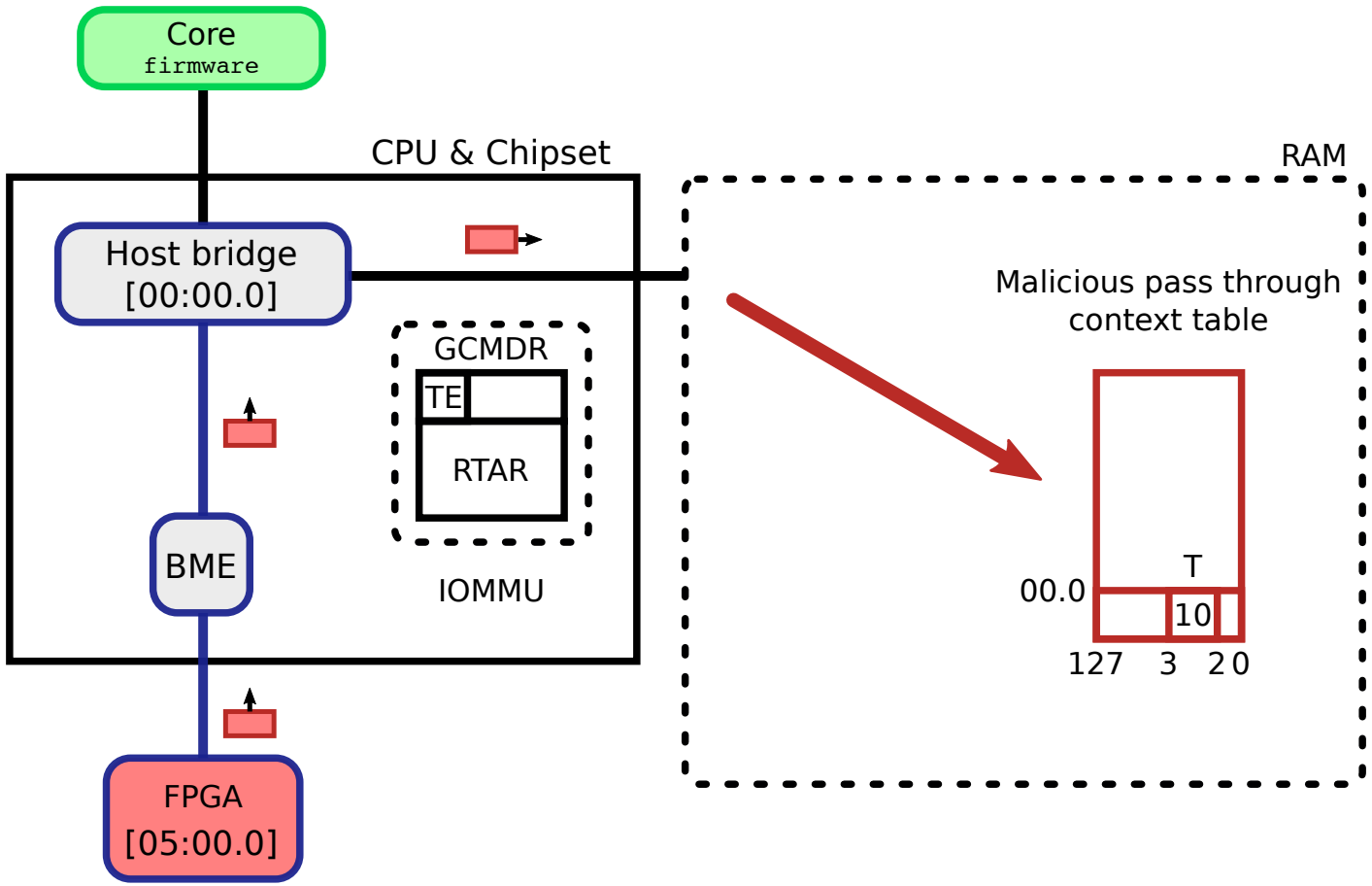
- Comment conserver l'accès à l'espace mémoire tout en préservant l'intégrité du code de linux ?

