2018-00964 - Validation and Synthesis of DWARF Debugging Information

Contract type: Public service fixed-term contract
Renewable contract: Oui
Level of qualifications required: Graduate degree or equivalent
Fonction: Temporary scientific engineer

Context
Parkas project-team
Département d'Informatique
École normale superieure
45 rue d’Ulm
75005 Paris, France

Assignment
DWARF is a standardised debugging data format; it is part of the ELF and Mach-O binary formats, and as such it is widely used. DWARF is obviously relied upon by debuggers, but it plays an unexpected role in the runtime of high-level programming languages and in the implementation of program analysis tools. For instance the C++ runtime relies on DWARF’s .debug_frame table to unwind the stack and implement C++ exceptions, while program analysis tools require the .debug_types table to reconstruct the initial state of a program from its binary.

Generating the DWARF tables tends to be a burden for compiler authors, as each optimisation pass potentially invalidates several of them; keeping tables and code synchronised pass after pass requires a tedious and error prone logic to be added to the already twisty optimiser passes. In practice there are bugs in the generated tables: these hard to detect because DWARF information never get any rigorous testing. Even worse, DWARF tables include scripts expressed in a Turing complete bytecode: a malicious attacker, by injecting crafted DWARF tables in a binary, can create powerful and unsuspecting trojans.

An ongoing project I lead aims to develop theories and tools to cross-check binaries against their DWARF tables, and develop techniques to synthesise correct-by-construction DWARF tables. The resulting tools have the potential to be routinely used to validate software and compilers and make an impact in the real world.

Main activities
Contribute to the above project on tasks discussed with the project leader.

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport

Remuneration
- Location: 45 Rue d’Ulm, 75005 Paris
- Gross Salary per month: according to experience

General Information
- Theme/Domain: Architecture, Languages and Compilation System & Networks (BAP E)
- Town/city: Paris
- Inria Center: CRI de Paris
- Starting date: 2018-09-01
- Duration of contract: 29 days
- Deadline to apply: 2018-08-12

Contacts
- Inria Team: PARKAS
- Recruiter: Zappa Nardelli Francesco / francesco.zappa_nardelli@inria.fr

About Inria
Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world’s top universities, Inria’s 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

Conditions for application
- Defence Security: This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorization to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy:
As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning: you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.