

# Un algorithme pour concevoir des processeurs sans faille matérielle

Par *mogirard*

Créé le 23/05/2019 - 07:32

## Un algorithme pour concevoir des processeurs sans faille matérielle

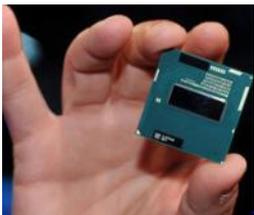
Jeudi, 23/05/2019 - 06:32 [0 commentaire](#)

- [Diminuer la police](#)
- [Augmenter la police](#)
- [Imprimer](#)
- [Version PDF](#)

- 
- 
- 
- 

[Tweeter](#)

0 avis :



[zoom](#)

Début 2018, la découverte des failles matérielles de sécurité informatiques Spectre et Meltdown a semé la panique chez les constructeurs de microprocesseurs. Ces failles ont mis en lumière la dangerosité des attaques dites par canaux cachés, qui permettent de récupérer des informations en observant le fonctionnement matériel ? et non logiciel ? d'une puce.

Des chercheurs de l'Université technologique de Kaiserslautern, en partenariat avec Stanford, ont élaboré un système mathématique permettant de détecter ce type de faille pendant la conception d'un processeur. Cet outil leur a permis d'identifier de telles failles dans des puces largement utilisées dans l'Internet des objets (IoT) et la conduite autonome.

Les algorithmes de chiffrement des données fonctionnent sur la couche matérielle d'un système informatique : lorsqu'ils sont activés, ils utilisent les composants électroniques du système pour effectuer des calculs et interagir. Les attaques dites matérielles se fondent sur l'observation des phénomènes physiques impliqués pour en déduire le fonctionnement des algorithmes de protection, afin de les

contourner.

Les attaques par canaux cachés sont des attaques matérielles particulières, lors desquelles un logiciel malveillant obtient directement les informations protégées par les algorithmes en analysant le fonctionnement des composants d'un système.

Pour faire face à ce type d'attaque, les chercheurs ont défini un algorithme nommé **Unique Program Execution Checking**, ou UPEC. « C'est une forme de vérification automatisée de la sécurité, qui va alerter les concepteurs d'une faille potentielle dans leur microarchitecture, bien avant que la puce ne soit produite en masse », explique le professeur de l'université de Kaiserslautern, Wolfgang Kunz, dans un communiqué de presse de l'université.

L'algorithme analyse les répercussions de chaque décision de conception sur la microarchitecture d'un processeur et détecte si elles peuvent être exploitées. « Le point clé est que même les étapes simples du design, comme ajouter ou enlever de la mémoire tampon, peuvent introduire par inadvertance une vulnérabilité aux canaux cachés, sur à peu près n'importe quel processeur », détaille le chercheur Mo Fadiheh.

Selon les chercheurs, l'UPEC a l'avantage d'être exhaustif. Il prend en compte tous les programmes qui peuvent fonctionner sur un processeur donné pour faire son analyse et peut permettre la détection de n'importe quelle vulnérabilité sur une puce en conception.

Article rédigé par Georges Simmonds pour RT Flash

[L'Usine Nouvelle](#)

**Noter cet article :**

**Recommander cet article :**

- 
- [Tweeter](#)
- 
  
- **Nombre de consultations :** 0
- **Publié dans :** [Informatique](#)
- **Partager :**
  - [Facebook](#)
  - [Viadeo](#)
  - [Twitter](#)
  - [Wikio](#)

[Informatique](#) [données](#) [faille informatique](#) [microprocesseurs](#) [piratage](#) [puces](#)

---

URL source: <https://www.rtfash.fr/algorithme-pour-concevoir-processeurs-sans-faille-materielle/article>