PhD in Computer and Control Engineering

Research Title:
Secure Computer Hardware Architectures

Funded by	Comitato ICT

Supervisor	Paolo Prinetto – Paolo. Prinetto@polito.it

Contact	https://cybersecnatlab.it - Cybersecurity National Lab

Context of the research activity	In recent times, security has taken on the role of essential requirement for any type of computing machine, from the server clusters of large corporates to end-points represented by smart objects surrounding our daily lives. The communication encryption systems, which are considered the basis against the misuse of data and functions, are fundamental but not sufficient. Computing systems need to implement defenses that are not limited to application data protection, but scale more and more towards the lowest levels of abstraction, until they reach the hardware on which programs and services run. If the concepts of virtualization, isolation, supervision, memory protection and secure execution are included in the design paradigm of microprocessors and hardware components, the systems would benefit from an architectural protection that goes beyond all possible vulnerabilities of software or communication protocols. The PhD proposals aims at proposing, studying, and developing architectural solutions for computing hardware, able to guarantee predefined level of security to systems. The work will target examples of open core architecture suitable for research purposes (e.g., RISC-V) to reason about, elaborate and test such solutions.

Objectives	The research objectives will be: 1) Analyzing security issues by considering different vulnerabilities and possible attack surfaces related to processor architectures. 2) Several different solutions will be considered, depending on the type of vulnerability and the level of criticality of the system that uses the devices. These will include solutions aimed at: a. preventing the leakage of information between different security domains, defined and enforced in hardware; b. preventing the hijacking of the behavior of the system into malicious actions (e.g., Arbitrary Code Execution); c. detecting potentially suspect behavior and warning the execution environment about possible threats; d. confining the potential malicious execution outside the access to critical resources, without affecting the overall execution environment; e. exploiting *trust zones*, i.e., regions of the computing hardware used to run critical code or to store critical information; f. exploiting coordination between existing features of processors to implement security policies. While the results obtained during the research period are expected to be general and hold for any platform, the work during the PhD thesis will explicitly focus on the RISC-V open architecture [https://riscv.org/].

Skills and competencies for the development of the activity	• Hardware design methodologies, including VHDL/Verilog based synthesis • Processor architectures • RISC-V open architecture • Cybersecurity • Hardware security