2-year Postdoc Position

Control Flow Integrity for Remote Attestation

Keywords: Control Flow Integrity, Remote Attestation, Runtime Verification, Static Analysis, Source Code Generation

Programming Languages: *OCaml*, *C*

Tool: *Frama-C*

Context: CEA LIST, Software Safety and Security Lab

CEA LIST's offices are located at the heart of Université Paris-Saclay, the largest European cluster of public and private research. Within CEA LIST, the Software Safety and Security Lab has an ambitious goal: help designers, developers and validation experts ship high-confidence systems and software.

Systems in our surroundings are getting more and more complex, and we have built a reputation for efficiently using formal reasoning to demonstrate their trustworthiness through the design of methods and tools to ensure that real-world systems can comply with the highest safety and security standards. In doing so, we get to interact with the most creative people in academia and the industry, worldwide.

Our organizational structure is simple: those who pioneer new concepts are the ones who get to implement them. We are a fifty-person team, and your work will have a direct and visible impact on the state of formal verification.

Work Description

Remote attestation allows some authorized parties to detect unexpected changes (typically, performed by a malicious user) in a software component. It is critical for trusted computing by providing strong guarantees about the software component's integrity. Control flow integrity (CFI) is a security technique that checks that a program follows its expected control flow when being executed, so that the system is not being executed a piece of code in an unexpected way, which could bypass some security checks, or would attempt some malicious actions. Therefore, CFI can contribute to remote attestation by enforcing integrity of the program's control flow during its execution.

The goal of the postdoc consists in designing a runtime verification technique [2] that enforces CFI for remote attestation during a program execution. The works will be done in collaboration with researchers from the CEA LIST's Communicating System Lab that will be in charge of providing the necessary secure communications and system components. Therefore, the postdoc work will focus on the code analysis, code instrumentation and monitoring techniques that are necessary for generating an efficient CFI monitor from a given source code. They will be implemented as a new plug-in for *Frama-C* [1] (`http://frama-c.com`), the industrial-strength code analysis platform for C programs that is developed in our lab. *Frama-C* itself is developed in *OCaml*. More precisely, the following contributions are expected:

- designing a CFI-based technique for remote attestation;
- implementing this technique as a new *Frama-C* plug-in
- evaluating the implemented technique on concrete examples
- design one or several new intermediate representations that would make these developments easier
- (optionally:) designing and implementing optimization strategies to reduce the time overhead

References

[1] P. Baudin, F. Bobot, D. Bühler, L. Correnson, F. Kirchner, N. Kosmatov, A. Maroneze, V. Perrelle, V. Prevosto, J. Signoles, and N. Williams. The Dogged Pursuit of Bug-Free C Programs: The Frama-C Software Analysis Platform. *Communications of the ACM*, 2021.

[2] Yliès Falcone, Klaus Havelund, and Giles Reger. A tutorial on runtime verification. In *Engineering Dependable Software Systems*. IOS Press, 2013.

Application

Knowledge in at least one of the following fields is required:

- *OCaml* programming (at least, functional programming)
- *C* programming
- software security
- runtime verification
- static analysis
- program transformation

Salary: academic competitive (vary *w.r.t.* diploma and former experience)

Availability: as soon as possible; yet a 3+-month procedure for administrative and security purposes is required

Contact: Julien Signoles (julien.signoles@cea.fr)

Please join a detailed CV, a motivation letter and possibly reference letters.