Analyse de l'efficacité du service fourni par une I/O MMU

Fernand Lone Sang, **Éric Lacombe**,
Vincent Nicomette, Yves Deswarte

LAAS - CNRS
Toulouse (France)

Juin 2010

LAAS-CNRS

Contexte et problématique (1/3)

Vecteurs d'attaque logique sur les composants d'un système informatique :

1. Depuis la CPU
   - Détournement de fonctionnalités du système par abus de privilèges
     - Logicielle
       → Chargeur de modules, périphériques virtuels (`/dev/kmem`), ...
     - Matérielle
       → Mode SMM, fonctionnalités non-documentées de la CPU, ...
   - Exploitation de failles de conception / développement
     - Logicielle
       → Débordements de tampons, chaînes de format, ...
     - Matérielle
       → *Bugs* de la CPU, *bugs* du *chipset*, ...
2. Depuis un contrôleur d'E/S
   - Détournement de fonctionnalités du système
     → Accès direct à la mémoire (DMA), ...
   - Exploitation de failles de conception / développement
     → Débordements de tampons dans les *firmwares*, ...

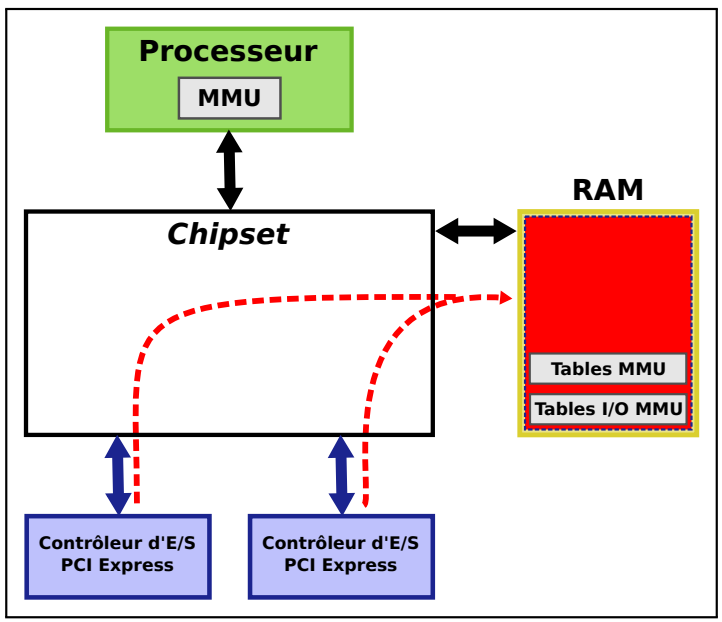
Contexte et problématique (2/3)

Accès direct à la mémoire (*Direct Memory Access* ou DMA) :

- Mécanisme de transfert de données entre contrôleurs d'E/S et mémoire
- Caractéristiques :
  - Nécessite un contrôleur spécifique pour effectuer le transfert
  - Décharge le processeur des transferts d'E/S

Les attaques de type DMA :

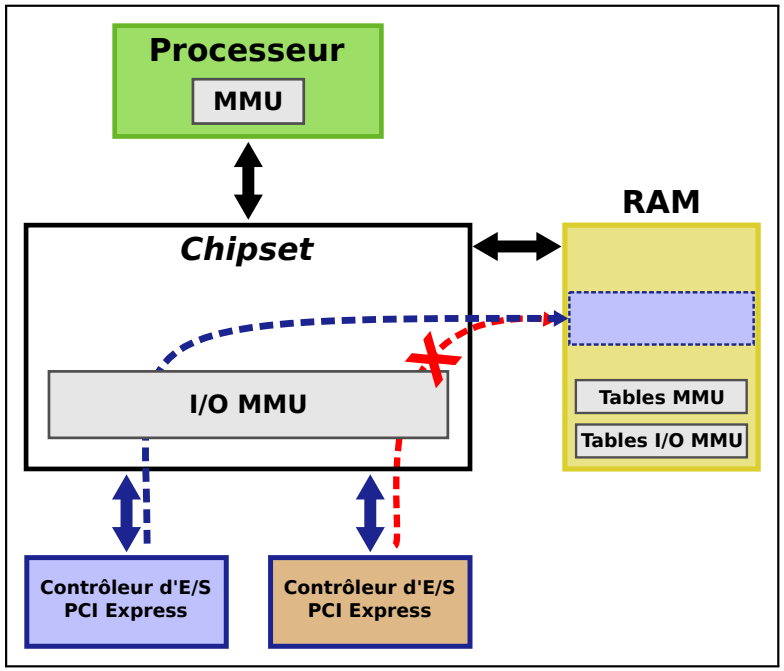
- Accès intégral à mémoire
- Exemples d'attaques FireWire :
  - M. Dornseif, PacSec'04
  - A. Boileau, Ruxcon'06
  - D. Aumaitre, SSTIC'08



Contexte et problématique (3/3)

Input/Output Memory Management Unit

- S'intercale entre les contrôleurs d'E/S et la mémoire
- Fonctionnement similaire à une MMU
  - Traduction d'adresse
  - Contrôle d'accès



Déroulement de la présentation

1. Description de la technologie Intel VT-d
2. Vecteurs d'attaque sur Intel VT-d
3. Exploitation d'une vulnérabilité matérielle : preuve de concept
4. Conclusion et perspectives

Déroulement de la présentation

Présentation d'Intel VT-d

Intel *Virtualization Technology for directed Input/Output* **(VT-d)**

- Implémente entre autres le principe d'I/O MMU
- Traduction de requêtes DMA issues des contrôleurs d'E/S
  - Adresse DMA virtuelle $\rightarrow$ Adresse DMA physique
- Contrôle de ces requêtes DMA

