Postdoc Positions

Software verification, security

Keywords: formal methods, software verification, software security, symbolic execution, static analysis, constraint solving

The CEA LIST, Software Security Lab (LSL) is looking for candidates for several postdoc positions in the area of software verification, to begin as soon as possible at Paris-Saclay, France.

Host Institution

Within CEA LIST, LSL is a twenty-person team dedicated to software verification, with a strong focus on real-world applicability and industrial transfer. We design methods and tools that leverage innovative approaches to ensure that real-world systems can comply with the highest safety and security standards. CEA LIST’s new offices are located at the heart of Campus Paris Saclay, in the largest European cluster of public and private research.

Quick position descriptions

All positions include theoretical research as well as prototyping (preferably in OCaml).

Constraint solving and decision procedures (with François Bobot): The aim of the SOPRANO project [1] is to prepare the next generation of verification-oriented solvers, by combining principles from both Satisfiability Modulo Theory and Constraint Programming. Within this ambitious agenda, the successful candidate will investigate one of the following topics:

- model synthesis for quantified 1st-order logic formulas, with applications to counter-example generation and test generation;
- efficient satisfiability solving for still-challenging theories, such as bit-vector theory and floating-point arithmetic theory [1]

Source-level software verification and testing (with Nikolai Kosmatov): Frama-C [2] is an open-source industrial-strength code analysis platform developed at LSL. The recent plugin LTest [3] builds on an innovative combination of static and dynamic analysis in order to bring powerful automated testing abilities to the platform. The successful candidate will contribute to improve the LTest plugin through working in one of the following directions:

- automatic detection of infeasible test objectives, through combination of static analyses [2]
- design of a (formal) language for specifying test objectives, and test automation through symbolic execution [3]

Binary-level security analysis: The BINSEC project [4] aims at developing formal methods for binary-level security analysis, lifting previous work developed for safety analysis of critical systems [4,5]. In this context, we are looking for a candidate willing to investigate the following challenges, and integrate them into an open-source platform [6]:

- smart fuzzing and exploitability analysis
- sound decompilation via static analysis

Context

Positions are up to 3-year long, to begin as soon as possible. The successful candidates will work in the CEA LIST’s new offices, located at the heart of Campus Paris Saclay, in the largest European cluster of public and private research [6].
Requirements

Candidates should have a Ph.D. in Computer Science, or be near completion. They should be familiar with some of the following topics: formal verification - preferably software verification (static analysis, model checking, deductive verification, symbolic execution, etc.), logic and the use of solvers in a verification setting, semantics of programming languages, compilation techniques, specification languages, security analysis and knowledge of assembly languages (3rd subject), functional programming (OCaml).

Application

Applicants should send an email to Sébastien Bardin sebastien.bardin@cea.fr - including a CV, a motivation letter and 2-3 recommendation letters, and (depending on the subject) to Nikolai Kosmatov or to François Bobot firstname.lastname@cea.fr.

Reference