PhD Position: *Software verification, security*

**Keywords:** formal methods, software verification, software security, exploitability, static and dynamic analysis

The CEA LIST, Software Security Lab (LSL), and the laboratory Verimag (University Grenoble-Alpes) have an open PhD position in the area of software verification and security, to begin as soon as possible at Paris-Saclay and Grenoble, France.

**Quick position descriptions**

One of the key points in cyber-security is to ensure that a given piece of software is free of exploitable bugs (vulnerabilities). Verification and automated testing methods are currently adapted to security concerns. However, while these methods are effective at finding bugs, these bugs are not always relevant in a security context since they may not be exploitable.

The proposed PhD work focuses on the exploitability analysis of a bug, given a faulty execution trace leading to this bug. The goal is to design methods able to automatically classify the "degree" of exploitability of a given bug, by using formal verification techniques for "generalising" the initial (non-exploitable) trace into an exploit. The candidate will build on state-of-the-art approaches in terms of binary code analysis and vulnerability detection. The main challenges here are to improve the following aspects: the generalisation method, the exploitability model and the environment modeling. The position includes theoretical research as well as prototyping (preferably in OCaml).

This work is part of the BINSEC project (2013-2017) [http://binsec.gforge.inria.fr/](http://binsec.gforge.inria.fr/) funded by ANR (French research agency), a 4-year project gathering top-level academic and industrial partners in order to advance the state-of-the-art of binary-level security analysis.

**Context**

The position is 3-year long. The successful candidate will be hosted at CEA (Paris area, France), with regular visits to University of Grenoble-Alpes (Grenoble, France). He will be supervised by Sébastien Bardin (CEA, co-supervisor) and Marie-Laure Potet (Uni. Grenoble-Alpes, supervisor).

**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.

Verimag is a leading research center in the domain of verification and validation of Embedded Systems [http://www-verimag.imag.fr/](http://www-verimag.imag.fr/) Research at Verimag provides theoretical and technical means for developing safe and secure systems, contributing to scientific advancement and industrial progress. Verimag owns a significant expertise in the domain of security analysis (cryptographic protocol verification, vulnerabilities analysis, security modeling and verification for high-level certification concerns) and is involved in several industrial projects.

**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](mailto:sebastien.bardin@cea.fr) including a CV, a motivation letter and a recommendation letter, and to Marie-Laure Potet [Marie-Laure.Potet@imag.fr](mailto:Marie-Laure.Potet@imag.fr).