Architecture matérielle

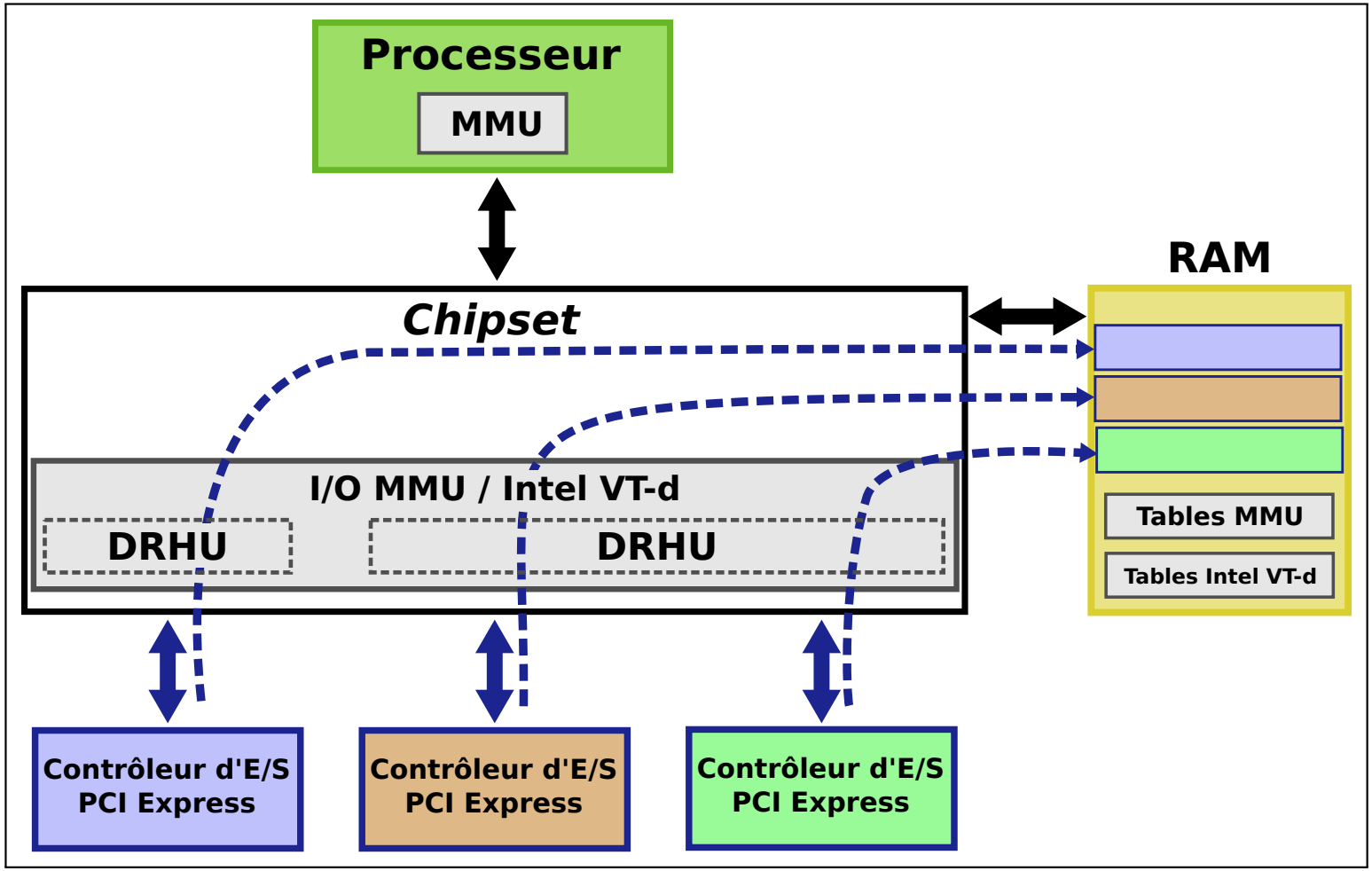
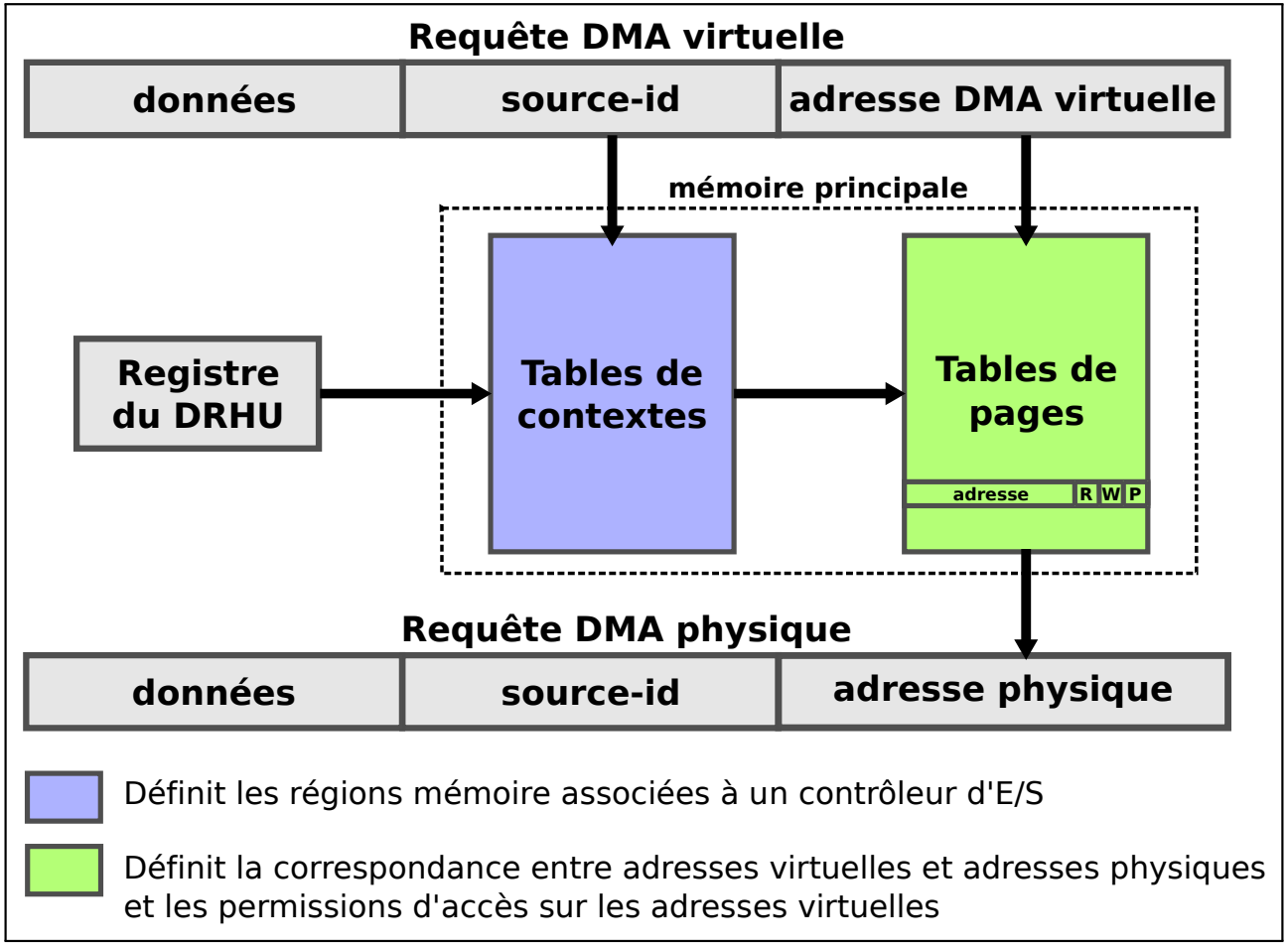


