For our location in **Hamburg**, we are looking for a

Master Student in Automated Software Security Testing (m/f/d)

NXP Semiconductors N.V. (NASDAQ: NXPI) enables a smarter, safer and more sustainable world through innovation. As the world leader in secure connectivity solutions for embedded applications, NXP is pushing boundaries in the automotive, industrial & IoT, mobile, and communication infrastructure markets. Built on more than 60 years of combined experience and expertise, the company has approximately 31,000 employees in more than 30 countries and posted revenue of $13.10 billion in 2023.

Subject of the Master Thesis: Hardware accelerated pre-silicon security testing

The ORSHIN project (Open-source ReSilient Hardware and software for Internet of thiNgs), funded by the European Union's Horizon Europe program, aims to address the critical need for secure open-source hardware and software systems. Within this initiative, pre-silicon security testing plays a pivotal role, enabling us to identify and address security vulnerabilities early in the design phase before a device is manufactured. By leveraging hardware-accelerated testing and advanced techniques like fault injection on FPGA emulators, we can simulate and detect potential security flaws in embedded devices, ensuring they are robust against physical and software-based attacks. Additionally, advanced software testing methodologies—such as fuzzing, symbolic execution, and concolic execution—will be applied to embedded firmware to uncover vulnerabilities across the IoT lifecycle.

We are seeking a motivated master's student to undertake a thesis project within the ORSHIN project, focusing on hardware-accelerated pre-silicon security testing. The candidate will work closely with a multidisciplinary team to develop tools and frameworks for effective testing of embedded systems. Key tasks will include:

- Study State-of-the-Art for software testing, and in particular firmware testing.
- Design and evaluate the applicability of hardware-based support for software testing.
- Apply and develop tools that automate fault injection testing using FPGA emulators, enabling efficient simulation of various attack scenarios on hardware prototypes.
- Apply and refine techniques such as fuzzing, concolic execution, and symbolic execution to thoroughly test embedded firmware for potential vulnerabilities.
- Expand state-of-the-art research on embedded security testing with a goal to produce a scientific publication

Skills and Qualifications:

- Master student in Computer Science, Electrical Engineering, Embedded Systems, or a related field.
- Strong understanding of embedded systems, cybersecurity principles and typical software vulnerabilities.
- Familiarity with software security testing techniques, including fuzzing, concolic execution, and symbolic execution.
- Proficiency in languages commonly used in embedded development, such as C, C++, or Python.
- Experience with hardware description languages (e.g., VHDL, Verilog) for FPGA programming (optional).
- Familiarity with open-source software development processes and tools (optional).
- Interest in cybersecurity research and innovation.
- Fluent in spoken and written English.

Please note that this is a full-time contract limited to 6 month.