Ph.D. in Information Technology
Thesis Defense

December 13, 2022
at 15:00
Room PT1

Niccolo' IZZO – XXXIV Cycle

GLOBAL PROTECTION FOR TRANSIENT ATTACKS

Supervisor: Prof. **Luca Breveglieri**

Abstract:

Computer security threats have a strong bond with information permanence, which is encoded in the physical state of a device. Attacks based on the trace left by the flow of information into a system in the form of its physical state are called transient. A secure device must store its state in a multitude of functionalities that have to be resilient to known and future attacks. In a mobile system, the security state of the device could switch between locked and unlocked, and the secure erasure of user data must be guaranteed during said transitions. Current DRAM-based main memories will be gradually replaced by Emerging Memories such as 3D XPoint, ReRAM, STT-RAM, Memristor or ULTRARAM, which are faster, more scalable and efficient than traditional NAND flash, even though their non-volatility is yet another potentially vulnerable state. Thus, a secure non-volatile storage architecture will have to employ well-known cryptographic building blocks to guarantee strong security properties on the stored data, such as confidentiality, integrity and replay protection, even when the device is turned off. Such properties must be guaranteed despite external physical threats, tampering with the bus signals, as well as internal threats, executing malicious code in a Virtual Machine on the same virtualized environment, or on the hypervisor itself. Another threat that originates from the variation of physical states are side-channel attacks. In fact, even the most efficient encryption architecture is rendered useless if a secret, e.g., a cryptographic key, is exposed through side-channel leakage, like power consumption, EM emission, or others. Masking techniques allow to implement effective software countermeasures, however their security proofs can be invalidated by hidden micro-architectural features. To restore the effectiveness of these countermeasures, a detailed model of the stateful elements of the data path has to be derived. Such model will allow the modification of the instruction scheduling of the sensitive code to implement side-channel countermeasures, e.g., masking, in a secure way.

PhD Committee

Prof. **Paolo Cremonesi**, DEIB - Politecnico di Milano
Prof. **Sylvain Guilley**, TELECOM-ParisTech
Prof. **Jean-Pierre Seifert**, TU Berlin