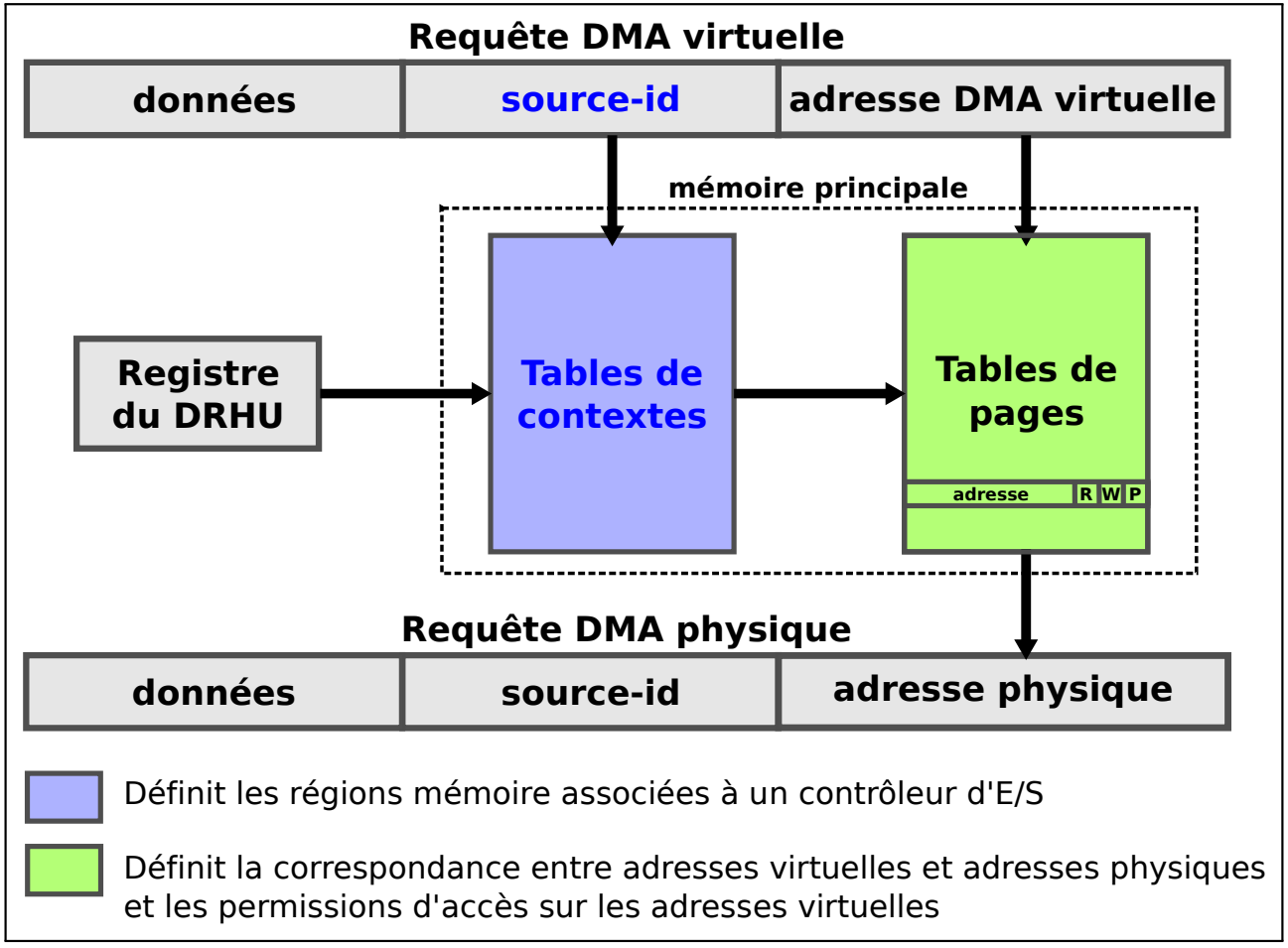
Figure: Intel VT-d se compose de *DMA Remapping Hardware Units (DRHU)*

Principe de fonctionnement d'Intel VT-d (1/3)



