PhD Positions: *Software verification, binary-level security*

Keywords: formal methods, software verification, software security, vulnerabilities, (de-)obfuscation, malware, static and dynamic analysis, symbolic execution

The CEA LIST, Software Security Lab (LSL), has several open PhD positions in the area of binary-level software verification and security, to begin *as soon as possible* at Paris-Saclay, France.

Quick position descriptions

Several major classes of security analysis have to be performed on raw executable files, such as vulnerability analysis of mobile code or commercial off-the-shelf, deobfuscation or malware inspection. These analysis are very challenging, due to the very low-level and intricate nature of binary code, and currently they are still relatively poorly tooled – essentially syntactic static analysis (disassembly) which are easy to fool, or dynamic analysis (fuzzing) which miss many subtle behaviors. Our long-term objective is to adapt software verification methods from source-level safety analysis to binary-level security analysis, in order to propose efficient semantic tools for supporting low-level security investigations.

We propose several PhD positions around this thematic, focusing on: vulnerability detection and symbolic fuzzing, semantic analysis of very large binary codes and malware deobfuscation and detection. The goal is to build on state-of-the-art approaches in terms of software verification, binary-code analysis, combination of formal methods (especially static analysis and symbolic execution) in order to design methods and tools addressing these extremely challenging problems.

This work will build on advances brought by the BINSEC project (2013-2017) `http://binsec.gforge.inria.fr/`, a 4-year project funded by ANR (French research agency) and dedicated to advance binary-level security analysis. Results will be included in the open-source BINSEC platform. All positions includes theoretical research as well as prototyping (preferably in OCaml) and experimental evaluation.

Context

The positions are 3-year long. The successful candidates will be hosted at CEA (Paris area, France), where they will be supervised by Sébastien Bardin. Possible collaborations: LORIA (Nancy), Université Grenoble-Alpes and DGA.

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 `https://www.universite-paris-saclay.fr/en`.

Requirements

Candidates should have a Master degree in Computer Science. They should be familiar with at least one of the following topics: formal verification, logic (especially automated solvers), semantics of programming languages, compilation techniques, security analysis, architecture and/or assembly languages. A good knowledge of functional programming (OCaml) is a plus.

Application

Applicants should send an email to Sébastien Bardin `sebastien.bardin@cea.fr` - including CV, motivation letter and reference. **deadline:** please contact us as soon as possible. **more information:** email, or `http://sebastien.bardin.free.fr/index_bg.html`