Attaque du driver linux `drivers/intel-iommu.c`



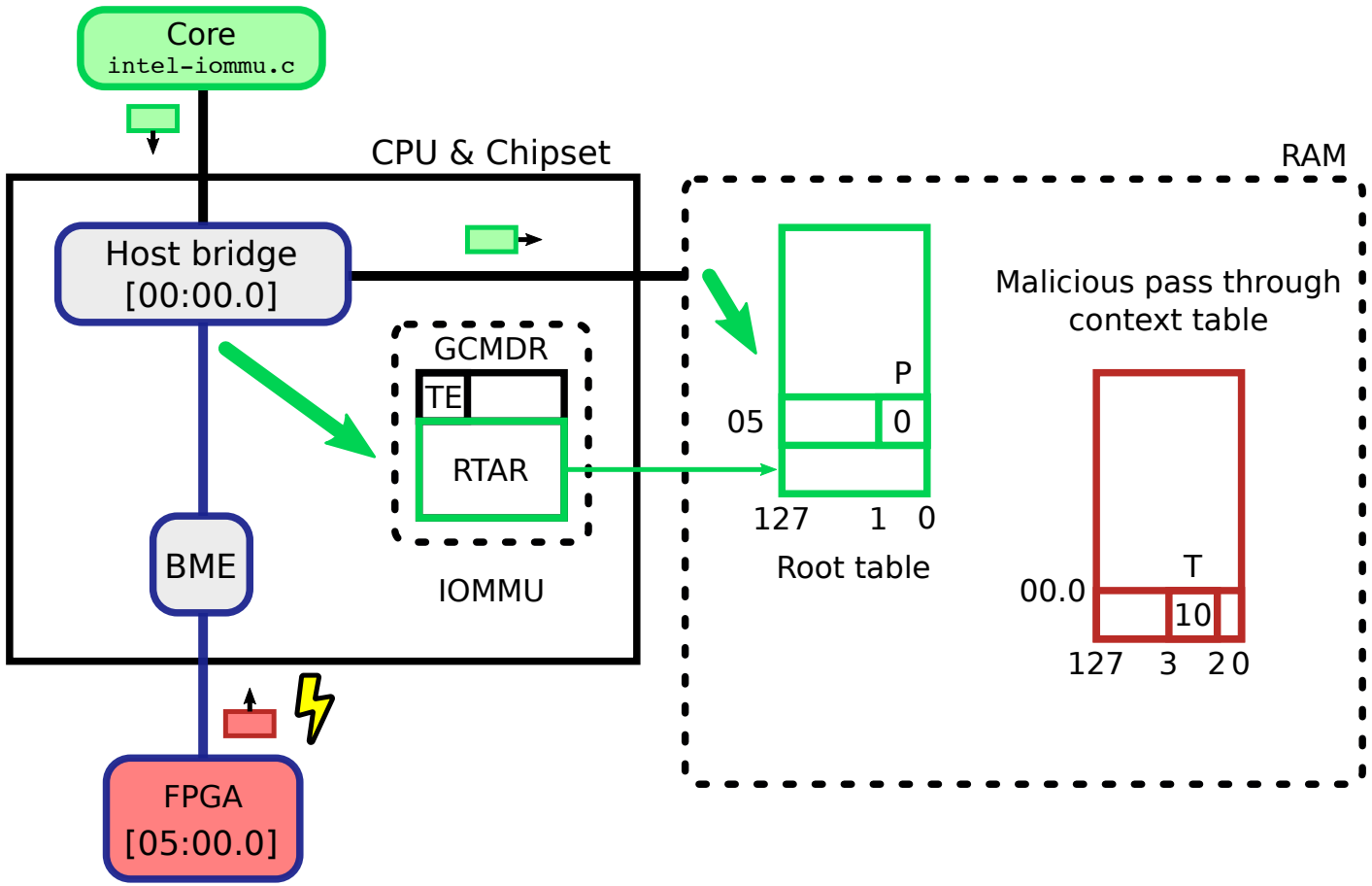
- Démarrage de la plateforme

