ENSEEIHT **3e année**
UE à choix sécurité **TP**

Attaques side channel temporels - *caches attacks*

19 octobre 2020

Ce TP a pour but de mettre en œuvre un *covert channel* et un *side channel*, à l'aide des classes d'attaques Flush+Reload et Prime+Probe.

Si vous travaillez sur machines virtuelles hors de la salle réseau

Depuis x2go ou sur une machine normale :

```
$ mkdir /work/fw
$ cd /work/fw
$ wget -c 'http://flash.enseeiht.fr/bemorgan/lubuntu-18.04.15-side.tgz'
$ tar xvf lubuntu-18.04.15-side.tgz
$ cd lubuntu-18.04.15-side
# sudo si vous n'avez pas le droit de créer des interfaces et de changer kvm
$ ./start.sh
```

Si vous travaillez dans les salles réseau / sécurité

En avant Guingamp.

1 Objectifs

Dans ce TP, nous allons successivement mettre en place un canal caché entre deux processus linux utilisant une mémoire partagée et sans mémoire partagée en mettant en œuvre une attaques Flush+Reload et Prime+Probe.

Par le suite, nous allons attaquer une implémentation cryptographique triviale à la fois en Flush+Reload et Prime+Probe.

2 Préparations

Dans cette partie du TP nous allons réaliser les étapes préalables à l'exécutions de nos attaques. Nous allons notamment identifier le processeur, préparer l'allocateur mémoire, constuire notre environement de travail en C et évaluer les temps d'accès à la mémoire.

2.1 Identification du processeur

Une étape préalable à la réalisation des attaques side channel est de connaître les paramètres de mémoire cache de notre processeur. Nous devons donc extraire le nombre de niveaux de cache, la taille d'une ligne de cache, le nombre de cœurs physiques et la taille du bus d'adresse physique :

— c : nombre de cœurs physiques

— N : nombre de niveaux de cache

— l : taille d'une ligne de cache

Si ces niveau sont partagés et enfin les paramètres de correspondance suivants :

— S_k : taille du cache

— s_k : nombre de sets

— n_k : associativité des sets

— partagé$_k$: niveau partagé entre les cœurs ?

2.1.1 Nombre de cœurs physiques

Le fichier spécial `/proc/cpuinfo` permet de récupérer le nomre de cœurs physiques du processeur.

```
$ cat /proc/cpuinfo | grep 'cpu cores' | uniq
```

Question 1: Récupérez le paramètre c à l'aide de ce fichier

Le système de fichier `/sys/devices/system/cpu/cpu0/cache/` permet d'identifier les paramètres N et l.

```
$ ls /sys/devices/system/cpu/cpu0/cache/
```

Question 2: Naviguez dans les dossiers `index*` et affichez le contenu des fichiers : `coherency_line_size` et `level` pour trouver les paramètres N et l.

Question 3: Pour

2.1.2 Nombre de niveaux de cache

2.2 Préparation de l'allocateur mémoire

Comme nous l'avons vu en cours, il est nécessaire de pourvoir manipuler les bits de sets d'un adresse physique. Or, plus la taille de page d'adresse virtuelle est petite, moins les bits de set sont directement accessibles 2.2.

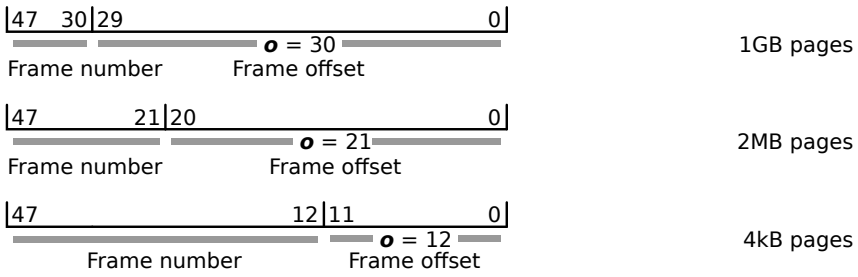

FIGURE 1 – Tailles des pages sur processeur Intel x86