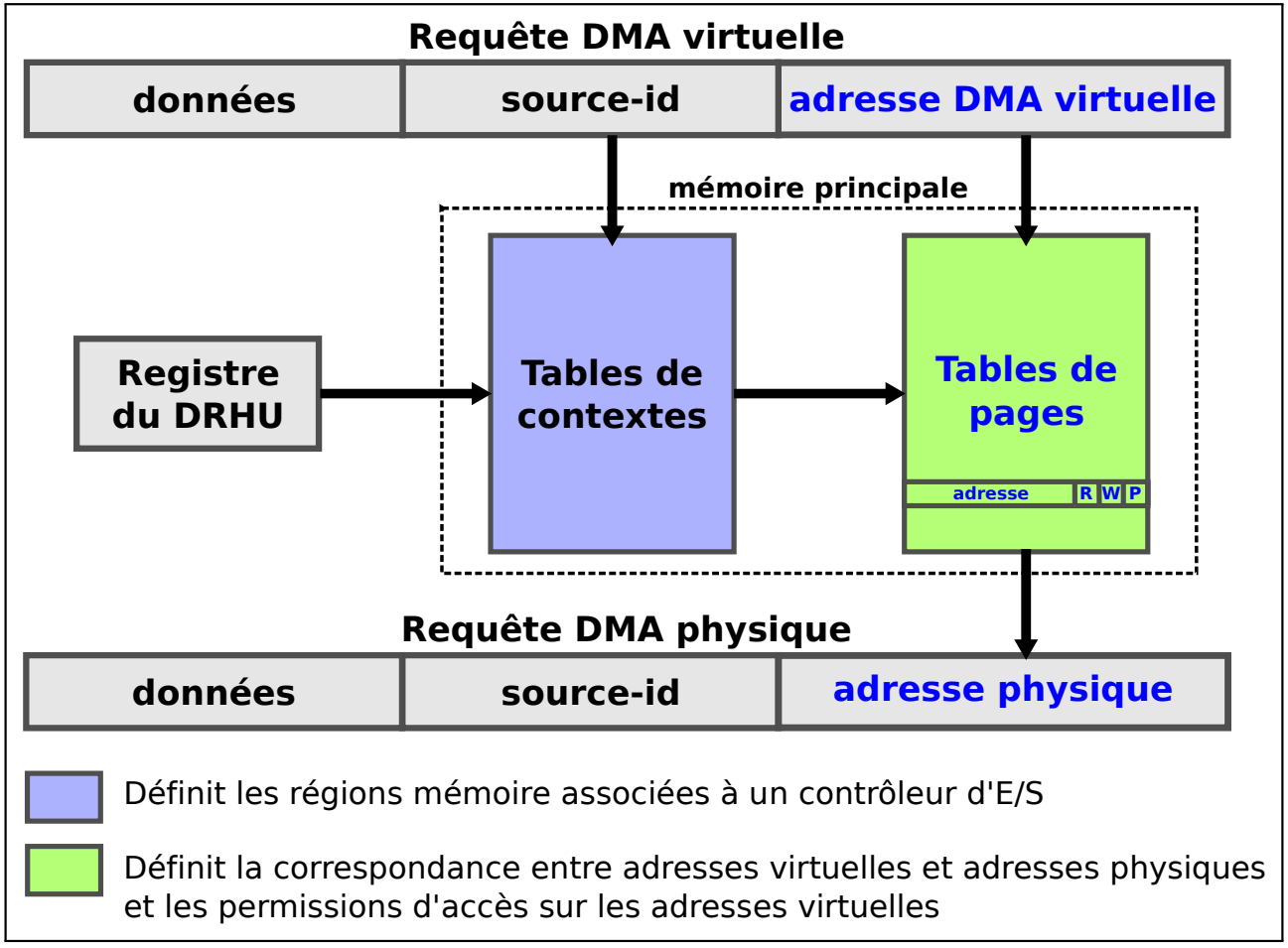
Vue simplifiée du fonctionnement d'une DRHU

Principe de fonctionnement d'Intel VT-d (2/3)



Vue simplifiée du fonctionnement d'une DRHU

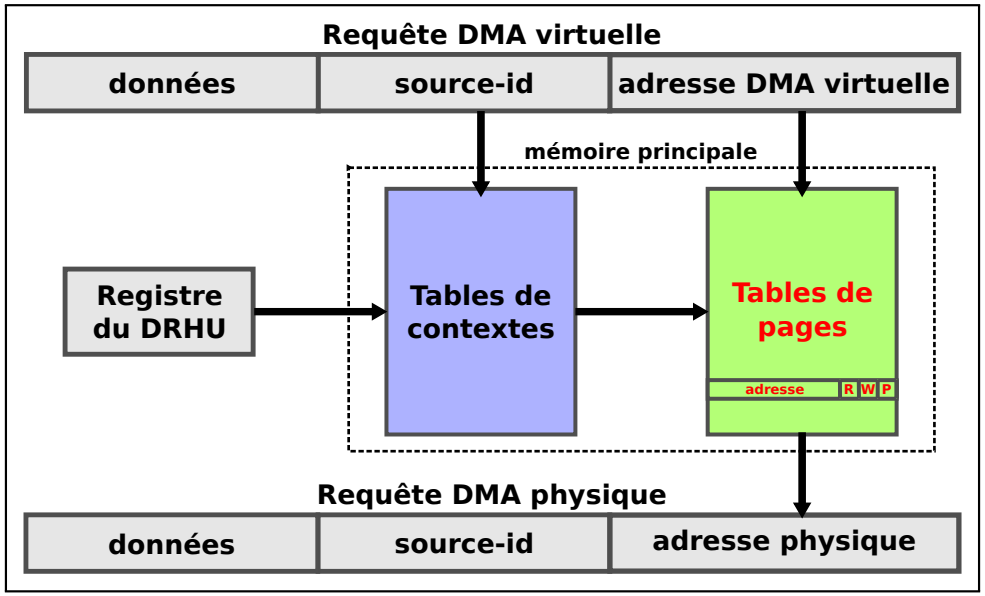
Principe de fonctionnement d'Intel VT-d (3/3)



Vue simplifiée du fonctionnement d'une DRHU

Déroulement de la présentation

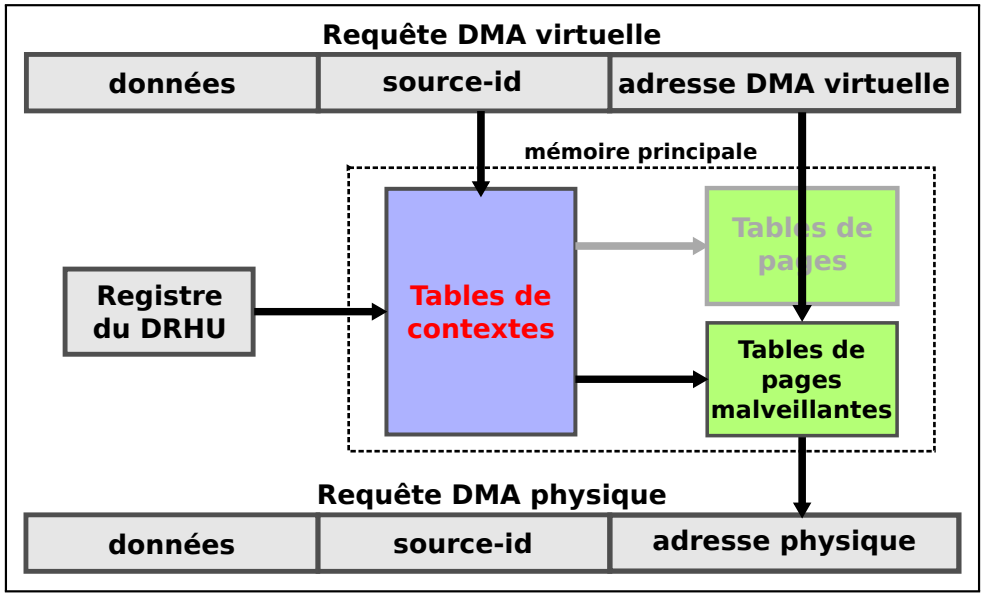
Modification de la configuration d'une DRHU (1/3)



