Research-oriented internships, 4-6 months, CEA Paris-Saclay, France
Software security through binary-level analysis

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

The CEA LIST, Software Security Lab (LSL) – located at Paris-Saclay (France), has several intern positions in the area of binary-level software security analysis. Positions are 4-6 month long and can open the way to a doctoral work. The successful candidates will be part of the binary-level analysis team, 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 clear background in Computer Science. Knowledge in *Software Verification or Security* is a plus.

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 general objective is to leverage recent advances in **software verification** *and* **security analysis** *in order to develop advanced tools supporting low-level security investigations*, with a special focus on vulnerability detection, reverse and malware analysis. We are especially looking for students willing to work on the following directions:

- [research] binary-level verification of a real-time OS,
- [research] reverse engineering of protected code (symbolic deobfuscation),
- [research] white-box cryptography,
- [research] binary-level static and symbolic analysis (tainting, sanitization),
- [research] code hardening and protection evaluation.

This list is not exhaustive, ask us if you have some project in mind.

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

Requirements

Candidates should have a clear background in Computer Science. We are looking for people enthusiastic about software development, security & hacking. Knowledge in *Software Verification, Security, Compilation* is a plus. A working knowledge of functional programming (OCaml) will be really appreciated.

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 and motivation letter. **More information:** email or `http://sebastien.bardin.free.fr/`

References

[1] Gogul Balakrishnan and Thomas W. Reps. WYSINWYX: What You See Is Not What You Execute. *ACM Trans. Program. Lang. Syst.*, 32(6), 2010.

[2] Benjamin Schwarz, Saumya K. Debray, and Gregory R. Andrews. Disassembly of executable code revisited. In *9th Working Conference on Reverse Engineering (WCRE 2002), 28 October - 1 November 2002, Richmond, VA, USA*, pages 45–54, 2002.

[3] Patrice Godefroid, Michael Y. Levin, and David A. Molnar. SAGE: whitebox fuzzing for security testing. *Commun. ACM*, 55(3):40–44, 2012.

[4] Sébastien Bardin, Robin David, and Jean-Yves Marion. Backward-bounded DSE: targeting infeasibility questions on obfuscated codes. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pages 633–651. IEEE Computer Society, 2017.

[5] Robin David, Sébastien Bardin. Code Deobfuscation : Intertwining Dynamic, Static and Symbolic Approaches (talk). In Black Hat Europe 2016

[6] Robin David, SébastienBardin, Tan Dihn Ta, Josselin Feist, Laurent Mounier, Marie-Laure Potet, Jean-Yves Marion. BINSEC/SE : A Dynamic Symbolic Execution Toolkit for Binary-level Analysis. In Proceedings of the 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016). Springer