Université Bretagne Sud

ubs : Lab-STICC

## (MS-Project)
## Sujet-01: Implementation of Cache-based Timing Side-Channel Attacks in Multi- & many-core systems

Computers are increasingly handling sensitive data (banking, voting), while at the same time we consolidate more services, sensitive or not, on a single hardware platform. This trend is driven both by cost savings and convenience. The most visible example is the cloud computing—infrastructure-as-a-service (IaaS) cloud computing supports multiple virtual machines (VM) on a hardware platform managed by a virtual machine monitor (VMM) or hypervisor. These co-resident VMs are mutually distrusting, for instance, high-performance computing software may run alongside a data centre for financial markets, requiring the platform to ensure confidentiality and integrity of VMs. In such execution scenario, a potentially malicious VM, running alongside a co-resident VM, could possibly deny services to that co-resident VM, which could be costly.

Side-Channel Attacks (SCAs) are a powerful method for breaking theoretically secure cryptographic primitives. These attacks have been used extensively to break the security of numerous cryptographic implementations. At a high level, it is possible to distinguish between two types of side-channel attacks, based on the means used by the attacker: hardware based attacks which monitor the leakage through measurements (usually using dedicated lab equipment) of physical phenomena such as electromagnetic radiation, power consumption, or acoustic emanation, and software based attacks which do not require additional equipment but rely instead on the attacker software running on or interacting with the target machine. Examples of the latter include timing attacks, which measure timing variations of cryptographic operations and cache attacks, which observe cache access patterns.

In this project, we want to implement some selected software cache-based timing SCAs and deploy them on real computation & crypto-systems in order to analyze their efficiency and potential threat level. The research group has expertise in analyzing SCAs and developing countermeasure solutions for such SCAs. This project will be conducted under the supervision of Dr. Vianney Lapotre, Associate Professor, and Maria Mushtaq, PhD researcher at Lab-STICC, UBS, Lorient.

Candidate:

- MS Project Student

Required Skills:

- Good implementation skills on Linux
- Good Programming skills such as C, C++, Python, Assembly Language
- Good understanding of Computer Architecture and Cryptography

Implementation Platform/Experimental Setup:

- Implementation will be performed on real machines such as Intel Core i-5, i-7

Time Line:

- MS-Project will lead to 6 months time (Starting from Feb-2018)

For further information, please contact: vianney.lapotre@univ-ubs.fr