Altération des tables de pages :

- Modification de la traduction d'adresses virtuelles en adresses physiques
  $\rightarrow$ Accès à de nouvelles pages physiques
- Modification des permissions d'accès d'un contrôleur d'E/S

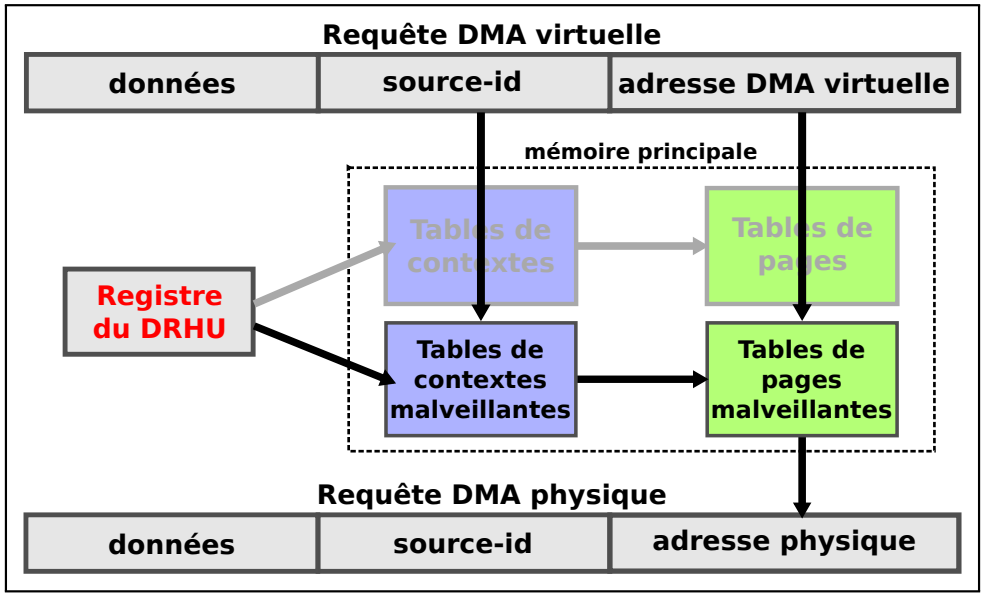
Modification de la configuration d'une DRHU (2/3)



Altération des tables de contextes :

- Pointe sur un nouveau jeu de tables de pages
  $\rightarrow$ Modification de l'association contrôleur d'E/S $\Leftrightarrow$ régions mémoire

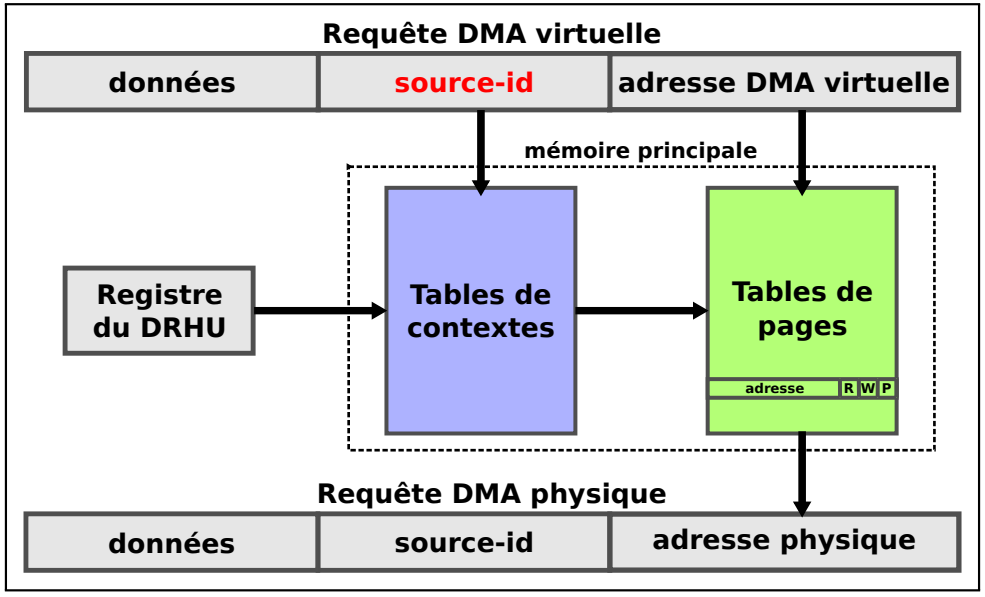
Modification de la configuration d'une DRHU (3/3)



Altération du registre d'une DRHU :

- Pointe vers un nouveau jeu de tables de contextes
  → Substitution de la configuration d'une DRHU
  → Plus difficile à détecter

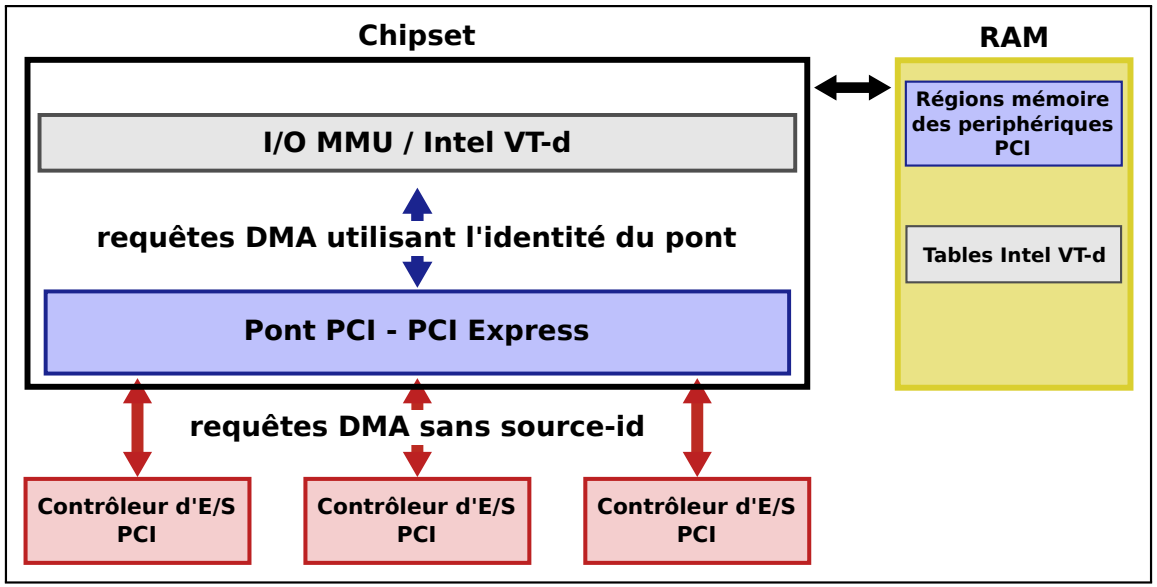
Exploitation des méta-données fournies par les contrôleurs d'E/S (1/2)