Attaque du driver linux `drivers/intel-iommu.c`



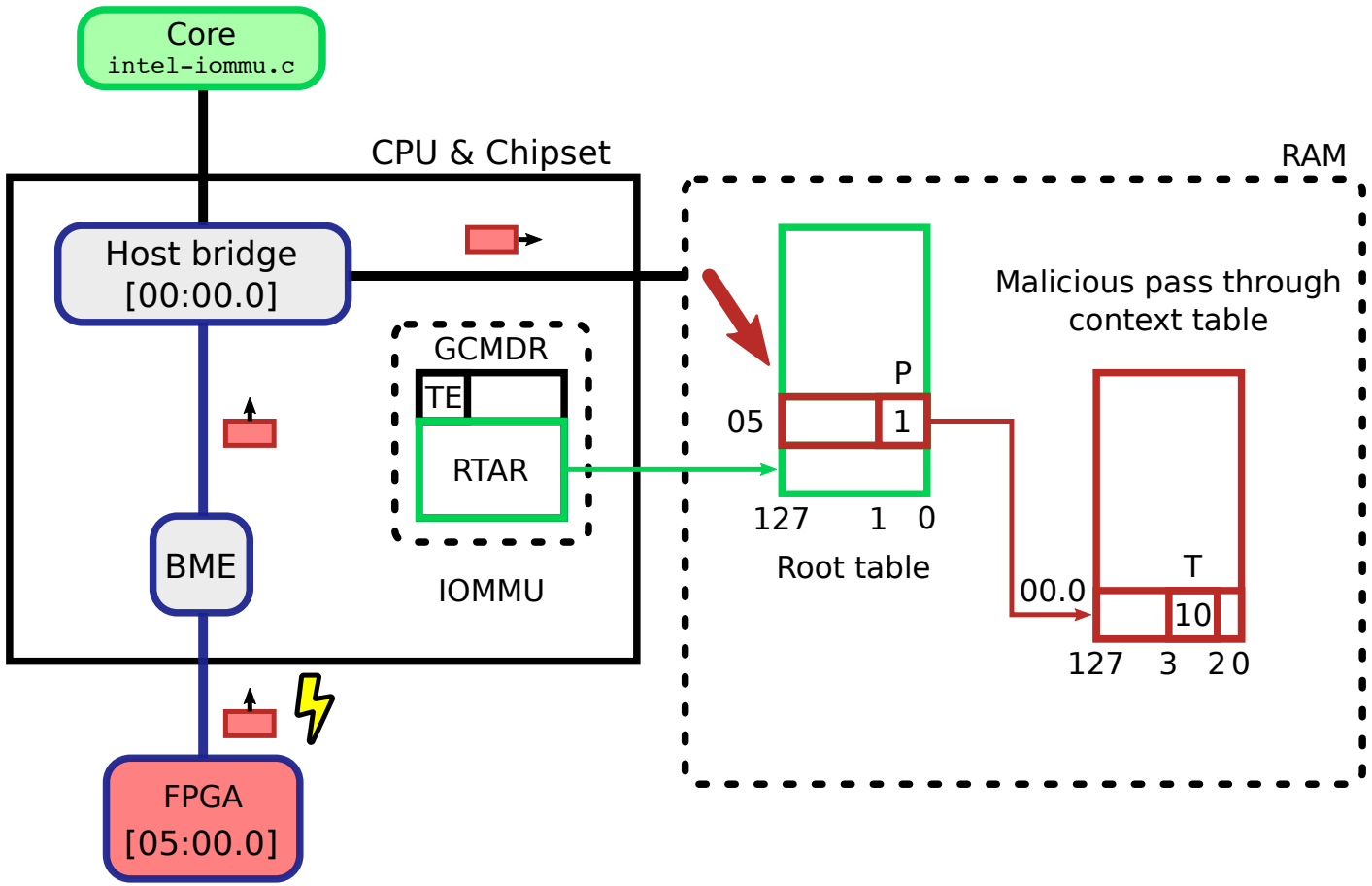
- Copie d'une *context table* malicieuse en mode *pass through*

