**PAGURUS: Low-Overhead Dynamic Information Flow Tracking on Loosely Coupled Accelerators**

Luca Piccolboni, Giuseppe Di Guglielmo, Luca Carloni
Columbia University, New York, NY, USA

---

**Systems-on-Chip (SoCs) are Heterogeneous**

- Processor Core (RISCy)
- Data RAM
- Boot. RAM
- Instr. RAM

**Hardware Accelerators**

- Viable: even if the rest of the SOC is secured with DIFT, accelerators can be used to implement software-based attacks similar to the ones DIFT should protect the SOC from. Why? Accelerators don’t propagate tags.

**Hardware Accelerators: A Way To Compromise SoCs**

- With DIFT, accelerators can be used to perform a specific functionality.

---

**Dynamic Information Flow Tracking (DIFT)**

- DIFT protects against software-based attacks.
- The shell is designed independent of the SOC’s design.
- Hardware accelerators: they are components designed to perform a specific functionality.

**Evaluation**

- The shell is designed with SystemC.
- We extended Pulpino with DIFT (C. Palermo et al., IEEE HPEC’18).

---

**A Security Metric: Information Leakage**

- The information leakage depends on four factors:
  - Factor #1: tag offset
  - Factor #2: acc. algorithm
  - Factor #3: acc. implement.
  - Factor #4: acc. workload

---

**Experimental Setup**

- Processor Core (Leon3)
- Memory Controller
- Embedded Scalable Platforms (ESP)

---

**Take-Home Message**

PAGURUS is a flexible methodology to design a shell circuit that extends the DIFT support to hardware accelerators.