PhD in Computer and Control Engineering

Research Title: Development of Vulnerability-Tolerant Architectures (two positions available)

Funded by	CINI Cybersecurity National Lab
Supervisor	Paolo PRINETTO paolo.prinetto@polito.it
Contact	www.consorzio-cini.it
Context of the research activity	As with software, hardware vulnerability may result from project bugs or intentionally inserted vulnerabilities (Hardware Trojans). In addition, unlike software, hardware can be: • observed and controlled (and therefore physically attacked) from outside, through physical quantities and/or its physical interactions with the real world (Side-Channel effect); • attacked exploiting the test infrastructures inserted in the device during its design phase to improve the testability of the target system; • attacked via the injections of physical faults that can lead the system to unexpected (and in most cases more vulnerable) states and conditions; • attacked to fraudulently steal not just data but also the intellectual property associated to the techno–logical solutions used to implement it; • counterfeited by means of fraudulent placement on the market of decommissioned and therefore typically worn out devices. The PhD proposals aims at proposing, studying, and developing architectures capable of guaranteeing pre-defined security levels, even in the presence of vulnerabilities of different nature (hardware and/or software), known or even not yet revealed. The proposed solutions will be adaptable to the criticality of the target systems. *The topic is so huge that two candidates are foreseen.*
Objectives	The research objectives will be: 1) Analyzing hardware security issues by considering different

vulnerabilities. Hardware vulnerabilities, regardless of their nature, can only be corrected by modifying the design and are therefore bound to remain permanently in the devices. To continue using vulnerable devices securely, it is necessary to develop architectural solutions capable of tolerating the vulnerabilities by preventing their exploitation by malicious attackers.

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:
    a. solutions based exclusively on software and aimed at preventing malicious attackers from exploiting known vulnerabilities;
    b. solution preventing the injection of the malicious code that could be used to launch attacks of any kind;
    c. solutions "confining" the vulnerable devices in protected (trusted) zones and allowing them to run trusted code, only;
    d. solutions aimed at tolerating behavior byzantine in the case of complex systems with many interacting devices [1];
    e. solutions exploiting advanced interactions among different components, including processors, FPGAs, Smart Cards, and dedicated hardware devices;
    f. solutions exploiting FPGA-based architecture to early detect both hardware and software attacks;
    g. solutions exploiting a proper subset of the built-in facilities today available in some of the most advanced processors.

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 SEcube™ platform [2], that will be made available to the candidates thank to a collaboration with Blu5 Labs and with the CINI Cybersecurity National Lab.

The SEcube™ (Secure Environment cube) platform is an open source security- oriented hardware and software platform constructed with ease of integration and service-orientation in mind. Its hardware component is a SoC platform: a single-chip design embedding three main cores: a highly powerful processor, an EAL5+ certified smartcard, and a flexible FPGA.

[1] Leslie Lamport, Robert Shostak, Marshall Pease "The Byzantine Generals Problem" *ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, Pages 382-401.*

Skills and competencies for the development of the activity	. Hardware Security . Hardware Design . Hardware Testing and Dependability . Assembler Language Programming . Basic concepts of Cybersecurity