# Driving decarbonization and digitalization. Together.

## Doctoral Thesis: “Large Language Models (LLMs) for Security" (f/m/div)

## Job description

The industrial doctorate at Infineon: Pursue a doctoral degree at a university and gain professional experience simultaneously - an ideal start for your career. Advance your research with us and profit from our vast network of doctoral candidates and the expertise of a university. Mentorship is handled by both professors and dedicated Infineon employees. We are presenting a doctoral thesis focused on the utilization of AI technologies to enhance software security in embedded devices. This work encompasses three interconnected research areas. The initial field of research involves leveraging Large Language Models (LLMs) to enhance fuzzing on embedded devices, which includes guiding a fuzzer through the binary code of an embedded device and automated root cause analysis for low-level crashes during the fuzzing process. Subsequently, we explore using LLMs to identify insecure code within an existing code base on the basis of metadata and code statistics, followed by the development of automated exploitation techniques for logical attacks. A crucial aspect of this endeavor is the close collaboration with the software security group to ensure that each aspect is thoroughly investigated. Furthermore, some of the selected research topics will be implemented as proof of concepts to validate the formulated thesis and assess its practical usage in real-world environments. The thesis will be written in cooperation with TUM Munich and under the supervision of Professor Alexander Pretschner.

The tasks within the thesis will consist of:

- Usage of LLMs to improve fuzzing on embedded devices
    - Guide a fuzzer through the code
    - Automatic root cause analysis of low level crashes
    - Generate harnesses for fuzzing
    - Assess the quality of a fuzzing campaign
- Usage of LLMs to detect insecure code (e.g. by analysis of metadata of commits and repositories)
- Usage of LLMs to implement logical attacks (AEG – automated exploit generation)

The learnings out of the thesis will be/lead to:

- Deep understanding of the use of LLMs in the context of fuzzing tools and improvement use of such tools in the embedded software environment. Realize on selected topics proof of concepts to use the knowledge in real life environment for practical use.

## At a glance

| | |
|---|---|
| Location: | **Munich (Germany)** |
| Job ID: | **HRC0760522** |
| Start date: | **Aug 01, 2024** |
| Entry level: | **0-1 year** |
| Type: | **Full time** |
| Contract: | **Temporary** |

Apply to this position online by following the URL and entering the Job ID in our job search. Alternatively, you can also scan the QR code with your smartphone:

Job ID: HRC0760522
www.infineon.com/jobs

## Contact

Antonie Stredak

- Detection of unsafe code by analyzing the code and the associated metadata. Exemplary application and verification of the findings in an internal or open source environment.
- Theoretical considerations on the automatic generation of exploits using LLMs and statistical analyzes. Practical implementation and verification of the developed solution

## Profile

A doctoral student is a research enthusiast,
› whose interests are scientific research combined with the passion for Infineon's innovative products and applications.
› who enjoys working in an industrial environment in combination with an Infineon partner university.
› who appreciates open communication and the contribution of an international environment.
› and is thus an excellent candidate for a further academic or industrial career after completion of their thesis.

As the ideal candidate you:

- Are **eligible for full-time PhD studies** and have a master's degree in Information Science or Electrical Engineering
- Good to very good grades
- Committed, quick comprehension
- Good IT and software knowledge in the embedded area
- Knowledge and experience of the creation, training and usage of LLMs
- Knowledge and experience with typical embedded programming languages
- Knowledge and experience of embedded microcontroller hardware and software
- Very analytical and systematic behavior
- Good English and German skills

Know-how in following topics is preferable - but not mandatory

- Background in software testing, fuzzing, software KPIs, build chains for CI/CD, static code analyzer, software engineering
- Knowledge in C, Assembler, Java, Python
- Experience in building small devices with microcontrollers

## Benefits

- **Munich:** Coaching, mentoring networking possibilities; Wide range of training offers & planning of career development; International assignments; Different career paths: Project Management, Technical Ladder, Management & Individual Contributor; Flexible working conditions; Home office options; Part-time work possible (also during parental leave); Sabbatical; On-site creche and kindergarden with 220 spots, open until 5:30pm; Holiday child care; On-site social counselling and works doctor; Health promotion programs; On-site gym, jogging paths, beachvolleyball, tennis & soccer court; On-site canteen; Private insurance offers; Wage payment in case of sick leave; Corporate pension benefits; Flexible transition into retirement ; Performance bonus; Reduced price for public transport and very own S-Bahn station; Access for wheelchairs; Possibility to work remotely from abroad (EU)

## Why Us

**Driving decarbonization and digitalization. Together.**

Infineon designs, develops, manufactures, and markets a broad range of semiconductors and semiconductor-based solutions, focusing on key markets in the automotive, industrial, and consumer sectors. Its products range from standard components to special components for digital, analog, and mixed-signal applications to customer-specific solutions together with the appropriate software.

**– Connected Secure Systems (CSS) is at the heart of the IoT –**

The CSS division provides end-to-end systems for a connected, secured world – building on trusted, game-changing microcontrollers as well as wireless and security solutions. CSS delivers microcontrollers plus Wi-Fi, Bluetooth® and combined connectivity solutions (known as connectivity combos) along with hardware-based security technologies to power the broadest application spectrum spanning consumer electronics, IoT devices, cloud security, IT equipment, home appliances, connected cars, credit and debit cards, electronic passports, ID cards, and more. The division is at the forefront of computing, wireless connectivity, and trusted technologies that are helping to securely connect the networked systems of today and tomorrow.

Click here for more information about working at CSS with interesting employee and management insights and an overview with more #CSSDreamJobs.

**We are on a journey to create the best Infineon for everyone.**
This means we embrace diversity and inclusion and welcome everyone for who they are. At Infineon, we offer a working environment characterized by trust, openness, respect and tolerance and are committed to give all applicants and employees equal opportunities. We base our recruiting decisions on the applicant´s experience and skills.
We look forward to receiving your resume, even if you do not entirely meet all the requirements of the job posting.
Please let your recruiter know if they need to pay special attention to something in order to enable your participation in the interview process.
Click here for more information about Diversity & Inclusion at Infineon.