Attaque du driver linux `drivers/intel-iommu.c`



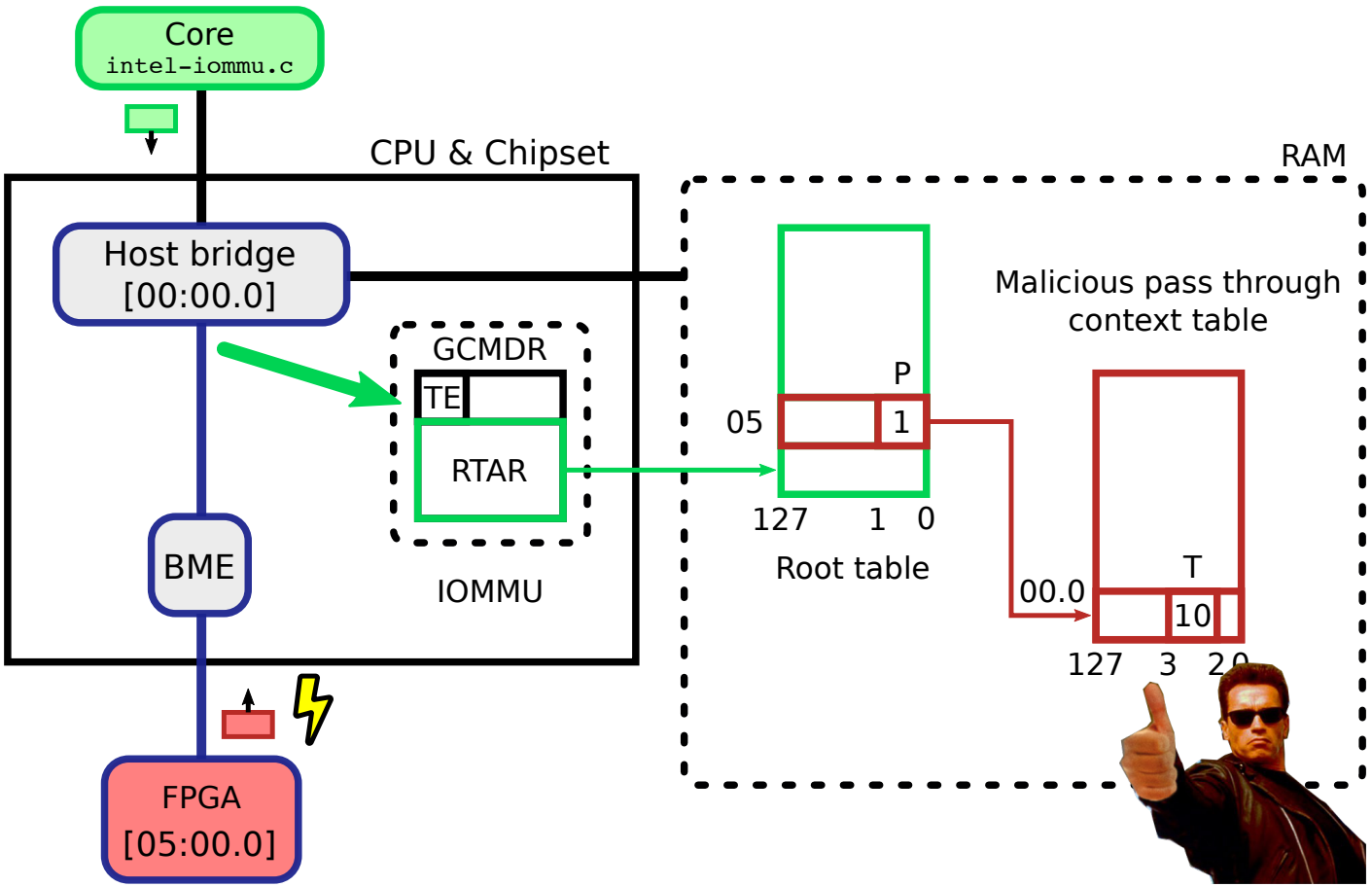
- Configuration de la *root table* légitime par le driver

Attaque du driver linux `drivers/intel-iommu.c`



- Écrasement de la *root entry* du FPGA malicieux

Attaque du driver linux drivers/intel-iommu.c



- Activation légitime du DMAR par le driver

Attaque : démonstration

- `http://homepages.laas.fr/nicomett/SSTIC2016/iommu-pwn-sstic.webm`

Plan

Conclusion et contremesures

- Les IOMMU ne sont toujours pas utilisées systématiquement par les systèmes opératoires pour effectuer du cloisonnement : Désactivée par défaut sous linux (Archlinux) et non utilisée sous windows, openbsd, etc.

- Revoir les responsabilités firmware / OS vis a vis de l'activation du DMAR
- Le bit BME des bridges, activé par le firmware dans la configuration standard, permettant de contrôler les accès DMA.
- Utiliser le démarrage sécurisé (Intel TxT) ?

Bypassing DMA remapping with DMA

Benoît Morgan, Guillaume Averlant,
Vincent Nicomette, Éric Alata

LAAS-CNRS, INSA Toulouse, Université de Toulouse

3 juin 2016

Références

[1] Yves-Alexis Perez and Loïc Duflot and Olivier Levillain and Guillaume Valadon, Quelques éléments en matière de sécurité des cartes réseau, Actes du 8ème symposium sur la sécurité des technologies de l'information et des communications (SSTIC), 2010