Usurpation de l'identité d'un contrôleur d'E/S :

- Modification du `source-id`
  → Accès aux régions mémoire associées à un autre contrôleur d'E/S

Exploitation des méta-données fournies par les contrôleurs d'E/S (2/2)



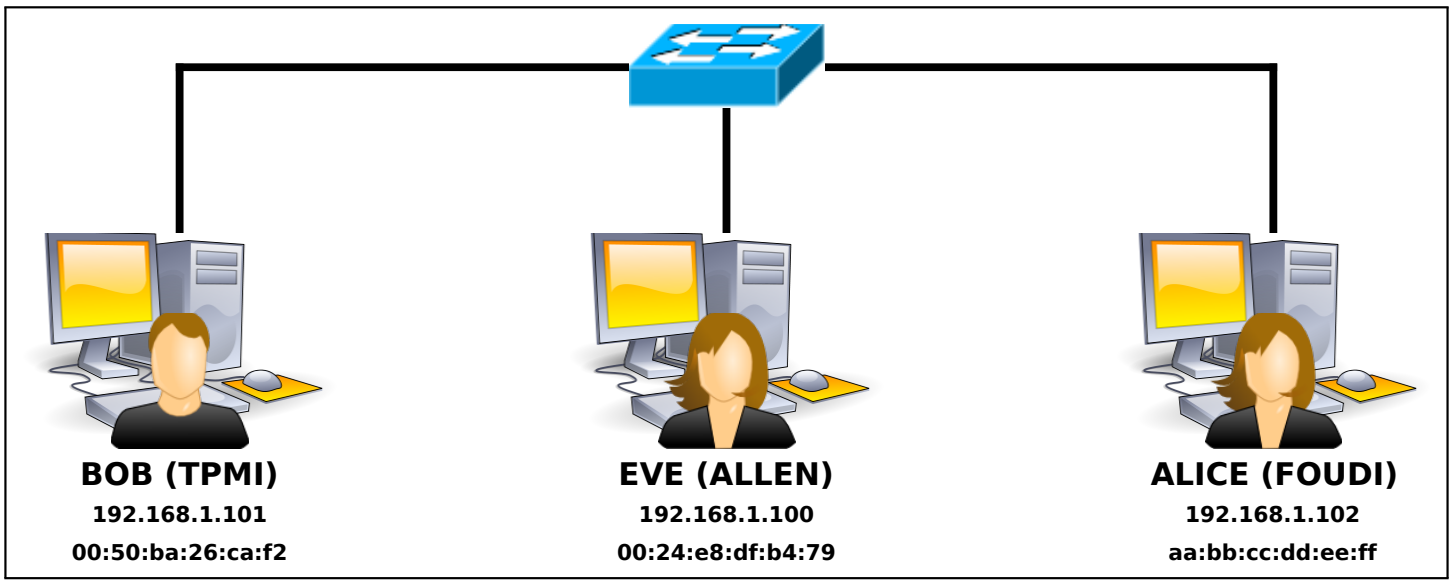
Partage d'identité entre contrôleurs d'E/S PCI :

- Dûe à la co-existence de bus PCI et PCI Express
  - Utilisation des mêmes tables de contextes
  - Accès aux mêmes régions mémoire
  - Mêmes permissions d'accès à ces régions

→ Altération de la mémoire d'un autre contrôleur d'E/S PCI possible

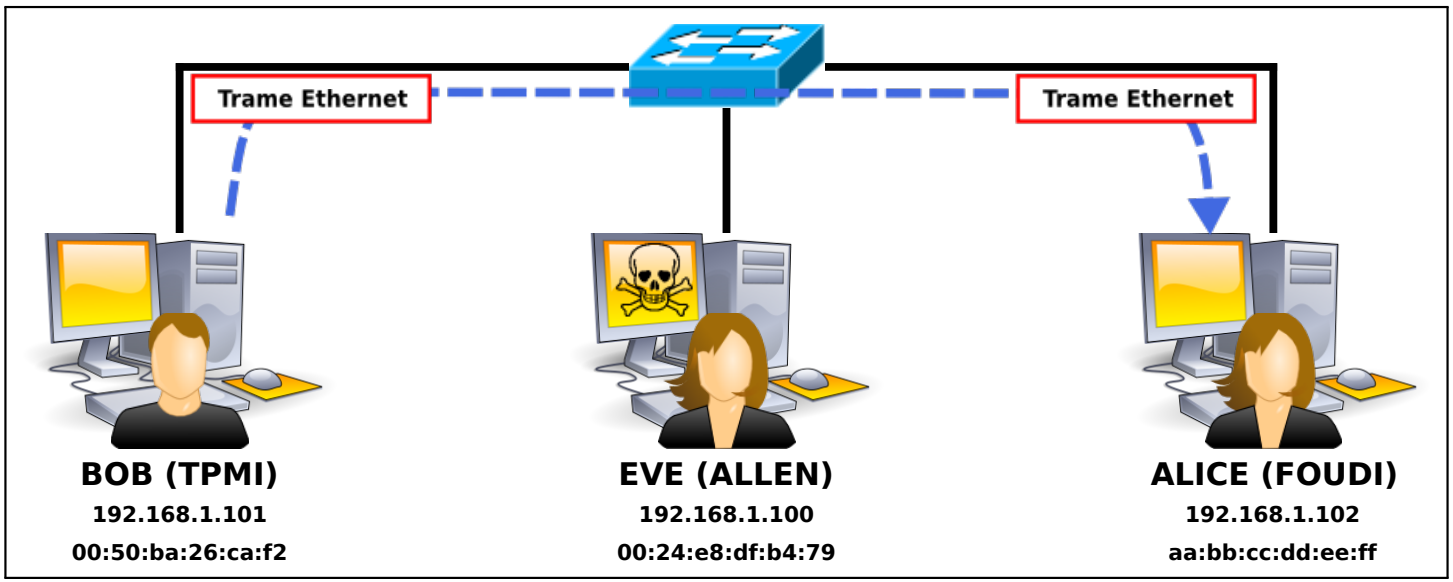
Déroulement de la présentation

Contexte (1/2)



