Master's Thesis Subject

Typestates analysis in Frama-C

Keywords: program verification, static analysis

Context

CEA LIST is a French technological research institute with a focus on smart and complex systems. Its research programs are conducted in coordination with major industrial actors from nuclear, automotive, aeronautics, defense and medical sectors, in order to design and develop innovating solutions tailored to their needs. Within CEA LIST, the Software Security Laboratory, based in Palaiseau (in the Paris area), develops tools for the verification and validation of software and mixed hardware/software systems. Frama-C (`http://frama-c.com`) is a software platform written in *OCaml*, dedicated to the analysis of C programs. The thesis will take place in the R&D team developing Frama-C.

Objectives

Typestates have been introduced by [SY86] as an extension to type-checking. Briefly, an object of a given type can be in distinct typestates during its lifetime, that restrict the set of operations that can be applied to it. For instance, a `FILE` handler will be successively in the states `uninitialized` (right after allocation), `initialized` (after proper initialization), `open` (after having applied `open`), and `initialized` (after having applied `close`) again. User can read from it only in the `open` state, and no `FILE` is supposed to be freed if it is still in the `open` state, to avoid leak of file descriptors. The notion of typestates can be encoded in ACSL, Frama-C's specification language, but this encoding is not very convenient and not very well suited for existing Frama-C's analyzers. The main goals of the thesis are thus to propose an extension to ACSL allowing to easily specify typestates, and to develop static analyses dedicated to the verification of the correctness of a program with respect to such typestates.

Applying

Skills

- Good knowledge of *OCaml*
- Interest for static analysis of real-world programs
- Ability to work within a team
- Some knowledge of C programming

Conditions : paid internship; housing stipend possible (under conditions); access to CEA's shuttle service for commuting.

Contact : Virgile Prevosto (virgile.prevosto@cea.fr)

The instruction of the administrative paperwork can take up to 2 or 3 months, you are thus encouraged to apply as soon as possible.

References

[SY86] Robert E Strom and Shaula Yemini. Typestate: A programming language concept for enhancing software relability. *IEEE Transactions on Software Engineering*, 12(1), 1986.