UMR IRISA

Scientist who joined IRISA

2017

Institut de Recherche en Informatique et Systèmes Aléatoires

Clémentine MAURICE

D1 - Large Scale Systems (LSS)

EMSEC

Short BIO

Clémentine Maurice is working as a CNRS researcher (CR2) in the EMSEC team. Her research focuses on the security of computing systems, and more precisely on the interaction between hardware and software. Among other topics, she is interested in micro-architectural side channels and software fault attacks in commodity computers, servers, and mobile devices, as well as reverse-ngineering processor parts, and fingerprinting everything.

She obtained her PhD (CIFRE) from Telecom ParisTech in October 2015, while working at Technicolor in Rennes, jointly with the S3 group of Eurecom in Sophia Antipolis. She then worked as a postdoctoral researcher in the Secure Systems group at the Graz University of Technology in Austria.

Short BIO

Parcours professionnel

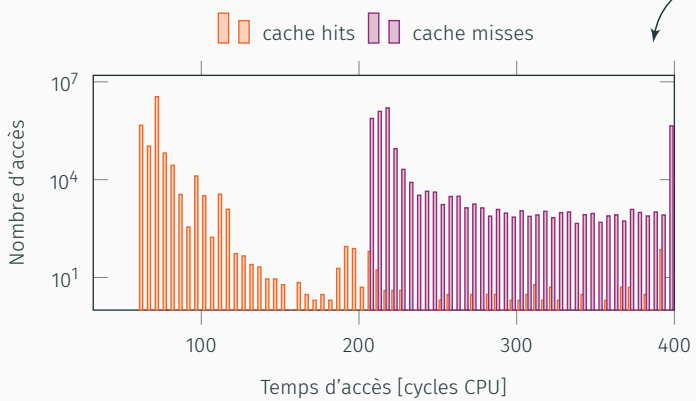
- Clémentine Maurice
- Depuis Octobre 2017 : CR2 CNRS dans l'équipe EMSEC
  - → Sécurité des systèmes d'informations : interaction entre matériel et logiciel, attaques sur la micro-architecture
- Février 2016—Août 2017 : postdoctorat à TU Graz, Autriche
- Octobre 2015 : thèse CIFRE, Technicolor/Eurecom (Rennes/Sophia Antipolis)

Research project

Domaine de recherche : Attaques sur la micro-architecture

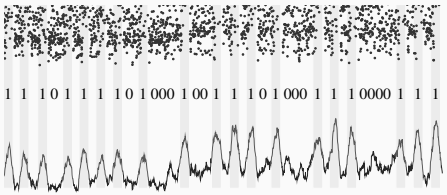
- Matériel habituellement modélisé comme couche abstraite correcte, mais attaques possibles
  - Par faute : contourner les protections logicielles par des erreurs sur le matériel
  - Par canal auxiliaire : observer les effets de bord du matériel sur les calculs

identification



→

attaque



- récupérer clés secrètes, intervalles de frappes de clavier
- contourner sécurité système (ASLR)

Research project

Projet de recherche

"Analyse des attaques liées à la micro-architecture et contre-mesures"

Enjeu

Sécurité des systèmes face aux attaques sur la micro-architecture

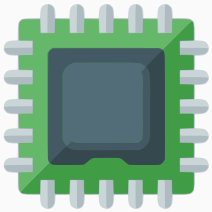
Obstacles principaux

- Surface d'attaque matérielle et logicielle mal connue
- Problèmes d'adoption des contre-mesures proposées : performance, coût, passage à l'échelle

Research project

Verrou scientifique et axes de recherche

Comment contrer des attaques basées sur des optimisations matérielles, sans réduire les performances apportées par ces optimisations ?



1. Analyser la surface d'attaque matérielle

2. Détecter les vulnérabilités logicielles

3. Mettre au point de nouvelles contre-mesures

Research project

Axe #1 : Analyser la surface d'attaque matérielle

Problème #1 : *Manque de documentation du matériel*

→ **Rétro-ingénierie du matériel** COURT TERME

Problème #2 : *Canaux auxiliaires découverts manuellement*

→ **Automatisation de la découverte de canaux auxiliaires** COURT/MOYEN TERME

Problème #3 : *Peu d'études sur les attaques par fautes purement logicielles*

→ **Investigation de nouvelles attaques par fautes** PROSPECTIF/LONG TERME

Research project

Axe #2 : Détecter les vulnérabilités logicielles

Problème #1 : *Méthodes d'analyse statique basées sur des hypothèses pouvant être insuffisantes, changeantes ou fausses : faux négatifs en pratique*

→ **Nouvelles méthodes d'analyse dynamique des vulnérabilités** MOYEN TERME

Problème #2 : *Solutions ciblant uniquement la sécurité, et non la vie privée*

→ **Protection de la vie privée** COURT TERME

Research project

Axe #3 : Mettre au point de nouvelles contre-mesures

Problème #1 : *Peu probable de voir une disparition des canaux auxiliaires*

→ Environnements d'exécution sécurisés considérant les canaux auxiliaires

MOYEN/LONG TERME

Problème #2 : *Difficile d'isoler tous les composants d'un système*

→ Mesures matérielles ou applicatives ciblant les portions de code sensible

MOYEN/LONG TERME