Offer #2025-08654

PhD Position F/M [Campagne Allocation Région 2025] Automatic Generation of Attack Chains for Detecting and Preventing Software Vulnerability (F/M)

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

About the research centre or Inria department

Created in 2008, the Inria center at the University of Lille employs 360 people, including 305 scientists in 15 research teams. Recognized for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria center at the University of Lille maintains a close relationship with large companies and SMEs. By fostering synergies between researchers and industry, Inria contributes to the transfer of skills and expertise in the field of digital technologies, and provides access to the best of European and international research for the benefit of innovation and businesses, particularly in the region.

For over 10 years, the Inria center at the University of Lille has been at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

Context

Within the framework of a partnership (you can choose between)

- not applicable

The goal is to develop methods, techniques and tools to prevent deserialization attacks in applications.

Is regular travel foreseen for this post ? No

Assignment

Assignments :
The recruited person will be taken to: (1) develop a modular approach to vulnerability analysis, (2) build a tool dedicated to the automatic generation of attack chains via fuzzing and mutation and (3) study the history and semantics of code changes for the understanding of attacks. Prototypes will be developed in the Pharo language.

For a better knowledge of the proposed research subject :
A state of the art, bibliography and scientific references are available at the following URL, do not hesitate to log in:

https://www.inria.fr/fr/evref.

Collaboration :

The recruited person will be in connection with the members of the EVREF team who have skills in software analysis and software quality to meet the challenges defined in this thesis.

Responsibilities :

The person recruited is responsible for:

- Conducting original research related to the problem of vulnerability detection within the framework of this thesis.
- Performing scientific monitoring to stay up to date with advancements in the field of software analysis for vulnerability detection.
- Carrying out simulations and analyses of existing software attacks to define their behavior.
- Writing scientific papers and present work at national and international conferences.
- Collaborating with other researchers in the EVREF team and take part in team and GL working group meetings in the laboratory.
- Participating in team meetings and activities (including EVREF Sprints and presentations).
- Writing and defending thesis in front of a jury at the end of this research work.

Steering/Management :

The person recruited will be in charge of:

- Managing his/her research project by planning the various stages of the thesis topic and meeting deadlines.
- Coordinating collaborations with other researchers in the software security field and with the EVREF team's industrial partner Berger-Levrault.
- Leading weekly follow-up meetings with supervisors.
- Contributing to the writing of deliverables and scientific papers.

Main activities

Main activities :

- study of the state of the art in software attacks, static/dynamic analysis techniques and fuzzing
- analysis of existing attacks and extraction of their behavior
- definition of attack model
- design and evaluation of a tool-based approach for detecting and preventing attack (using the Pharo language (www.pharo.org))
- writing deliverables and reports

Additional activities :

- validation of the proposed approach by analyzing existing attacks and referring to attack catalogs and databases (Mitre, NVD, etc.)
- qualitative/quantitative experimentation of the developed prototype
- dissemination of results to security communities at national (e.g. GDR days) and international level in top venues (conferences, journals, etc.)

Skills

Technical skills and level required : Object programming, static code analysis

Languages : French, English

Relational skills :

- Ability to work as part of a team: collaboration and interaction with EVREF team members and researchers in Software Engineering working groups.
- Oral and written communication skills: present work in meetings, conferences and articles.
- Adaptability and active listening skills: incorporating feedback from supervisors and colleagues to develop research.

- Ability to communicate results to a variety of audiences.
- Exchanges with researchers from industrial partner Berger-Levrault.

Other valued appreciated : ability to organize thematic days on software security for the team and the host laboratory.

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration

2200 € monthly gross salary from October to December 2025

2300 € monthly gross salary after January 1st 2026

General Information

- **Theme/Domain :** Distributed programming and Software engineering
  Software engineering (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2025-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-04-20

Contacts

- **Inria Team :** EVREF
- **PhD Supervisor :**
  Polito Guillermo / Guillermo.Polito@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

There you can provide a "broad outline" of the collaborator you are looking for what you consider to be necessary and sufficient, and which may combine :

- Strong experience in code analysis and programming.
- Good knowledge of software security research methodologies.
- Expertise in Object-oriented programming languages. Knowledge of Pharo is an asset for this position.
- Research experience (via a research internship or Master's project, or a scientific publication) is a plus.
- Good level of English.

This section enables the more formal list of skills to be completed and 'lightened' (reduced) :

- Analytical and rigorous thinking.
- Autonomy and ability to take initiative.
- Good written and oral communication skills in English and French.
- Aptitude for teamwork and collaboration with other researchers in the thesis domain and the Pharo programming language industry consortium (https://consortium.pharo.org).
- Scientific curiosity and motivation for research.

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.

Instruction to apply

Please send your CV and cover letter.

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).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.

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