Overview of micro architectural attacks and application to a RISC-V core

Yannick Teglia*[1]

[1]Thales DIS – Thales DIS France SAS – France

Résumé

Over the past decades the electronic devices have been facing several threats. Initially logical attacks were using software means to steal secrets of users from applications like the Morris worm in 1988. Then in the late 90's side channel attacks took advantage of physical leakages to recover information while requiring a physical access to the device, such as the famous DPA of Paul Kocher and many others came after. More recently software based hardware attacks like Rowhammer and SideLine allowed the bad guys to remotely turn the internal resources of victim device into means of fault injection or eavesdropping using malicious software.

In the same spirit micro architectural attacks make use of malicious code located on the victim device to steal secrets by leveraging the innermost parts of the CPU as the data cache or other internal buffers as the source of leakage. While the first attack of this kind was reported in 2006, it was in 2018 that those threats gained momentum through the famous Spectre and Meltdown targeting Intel CPUs. The number of attacks never stopped growing, now threatening all high-end CPUs by turning their own computational speed-up capabilities into leakage generators.

In this talk we will propose an overview of the micro architectural attacks, a description of their behaviour as well as some counter-measures. We will conclude by a recent application on a 64-bit RISC-V CPU, the CVA6.

*Intervenant