Postdoc Positions
Software security through binary-level analysis

Keywords: software security, vulnerabilities, reverse engineering, deobfuscation, malware, software verification, static and dynamic program analysis, machine learning

The CEA LIST, Software Security Lab (LSL), has several open postdoc positions in the area of binary-level software security analysis, to begin *as soon as possible* at Paris-Saclay, France. Positions are two year long. The successful candidates will be part of the binary-level analysis team, led by Sébastien Bardin, and they will contribute to extend the BINSEC open-source platform – `http://binsec.gforge.inria.fr/`. We are mainly looking for enthusiastic candidates with a strong background in *Software Verification, Security or Artificial Intelligence.* The positions are not tied to a particular project, and there is freedom to choose a research topic.

Short position descriptions

Several major classes of security analyses have to be performed on raw executable files, such as vulnerability analysis of mobile code and commercial off-the-shelf software, deobfuscation or malware inspection. These analyses are very challenging, due to the very low-level and intricate nature of binary code. Currently they are still relatively poorly tooled, basically with syntactic static analyses (disassembly) which are easy to fool, or dynamic analyses (fuzzing) which miss many subtle behaviors.

Our objective is to leverage recent advances in **software verification***,* **security analysis** *and* **machine learning** *in order to develop advanced tools supporting low-level security investigations.* The main domains of application include:

- efficient and precise vulnerability detection,
- static analysis of very large binary codes,
- malware deobfuscation and detection,
- certified disassembly and computer-assisted reverse,
- software quality evaluation.

Results will be integrated in the open-source BINSEC platform. All positions include theoretical research as well as significant prototyping (preferably in OCaml or Python) and experimental evaluation on real-world case-studies.

Requirements

Candidates should have a Ph.D. in Computer Science, or be near completion. We are looking for candidates enthusiastic about software development, security & hacking, together with a strong background in *Software Verification, Security or Artificial Intelligence*, especially:

- formal methods (abstract interpretation, symbolic execution, software model checking, etc.)
- static and dynamic security analysis (reverse, fuzzing, tainting, etc.)
- machine learning applied to program analysis, security or software engineering,
- privacy, quantitative reasoning and automated solvers.

Applications with background in semantics of programming languages, compilation, empirical software engineering or assembly languages may also be considered. A good knowledge of functional programming (OCaml) is a plus.

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`.

Application

Applicants should send an email to Sébastien Bardin `sebastien.bardin@cea.fr` and Richard Bonichon `richard.bonichon@cea.fr` with CV, motivation letter and references.
Deadline: Contact us as soon as possible. A first round of selection will take place by mid-May 2017.
More information: email or `http://sebastien.bardin.free.fr/`