Microarchitectural Attacks On Ubiquitous Systems
MIAOUS

anr agence nationale de la recherche

Appel : AAPG

Année : 2019

Instrument : JCJC

Contact :
clementine.maurice@inria.fr
https://miaous.cmaurice.fr/

COORDINATRICE : Clémentine Maurice

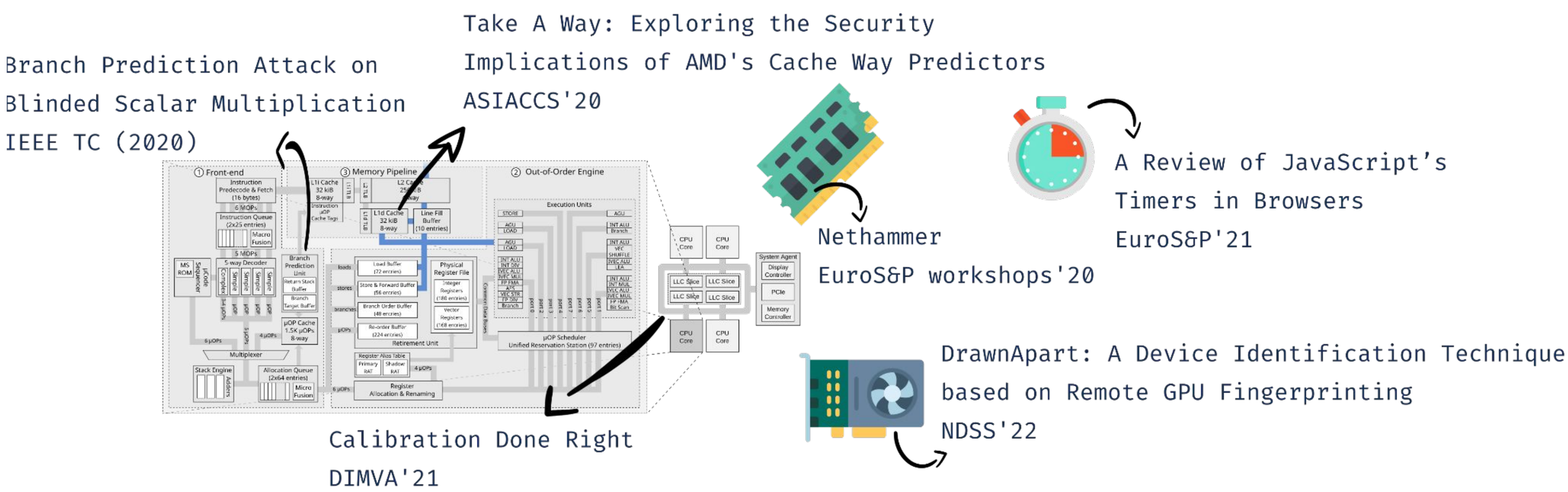
PARTENAIRES : IRISA (Rennes)

Ce projet s'intéresse à la sécurité des systèmes d'information et à la protection de la vie privée dans l'interaction entre le logiciel et le matériel, et en particulier aux fuites d'informations par canaux auxiliaires qui sont dues à la micro-architecture des processeurs, ainsi qu'à la construction de nouvelles contre-mesures.

CONTEXTE ET OBJECTIFS

Le matériel est souvent considéré comme une couche abstraite qui se comporte correctement. Cependant, les effets de bord dus à l'implémentation du logiciel et à son exécution sur le matériel réel peuvent causer des **fuites d'informations par des canaux auxiliaires**, ce qui entraîne des vulnérabilités critiques, affectant à la fois la sécurité et la confidentialité de ces systèmes. Le projet MIAOUS vise en particulier les fuites d'informations qui ne nécessitent pas la proximité physique des appareils et qui sont dues à la microarchitecture des processeurs, ainsi que la construction de nouvelles contre-mesures.

L'objectif principal de ce projet est de proposer un cadre générique permettant une meilleure compréhension de la surface d'attaque des attaques microarchitecturales, tant du côté matériel que logiciel, ainsi que des outils permettant de fermer cette surface d'attaque. Nous travaillons sur trois axes : (1) la **rétro-ingénierie** des composants microarchitecturaux, (2) la systématisation de la **découverte de canaux auxiliaires** dans la microarchitecture, et (3) la **détection automatique de vulnérabilités** liées aux canaux auxiliaires dans les logiciels.



MÉTHODOLOGIE ET RÉSULTATS

Méthodologie : Expérimentations sur différents appareils et différentes microarchitectures : Intel, AMD, appareils mobiles…

Collaborations internationales : TU Graz (Autriche), Ben Gurion University (Israel), Adelaide University (Australie), IIT Kharagpur (Inde), NTU (Singapour).

Résultats majeurs du projet : 6 articles scientifiques. Résultats consolidés sur la rétro-ingénierie, et travaux en cours sur la détection automatique de vulnérabilités. Ouverture sur les attaques sur les navigateurs et les conséquences sur la vie privée.

Autres retombées : nouvelle ANR PRCI avec CISPA (Allemagne) sur les attaques microarchitecturales et le fingerprinting sur les navigateurs web.

---

cnrs UMR IRISA