# Research internship proposal (early 2019) : Compatibility between security and reliability; study and practical evaluation

**Key words:** Physical and logical attacks, safety, software/hardware architecture

## 1 Context

Today's world is surrounded by connected electronic devices that might be critical at a different level; from devices manipulating personal or private data, to devices responsible for the proper functioning of production lines, or even for the safety of human beings in the case of autonomous vehicles for example. It is therefore necessary to take into account the dependability of a system, including among others, reliability (resilience against possible malfunctioning due to natural events), and security properties (resilience against possible malfunctioning due to voluntary attacks). However, despite this global definition of dependability (also called safety), today, we are still not able to realistically evaluate the degree of reliability and security of such electronic systems.

## 2 Scientific issues

State-of-the-art clearly shows that the studies simultaneously addressing both, reliability and security are (very) few. Indeed, numerous work and contributions exist but have only considered one of these two properties. This is explained by several important scientific issues. In fact, in addition to the increasing complexity of embedded devices, and to the constant evolution of logical and physical faults/attacks, we see today that, if reliability and security properties are tightly correlated, they are not necessarily compatible. Indeed, these two domains are based on contrasting principles; reliability is generally based on determinism principles, whereas security is often based on the integration of randomness in values and behavior. It is therefore necessary to study and to evaluate the compatibility of state-of-the-art solutions in order to simultaneously answer to the reliability and security requirements. Finally, this evaluation must encompass both, theoretical study and practical experimentation.

## 3 Objectives and expected contributions

The first objective of this internship will be to investigate the impact on security of current state-of-the-art solutions initially proposed to answer to reliability requirements, and vice versa. This work will be based on a theoretical study of current state-of-the-art contributions, as well as on the practical evaluation of the degree of reliability and security. For this latter, the successful candidate will use the analysis/audit (communication buses, memory dump,...) and physical attack equipment (side-channel attacks and fault injection) of the IETR lab.

According to provided results and if necessary, a second objective will be to propose and implement i) an enhancement of the considered contributions and/or ii) a new approach dealing with reliability and security.

Among the scientific challenges to be addressed, this internship project will focus on:

- The study and selection of state-of-the-art reliability/security mechanisms to consider;

- The handling of our lab analysis/audit and physical attacks equipments;
- The proposal and implementation of enhanced/new ”safety approaches”, as well as their evaluation via practical experimentation in terms of reliability and security;
- The promotion and dissemination of this work via research publications.

This internship work will leverage the knowledge and motivation of the internship candidate but also the expertise of the SYSCOM team in reliability and in security. Finally, for practical experimentations, the successful candidate will leverage the lab equipment for analysis/audit and logical and physical attacks.

## 4 Candidate profile

The candidate must be able to demonstrate theoretical (/and practical) knowledge in the area of computer and architecture design. Skills in programming (C language, python) is a prerequisite and knowledge and experience of computer and/or hardware security would be highly appreciated. English written and oral communication skills are a prerequisite as well. Finally, the utilization of hardware design languages such as VHDL and SystemC would be a good asset.

Applying candidates will prove and/or justify the requested knowledge and skills by providing:

- A CV;
- A motivation letter consistent with the proposed internship project;
- All documents attesting the requested skills and knowledge;
- Academic records and marks of the two years of Master, or of the two last years of Engineer school.

## 5 Internship context

- **Research Laboratory:** Institut d’Electronique et de Télécommunication de Rennes (IETR), UMR CNRS 6164
- **Research Team:** SYStems and COMmunications (SYSCOM)
- **University:** Polytech, Université de Nantes
- **Location:** IETR/Polytech, Nantes, FRANCE
- **Starting date:** Early 2019 (5 month duration)
- **Funding:** Research internship contract

## 6 To apply

- **Dr. Maria Méndez Real**, maria.mendez@univ-nantes.fr
- **Prof. Sébastien Pillement**, sebastien.pillement@univ-nantes.fr