Micro-architectural attacks: from CPU to browser

Clémentine Maurice*[1]

[1]CNRS, CRIStAL, Lille – Centre National de la Recherche Scientifique - CNRS – France

Résumé

Hardware is often considered as an abstract layer that behaves correctly, just executing instructions and outputing a result. However, the internal state of the hardware leaks information about the programs that are executing, paving the way for covert or side-channel attacks. Many micro-architecural components can be used for such attacks; in particular, the CPU cache has been a target highly studied in the last years.
In this presentation, we will first cover the evolution of micro-architectural attacks, having a look at a historical recap of past attacks and how the field evolved in the last years. We will then focus on how to mount these attacks from web browsers. Indeed, micro-architectural attacks require precisely monitoring low-level hardware features. In contrast, browsers only provide high-level sandboxed languages with a limited set of functions. Porting these attacks to the web thus exposes a series of challenges.

*Intervenant