Post-doc offer: Design, modeling and implementation of Secure by design Systems-on-Chips

DurDuration : 24 month
Start : 2023
Team : Laboratoire Lab-STICC (UMR 6285) - ENSTA Bretagne, Brest

1 Objectives

This position is open within the framework of the Trust Soc project funded by the french Innovation Agency for Defence (AID). This project aims at the implementation of secure-by-design systems-on-chip. It is a reversal of the conventional approach of taking a system-on-chip (SoC) and making it secure. In contrast, the TrustSoc approach aims to set out the security rules upstream of the SoC design, and then to apply them during implementation.

2 Context

The open position is located at ENSTA Bretagne, a major engineering school under the auspices of the Ministry of the Armed Forces. The scientific environment is the UMR 6285 Lab-STICC. The future employee will join a team with a strong expertise in the design of CAD tools for embedded systems.

3 Job description

Global security is based on three pillars. Firstly, local security policies, which are implemented through a distributed system of controllers acting on the bus that architects the SoC. These policies ensure that rights are granted before any read/write/activate operation. Secondly, a set of rules to which the local policies must conform. Finally, the dynamic deployment/updating of policies based on the global execution.

The new employee will be responsible for designing and modelling in executable form the link between the rules and the security properties of the SoC. A formal verification approach will explore multiple execution paths with security guarantees (no rules to violate) and meta-properties (liveness, reachability). During the development phase, this approach will allow expressive debugging (time travel, co-evaluation of multiple paths, etc.).

The work will benefit from the support of a software engineer in charge of the refactoring and enrichment of the current model of SoC. This work will also articulate with a thesis that started in

October 2021 in collaboration with the Embedded Systems Security and Hardware Architecture group of the Jean Monnet University.

Scenarios will be implemented to demonstrate the realization: SoC including representative peripherals (DMA access, processor with or without enclave, RAM, I/O), several levels in the bus hierarchy, and reference application cases (illegal burst write attempt, NR bit privilege projection attempt on remote processor, etc).

4 Candidate

The candidate must have a PhD or equivalent. The candidate will justify the good adequacy of his/her skills with the expectations of the project: Formal verification, object-oriented software programming (python, Java, smalltalk, ...), security, scientific writing, supervision of engineer/doctoral student.

5 Contacts

Application documents: CV, diploma, grades, cover letter, letter of recommendation.

— Prof. Loïc Lagadec, loic.lagadec@ensta-bretagne.fr
— Dr. Pascal Cotret, pascal.cotret@ensta-bretagne.fr
— Dr. Théotime Bollengier, theotime.bollengier@ensta-bretagne.fr
— Pr. Lilian Bossuet, lilian.bossuet@univ-saint-etienne.fr