PhD (M/F) in computer science: vulnerabilities in code generated by LLMs (TAP project)

Contract type: Fixed-term contract
Start date: As soon as possible
Duration: 36 months
Required degree level: Master's degree or equivalent

PhD topic description

For the last 60 to 70 years, programming has largely prevailed in the field of computer science, encompassing the capture of intentions and the production of code. Formal specifications have gained in importance thanks to advances in systems modelling and design, enabling more precise capture of objectives. Despite these advances, software engineers are reluctant to write formal specifications, resulting in the absence of a formal statement of intent for large software systems, making debugging and error correction difficult. Despite the lack of intent capture, testing and analysis have been used to build reliable code bases. In testing, this work aims to achieve greater behavioural coverage and uses test oracles. Fuzzing approaches have gained in importance over the last decade. However, achieving functional correctness of software without extensive formal requirements remains a difficult goal.

Recent advances in automatic code generation from large language models (LLMs) offer a new perspective. It is possible to program from natural language specifications using LLM-based code generation, suggesting that self-coding is feasible. This raises the question of the correctness and security of code automatically generated by LLMs and the conditions under which it can be trusted.

The TAP (Trustworthy Automatic Programming) project focuses specifically on these aspects. The objectives of this project are to identify vulnerabilities in LLM-generated code, to analyse and classify them, and to determine whether certain types of vulnerability are more frequent in LLM-generated code than in code written by humans. The objectives of the project also include the automatic correction of vulnerabilities in LLM-generated code and the strengthening of LLM against vulnerabilities in generated code.

The main objective of the DiverSE team on this project is to carry out research to identify vulnerabilities in code generated by LLMs. To achieve this objective, we will set up a system capable of automatically generating datasets of vulnerabilities. This will be achieved by using the web catalogues available for vulnerabilities and by modelling these vulnerabilities in such a

way as to integrate them seamlessly into a test tool, enabling us to analyse the code and libraries generated by LLM. The target languages will primarily be C and Java, due to their widespread use and in order to maximise the impact of our work.

In this context, the DiverSE team (in close collaboration with the IPAL laboratory and the DGA) is **recruiting a student as a PhD candidate for a period of 36 months**, under the scientific and technical supervision of permanent members of the team involved in the project. This person will be responsible for research and design work related to the DiverSE objectives indicated above, with the aim of analysing the state of the art, and designing techniques and methods that will then be implemented in prototypes and demonstrators. Synergies with other work carried out in the team will also be explored and exploited.The results of our work will be used by NUS partners in Singapore.

The exponential growth in the use of LLMs for all kinds of tasks, including the assisted production of source code, ensures that the results of the project will have a considerable impact. Indeed, the security of code produced by LLMs is currently in its infancy, and providing a system that performs this task automatically would meet a huge global need. The resulting cybersecurity challenges are therefore considerable in practice.

This position may involve travel in France and abroad, including by air.

Work Environment

IRISA (Research Institute of Computer Science and Random Systems) is one of France's largest research laboratories in computer science and information technology, with over 850 members. Organized into seven scientific departments, IRISA focuses on key areas such as bioinformatics, system security, software architectures, virtual reality, big data analysis, and artificial intelligence.

IRISA is part of a dynamic regional ecosystem, recognized for its expertise through international scientific collaborations. Focused on the future of computer science, IRISA plays a key role in digital transformation, cybersecurity, health, environment, transportation, robotics, energy, and AI.

The **DiverSE research team** specializes in software engineering techniques for building reliable and efficient applications, focusing on areas such as cybersecurity and LLMs. The team consists of about 15 permanent members (Inria and CNRS researchers, university lecturers, including 3 members of the French University Institute), 15 PhD students, several engineers, and a DGA associate engineer. DiverSE is internationally recognized and maintains strong ties with global, national, and local industries. The team also prides itself on a friendly and engaging work atmosphere.

The position is located in a sector covered by the protection of scientific and technical potential (PPST), and therefore requires, in accordance with the regulations, that your arrival be authorised by the competent authority of the MESR.

Why Join Us?

Project Highlights:
In addition to the PhD degree itself, this project offers unique opportunities due to its application domain, ambition, international network, and potential impact. It lies at the core of DiverSE's activities and involves collaboration with a dynamic team in Singapore.

Ambition:
While pursuing your PhD degree in Computer Science, you will contribute to a worldwide open-source project. In an era where source code security is a strategic concern, TAP aims to address this challenge directly. This project could also lay the groundwork for stronger collaboration between DiverSE and NUS, enhancing national, European, and global sovereignty and security in software engineering, AI, LLMs, and cybersecurity.

Network:
TAP involves frequent interactions with partners from NUS and IPAL. Visits to Singapore may be arranged based on your preferences. The project offers opportunities to engage with various research, innovation, and industry transfer projects within and beyond the DiverSE team. After the project, you'll be one of the (many) alumni of the DiverSE team, most of whom are still in touch.

Benefits

- Remote work up to 2 days per week.
- Partial reimbursement of public transport or sustainable mobility costs.
- Partial coverage of health insurance costs.
- Subsidized on-site dining.
- Free car and bicycle parking; bus stop 5 minutes away; metro station 10 minutes away.

Salary

Monthly salary will be equal to or above **€2,200gross** (€1,769 net)

Location

Campus de Beaulieu, IRISA/Inria Rennes
Building 12

263 Avenue du Général Leclerc
35042 RENNES Cedex, France

Contacts and PhD advisors

- **Olivier BARAIS**, Professor, University of Rennes: Olivier.Barais@irisa.fr
- **Olivier ZENDRA**, Researcher, Inria: Olivier.Zendra@inria.fr