In Grenoble, in the center of the Alps, LETI is an applied research institute in micro and nano technologies, information technologies and health.
As a privileged interface between the industrial world and academic research, it ensures each year the development and transfer of innovative technologies in various sectors through research programs using our technological platforms.

Funded PhD (2023-2026)

Management of Spectre and Meltdown data leakage in a RISC-V Out of Order processor

Since 2018 and the announcement of the Spectre[1] and Meltdown[2] vulnerabilities, the hard-won performance gains of desktop and server processors over the past decades have been called into question. These vulnerabilities effectively exploit the speculative and out of order execution found in all modern processors to gain in the number of instructions performed per clock cycle. These types of execution open the door to transient microarchitectural changes that can be disclosed due to shared resources within the pipeline and caches and the presence of covert channels that allow the extraction of leaked data. The latter can be caches but also other internal buffers.
The objectives of the PhD will be to understand these mechanisms through the implementation of attacks and leakage evaluation systems via for example the mutual information calculation.
Then, for each leak and each microarchitecture (branch prediction, prefetcher, TLB, Load Store unit, execution stage, caches,...), we will have to find the approach that penalizes the least performance. An implementation of these countermeasures is planned on the open source NaxRiscV[3] 64 bits processor and Out of Order written in the SpinalHDL language which allows to host and test them with a great modularity.
The resolution of these problems can both take advantage of the work done in the laboratory on authenticated memory encryption and the partitioning in the pipeline of data and instructions according to the processes executed. Logical elements will also have to be added to ensure the boundary between the different processes inside the CPU. Finally, random addressing and/or highly selective eviction techniques will be used for microarchitectural components where partitioning would be too costly, especially in caches. Finally, the implemented countermeasures will have to be characterized with respect to the developed evaluation tools.
This thesis will be carried out within the large PEPR Cybersecurity project gathering most of the French laboratories working around hardware security, allowing to work in a very motivating environment.

[1] P. Kocher *et al.*, "Spectre Attacks: Exploiting Speculative Execution." arXiv, Jan. 03, 2018. doi: 10.48550/arXiv.1801.01203.
[2] M. Lipp *et al.*, "Meltdown." arXiv, Jan. 03, 2018. doi: 10.48550/arXiv.1801.01207.
[3] https://github.com/SpinalHDL/NaxRiscv

Laboratory : LETI/DSYS/SSSEC/LSCO/TIMA
Address: 17 avenue des Martyrs
38054 GRENOBLE cedex 9
Contact : olivier.savry@cea.fr
giorgio.di-natale@univ-grenoble-alpes.fr

Required Training :
Digital design, computer architecture, security

Start date : possible as early as March 2023