Abstract:
Hardware is often considered as an abstract layer that behaves correctly, just executing instructions and outputting 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. Yet, the internal state of a CPU is tightly tied with its micro-architecture, which is becoming increasingly complex and is often undocumented by manufacturers.

In this talk, we present methods to reverse-engineer modern CPU components. In the first part, we present one automatic and generic method to reverse engineer the addressing function of the last-level cache in Intel CPUs, using performance counters. As the last-level cache is shared between cores, we then explain how to use this function in a cross-core side-channel attack. In the second part, we focus on the DRAM addressing function on both x86 and ARM CPUs. We then demonstrate covert and side-channel attacks across CPUs without any shared memory, leveraging DRAM row buffers.

Bio:
Clémentine Maurice is a system security researcher working for CNRS, in the EMSEC research group at IRISA (Rennes, France). Previously, she worked as a postdoctoral researcher in the Secure Systems group at the Graz University of Technology, Institute of Applied Information Processing and Communications, in Austria. She obtained a PhD from Telecom ParisTech in 2015 while working at Technicolor in Rennes, jointly with the S3 group of Eurecom in Sophia Antipolis. Among other topics, she is interested in microarchitectural covert and side channels in commodity computers and servers, reverse-engineering processor parts, virtualization security and fingerprinting systems.