Meltdown

Nathan Verdier
Lucie Bedouret
Chloé Mourgand
Thomas Chazot
Rémi Regnault

Qu'est-ce que c'est ?

- Processeurs
  - exécution spéculative => tous depuis 1995
- Faille
  - mémoire utilisateur || mémoire noyau
- Découverte
  - Chercheurs de google
  - 1er janvier 2018
    - => émission code CVE (Common Vulnerabilities and Exposures)
- Exploitée ?

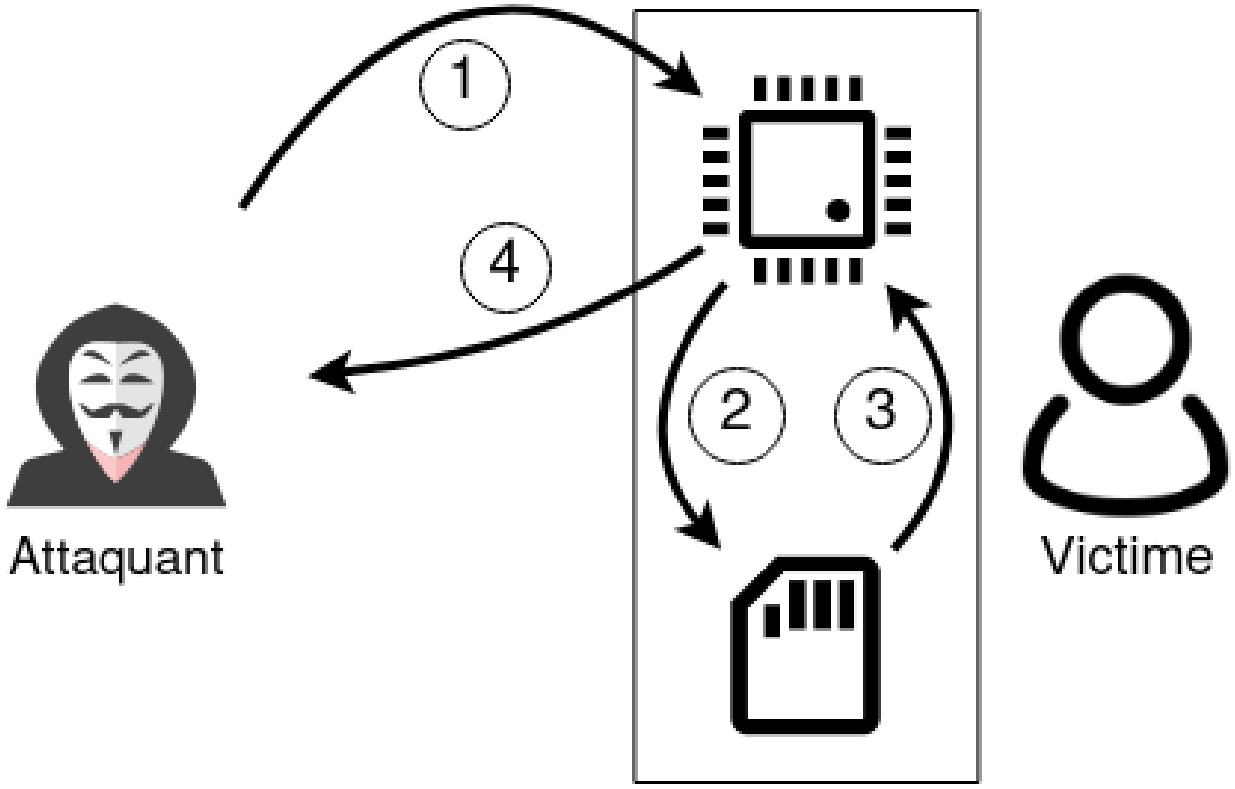
Exécution Spéculative

Exécution Spéculative

Anticipation pour gagner du temps lorsqu'il y a plusieurs possibilités d'opération

Exemple

- 2 branches possibles (A et B)
- Prédiction A est plus rapide
- Processeur => exécute A
- Finalement, A trop lent
- Processeur => annule les opérations et exécute B



Concrètement

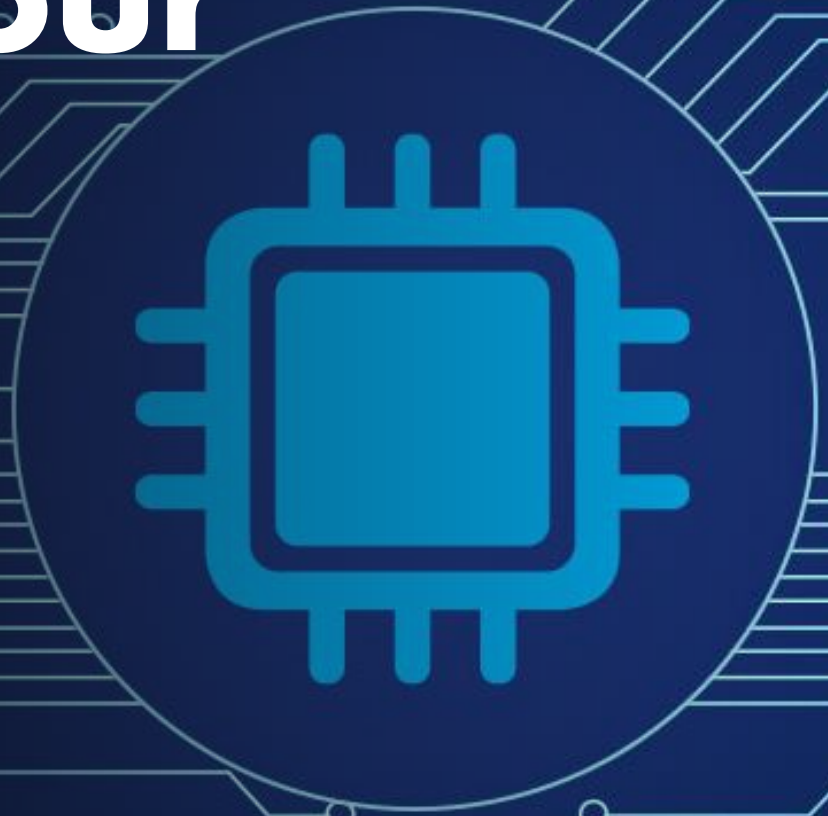
- Exécution du programme par le noyau
- Récupération des données stockées en mémoire
- Envoie des données à l'attaquant

Correctifs

- Plus grande séparation mémoire utilisateur/processus
- Fonctionnement de l'exécution spéculative modifiée

➡ Diminution des performances

Merci pour votre écoute



Nathan Verdier

Lucie Bedouret

Chloé Mourgand

Thomas Chazot

Rémi Regnault