Proposition de stage

Proving the absence of errors in critical software with Frama-C / Eva

Mots clés : Software verification, Static analysis, Formal methods, Abstract Interpretation

Institution

The French Alternative Energies and Atomic Energy Commission (CEA) is a key player in research, development, and innovation. Drawing on the widely acknowledged expertise gained by its 16,000 staff spanned over 9 research centers with a budget of 4.1 billion Euros, CEA actively participates in more than 400 European collaborative projects with a large number of academic (notably as a member of Paris-Saclay University) and industrial partners. Within the CEA Technological Research Division, the CEA List institute addresses the challenges coming from smart digital systems.

Among other activities, CEA List's Software Safety and Security Laboratory (LSL) research teams design and implement automated analysis in order to make software systems more trustworthy, to exhaustively detect their vulnerabilities, to guarantee conformity to their specifications, and to accelerate their certification. In particular, the Frama-C platform is dedicated to perform a wide range of analyses over C programs (with an experimental C++ front-end).

Objectives

Inside Frama-C, Eva is a plugin dedicated to the automatic inference of properties about C programs such as finding all the possible values of variables or inferring arithmetic relations between variables. The primary goal of this analysis is to prove the absence of runtime execution errors (e.g. arithmetic overflows, invalid memory accesses, other C undefined behaviors, . . .). It is also used for code auditing and as a support for other analyses.

We are constantly improving the range and the precision of this analysis and we are looking for students to work on the following directions.

1. The definition of a new specification language, easily interpretable by the interpreter, and the developpement of the tools to manipulate and validate specifications using this language. Language features would include side effects and non-determinism. The objective is to be able to specify libraries, especially the standard C library, and to be able to write various useful stubs for analyses.
2. The development of new heuristics to guide the strategy choices made by Eva to improve the analyzes performances and precision.
3. Addressing the problem of the combination of analysis domains when they require a very different number of iterations to converge.

The results will be integrated into Frama-C. All positions include theoritical research as well as prototyping and experimental evaluation. Purely applied internships may also be available.

Qualifications

- **Minimal**
- master student in Computer Science
- knowledge of functional programming
- ability to work in a team
- **Preferred**
- some knowledge of Ocaml
- some knowledge in C
- a certain taste for mathematical matters would be preferable

Characteristics

- **Duration:** 5-6 months from early 2022
- **Location:** CEA Nano-INNOV, Paris-Saclay Campus, France
- **Compensation:**
  - €700 to €1300 monthly stipend (determined by CEA compensation grids)
  - maximum €229 housing and travel expense monthly allowance (in case a relocation is needed)
  - CEA buses in Paris region and 75% refund of transit pass
  - subsidized lunches

Application

If you are interested in this internship, please send to the contact persons an application containing:

- your resume;
- a cover letter indicating how your curriculum and experience match the qualifications expected and how you would plan to contribute to the project;
- your bachelor and master 1 transcripts;
- the contact details of two persons (at least one academic) who can be contacted to provide references.

Applications are welcomed until the position is filled. Please note that the administrative processing may take up to 3 months.

Contact persons

For further information or details about the internship before applying, please contact:

- Valentin Perrelle (valentin.perrelle@cea.fr)
- David Bühler (david.buhler@cea.fr)
- Maxime Jacquemin (maxime.jacquemin@cea.fr)