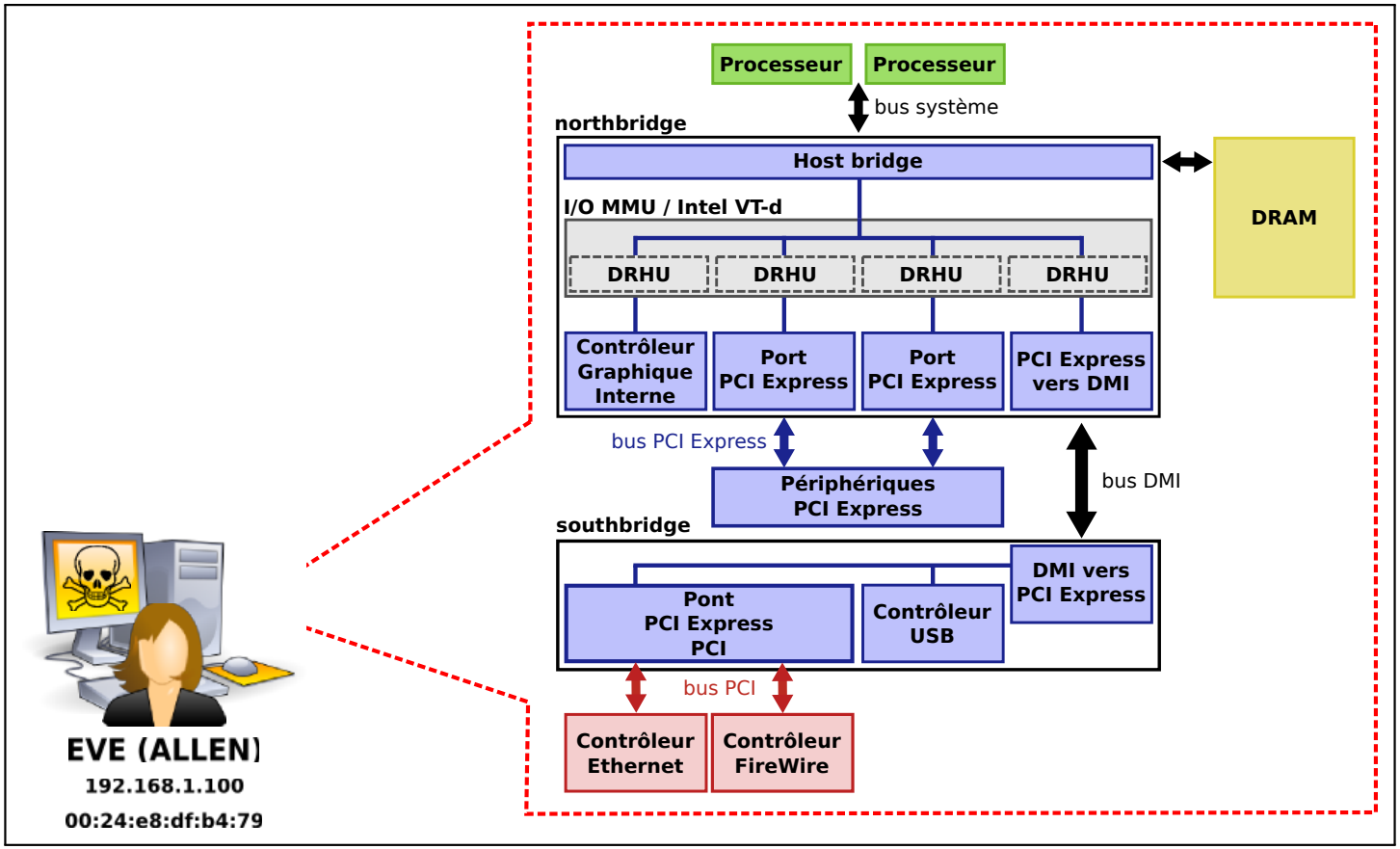
Cas d'étude : réseau d'entreprise avec des machines de configuration identique

Contexte (2/2)



Scénario : Ève souhaite faire de l'écoute sur le réseau

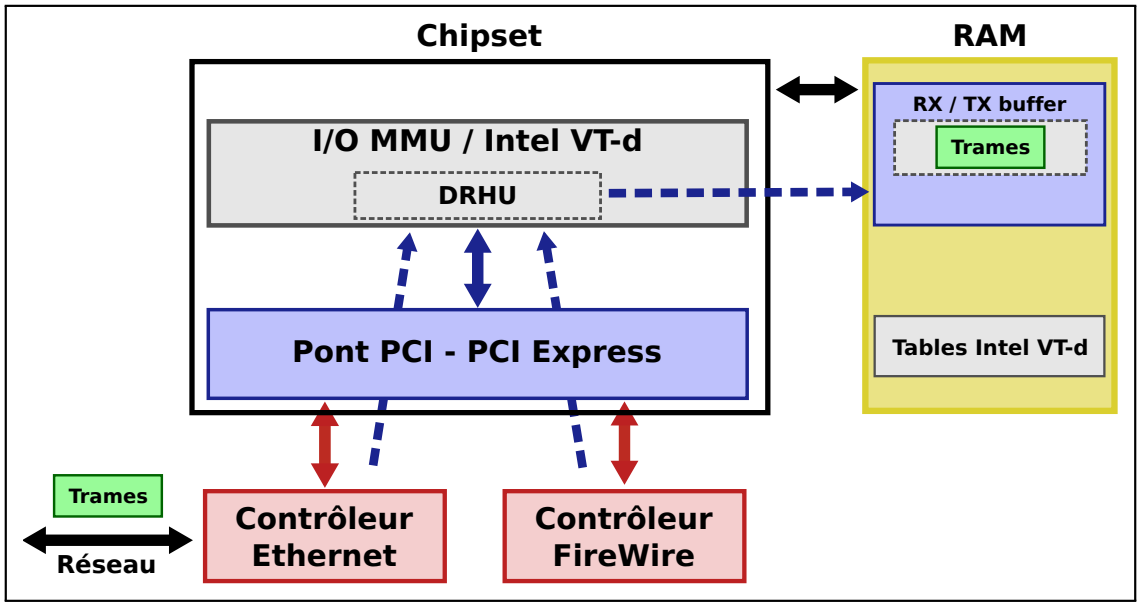
Mise en œuvre (1/4)



