A propos du centre ou de la direction fonctionnelle

Inria, le National French Institute for computer science and applied mathematics, promotes "scientific excellence for technology transfer and society". Graduates from the top engineering schools in France (Institut Mines-Télécom) and over 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.

Contexte et atouts du poste

The candidate will be hired in the ANTIQUE group.

ANTIQUE focuses on developing automated techniques to compute semantic properties of programs and other systems with a computational semantics in general. Such properties include (but are not limited to) important classes of correctness properties.

Verifying safety critical systems (such as avionics systems) is an important motivation to compute such properties. Indeed, a fault in an avionics system, such as a runtime error in the fly-by-wire command software, may cause an accident, with loss of life. As these systems are also very complex and are developed by large teams and maintained over long periods, their verification has become a crucial challenge. Safety critical systems are not limited to avionics: software runtime errors in cruise control management systems were recently blamed for causing unintended acceleration in certain Toyota models (the case was settled with a 1.2 billion dollars fine in March 2014, after years of investigation and several trials). Similarly, other transportation systems (railway), energy production systems (nuclear power plants, power grid management), and medical systems (pacemakers, surgery and patient monitoring systems) rely on complex software, which should be verified.

Beyond the field of embedded systems, other pieces of software may cause very significant harm in case of bugs, as demonstrated by the Heartbleed security hole: due to a wrong protocol implementation, many websites could leak private information, over years.

An important example of semantic properties is the class of safety properties. A safety property typically specifies that some (undesirable) event will never occur, whatever the execution of the program that is considered. For instance, the absence of runtime error is a very important safety property. Other important classes of semantic properties include liveliness properties (i.e., properties that specify that some desirable event will eventually occur) such as termination and security properties, such as the absence of information flows from private to public channels.

All these software semantic properties are not decidable, as can be shown by reduction to the halting problem. Therefore, there is no chance to develop any fully automatic technique able to decide, for any system, whether or not it satisfies some given semantic property.

The antique group focuses on the design of semantic analysis techniques that should be sound (i.e., compute semantic properties that are satisfied by all executions) and automatic (i.e., with no human interaction), although generally incomplete (i.e., not able to compute the best —in the sense of: most precise— semantic property). As a consequence of incompleteness, we may fail to verify a system that is actually correct. For instance, in the case of verification of absence of runtime error, the analysis may fail to validate a program, which is safe, and emit false alarms (that is reports that possibly dangerous operations were not proved safe), which need to be discharged manually. Even in this case, the analysis provides information about the alarm context, which may help disprove it manually or refine the analysis.

In the last five years, the group has engaged the design of the MemCAD framework for memory data structures abstraction, which allows to describe and infer complex structural invariants. Furthermore, it has initiated a study of the application of this technique to the verification of operating systems components.

Mission confiée

This position is made available as part of the SPARK (ERC Proof of Concept) project, that aims at developing a platform for the verification of specifications. This project supports an ongoing transfer activity following results obtained during the PhD thesis of Tie Cheng and the creation of the startup MatrixLead.

As of today, we have designed and implemented AiXi, a static analyzer for spreadsheet applications based on abstract interpretation. While spreadsheets tools such as Excel are probably a very weak programming model, where users may write wrong formulas and macros without ever noticing, the origin or even the existence of a problem. As a well known example, the economy publication "Growth in a time of debt" stated wrong conclusion based on a wrong statistical analysis in Excel, where important data points were ignored.

Informations générales

- Thème/Domaine : Preuves et vérification
- Ville : Paris
- Centre Inria : Cri de Paris
- Date de prise de fonction souhaitée : 2019-02-01
- Durée de contrat : 12 mois
- Date limite pour postuler : 2019-01-18

Contacts

- Équipe Inria : ANTIQUE
- Recruteur : Rival Xavier / xavier.rival@inria.fr

A propos d’Inria

Inria, l’institut national de recherche dédié aux sciences du numérique, promeut l’excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l’interface d’autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 startups. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

L'essentiel pour réussir

The candidate should hold either a Master Degree or a PhD Thesis degree in Computer Science, should be knowledgeable in formal methods, static analysis and program verification, and should be motivated to design and implement static analysis tools.

However, knowledge of abstract interpretation are not mandatory, and we expect the candidate to gain expertise in this field while working with us.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

Attention : Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d’autres canaux n’est pas garanti.
AiXi can successfully verify certain classes of correctness properties on Excel spreadsheets (such as typing issues), and will report any violation of this class of properties. Benchmarks have led to the identifications of dozens of bugs in public domain spreadsheet applications. As of today, the results produced by this tool are unique.

The SPARK project aims at advancing the state of the tool so as to help with its transfer to MatrixLead. The following tasks will be carried out:

- Design of a general toolbox for spreadsheet verification: while the existing tool is tied to a fixed set of logical predicates, we aim for a more general tool with a library of logical predicates descriptions so as to support for a wide variety of static analyses (possibly specific to some groups of users);
- Design of plugins implementing specific static analyses;
- Improvement of the analysis results in terms of precision (i.e., to make sure that it verifies more programs) and of performance (runtime and memory consumption);
- Verification of industrial use cases;
- Improvement of the tool output (better presentation of analysis results to users).

Development will be done in OCaml.

Design work will be done in collaboration with Xavier Rival (INRIA) and Tie Cheng (MatrixLead), who will bring expertise in abstract interpretation and verification of spreadsheet applications.

**Principales activités**

Main activities:

- Design improvements to an existing static analysis tool;
- Research on existing and novel analysis techniques (abstract domains, static analysis components);
- Generation of test cases, assessment of analysis results, and improvement based on these results;
- Implementation of static analysis techniques and experimental validation;
- Publication of the results.

**Compétences**

The candidate should have a good understanding of programming languages techniques (compilation, program analysis) and of formal methods.

A large part of the work will be carried out in English (scientific communication, writing or articles).

**Avantages sociaux**

- Subsidised catering service
- Partially-reimbursed public transport

**Rémunération**

- Location: Paris 12ème
- Gross Salary per month: 2 653€ brut/mensuel

**Security and defense procedure:**

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).

Authorisation 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.