Politecnico di Torino

COMPUTER AND CONTROL ENGINEERING

ACN - Security and Resilience of IoT and Cyber-Physical Systems through Open-Source RISC-V Architectures

Funded By	Agenzia per la cybersicurezza nazionale [C.F.: 96501130585]
Supervisor	DI CARLO STEFANO - stefano.dicarlo@polito.it
Contact	SAVINO ALESSANDRO - alessandro.savino@polito.it DI CARLO STEFANO - stefano.dicarlo@polito.it
Context of the research activity	This project develops modular RISC-V–based hardware/software solutions to strengthen cybersecurity in embedded and IoT systems. Focusing on side-channel and fault injection attacks, it integrates real-time defenses, adaptive AI-driven methods, and secure-by-design principles to ensure resilient, transparent, and trustworthy cyber-physical platforms.
	Hardware security is a key aspect of resilience in cyber-physical systems and IoT devices, since vulnerabilities at the hardware level can undermine even the most advanced software security measures. Threats such as side-channel attacks—which exploit information unintentionally leaked by hardware (e.g., power consumption, electromagnetic emissions, timing, micro-architectural events, etc.)—and fault injection attacks—which deliberately induce errors to compromise device operation—pose significant challenges for the security of embedded and IoT systems. Moreover, the increasing complexity and miniaturization of hardware components, often produced through opaque global supply chains, introduces further risks such as the presence of hardware Trojans or deliberately inserted backdoors during design or manufacturing. Addressing these challenges requires integrated approaches that combine advanced hardware monitoring techniques, secure-by-design principles, and targeted verification and validation methodologies, to ensure resilient and trustworthy cyber-physical systems over time. The growing importance of hardware security in the resilience of cyber-physical and IoT systems opens new opportunities for adopting open-hardware architectures such as RISC-V. Thanks to its open and modular nature, RISC-V enables greater transparency and control during hardware design and verification, reducing the risk of hidden vulnerabilities or backdoors. Its flexibility also allows the direct integration of customized security modules and the targeted application of advanced countermeasures against side-channel and fault injection attacks. This fosters the development of safer, more robust systems capable of resisting increasingly sophisticated

Objectives	threats. In this challenging context, the overall goal of this research project is to develop modular, efficient white-box solutions to reduce the attack surface in RISC-V–based embedded systems, with a particular focus on side-channel and fault injection attacks. The specific objectives of the PhD project are defined as follows: - Design and validation of RISC-V–based hardware/software cybersecurity solutions - Develop and validate high-performance security modules integrated into RISC-V platforms, carefully balancing performance, energy consumption, and hardware resource usage through advanced algorithmic optimization and integrated hardware/software co-design. - Integration of real-time security techniques into RISC-V architectures - Implement and evaluate real-time security countermeasures, such as low-latency cryptographic systems, continuous low-power monitoring, and rapid threat detection and response mechanisms, while maintaining compliance with the strict requirements of cyber-physical and industrial applications. - Development and experimentation of adaptive security methods with AI and advanced hardware monitoring on RISC-V platforms - Create adaptive hardware/software security solutions by leveraging machine learning techniques and RISC-V's built-in monitoring and logging capabilities to promptly detect cyberattacks. This includes designing mechanisms for proactive anomaly detection, correlating information from hardware registers, and automatically activating targeted countermeasures in response to emerging threats.

Skills and competencies for the development of the activity	A strong candidate should have skills in computer architecture (RISC-V or similar), embedded systems, hardware security (side-channel, fault injection), and hardware/software co-design. Experience with C/C++, HDL (VHDL/Verilog), FPGA prototyping, and cryptography is valuable. Knowledge of AI/ML for anomaly detection, verification/validation methods, and good research and communication skills are also important.