(1) Ève découvre que sa machine présente la vulnérabilité matérielle

(2) Ève déduit que les autres machines sont vulnérables (machines identiques)

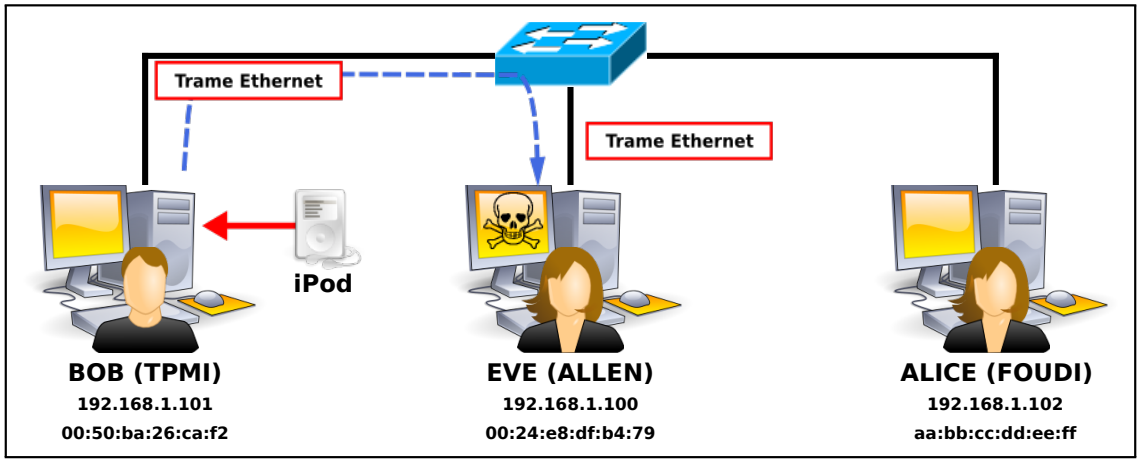
Mise en œuvre (2/4)



(1) Le contrôleur FireWire et contrôleur Ethernet partagent une même identité
→ Accèdent aux mêmes régions mémoire

(2) Le contrôleur FireWire peut modifier les trames Ethernet reçues

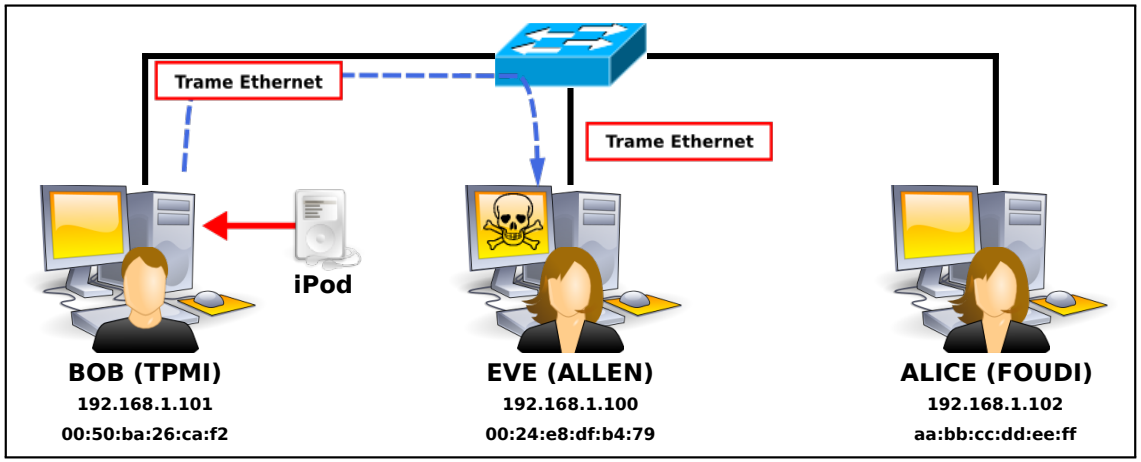
Mise en œuvre (3/4)



Détails de l'attaque :

1. Mise en place de l'attaque sur sa propre machine
   - Forger des paquets ARP à injecter
   - Localiser les régions mémoire utilisées par le contrôleur Ethernet
   - Programmer l'iPod pour injecter les trames malveillantes
2. Rejeu sur la machine de Bob
   - Prêter l'iPod à Bob
   - Recevoir les paquets réseaux détournés

Mise en œuvre (4/4)



Place à la démonstration

Déroulement de la présentation

Conclusion sur l'analyse de l'I/O MMU

Bilan sur la technologie Intel VT-d

- Point fort :
  - Efficace dans la majorité des cas contre les attaques DMA
- Limites :
  - Partage d'identité (`source-id`) entre contrôleurs d'E/S PCI possible
  - Nécessite d'avoir confiance en d'autres contrôleurs d'E/S
    $\rightarrow$ `source-id` fourni est correct
  - Ne contrôle pas les échanges internes au *southbridge*
    (ex : transactions `Peer-to-Peer`)

Recommandations

- Utilisation conjointe d'Intel VT-d avec d'autres technologies
  $\rightarrow$ Intel VT-x, Intel TxT, ...
- Connexion d'au plus un contrôleur d'E/S PCI par pont PCI-PCI Express

Perspectives aux travaux

1. Étude de la faisabilité de l'usurpation d'identité d'un contrôleur d'E/S
2. Étude de la possibilité de reconfigurer une DRHU depuis un contrôleur d'E/S
3. Analyse des attaques potentielles utilisant les transactions `Peer-to-Peer`
4. Développement de contre-mesures aux attaques précédemment citées

Merci de votre attention