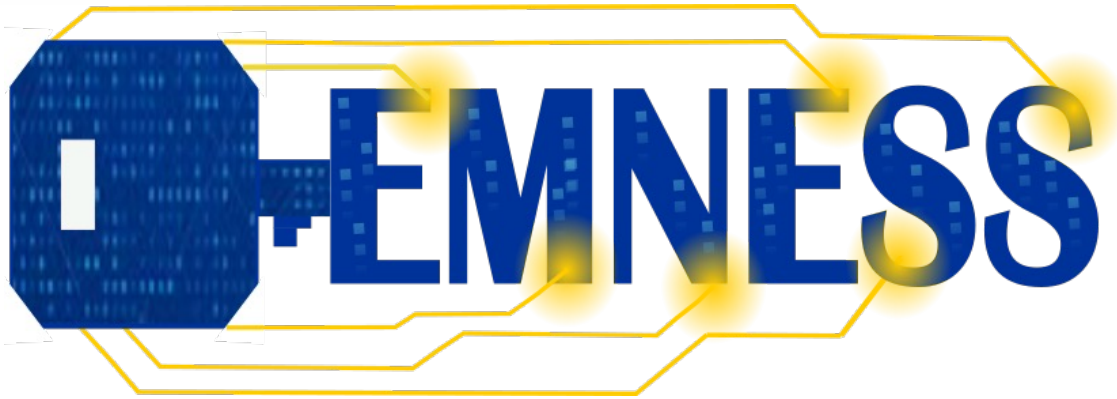
Politecnico di Torino



2020-1-FR01-KA203-080184

Deliverable D1.2.1 — Microarchitectural attacks

La Région Auvergne-Rhône-Alpes

AGENCE ERASMUS+ FRANCE · EDUCATION FORMATION

Erasmus+

Goal

- Teaching students of the Master in Computer and Electronic Engineering how embedded boards can suffer attacks that exploit weaknesses in the hardware architecture and microarchitecture

Co-funded by the
Erasmus+ Programme
of the European Union

Implementation

- A collaborative work between teachers and students of the “Operating Systems for Embedded Systems” course delivered in the Master in Computer Engineering at Politecnico di Torino.
  - Teamwork including students and teachers
  - Every team working on a specific attack
  - Final goal to study, implement and prepare lectures and laboratories on the selected attack

Co-funded by the
Erasmus+ Programme
of the European Union

Developed material

- **DMA Attacks:** a set of resources to understand what a DMA attack is, both from a theoretical point of view and in practical terms based on a LPC1768FET100 embedded board
  - https://github.com/japanninja74/ES_Security_DMA_Attacks
- **AES Cache Timing Attack on Raspberry Pi 4/Pico:** a set of resources to understand and implement the attack described in Cache-timing attacks on AES by Daniel J. Bernstein.
  - https://github.com/japanninja74/ES_Security_aes-cache-timing-attack-pi4
  - https://github.com/japanninja74/ES_Security_aes-cache-timing-attack-pico
  - https://github.com/japanninja74/ES_Security_aes_algorithm
- **Rowhammer Implementation Raspberry Pi 3:** a set of resources to understand and implement the Rowhammer attack on Raspberry Pi 3B+.
  - https://github.com/japanninja74/ES_Security_rowhammer_rpi3
- **Spectre Implementation on rpi3:** a set of resources to understand and implement the Spectre attack PoC on Raspberry Pi 3B+
  - https://github.com/japanninja74/ES_Security_Spectre_rpi3

Co-funded by the
Erasmus+ Programme
of the European Union