

Position for a Ph.D. Candidate or Postdoc in Information-Flow Security



We are looking for a researcher who is interested in addressing foundational problems that will be of practical relevance or in addressing practical problems based on solid foundations. The research focus shall be on enabling reliable security guarantees for programs that operate on sensitive data. Your research will contribute to improving the reliability and applicability of program analyses.

Information-flow security aims at providing end-to-end security guarantees for software-based systems that operate on sensitive data. There are many possibilities for how information can leak during the execution of a program. The complexity of real-world programs poses another difficulty in achieving information-flow security. Hence, reliable information-flow security guarantees can only be obtained based on solid formal foundations. In addition, to reduce the conceptual complexity of verifying information-flow security, compositional verification techniques are needed that are both reliable and precise. The overall goal of our research project is to develop a framework for the modular information-flow analysis of object-oriented programs that provides reliable end-to-end security guarantees without being too conservative.

Your research will address open issues in information-flow security, ranging from the adequate characterization of security requirements by information-flow properties, to the development of reliable security analyses and their implementation in tools, to the security analysis of real-world programs. Your research shall result in foundational insights and/or security analysis tools usable in practice. Concrete results could include, e.g., compositionality results that exploit the rely-guarantee principle to gain precision, sound combinations of analysis techniques and tools to achieve better efficiency and coverage, mechanization of soundness proofs in proof assistants, and applications of information-flow analysis to certify the security of mobile code and of programs that make extensive use of libraries. Your research shall be based on solid theoretical foundations to obtain reliable information-flow security for real-world object-oriented programs.

We are offering a productive and collaborative research environment in which you can discuss ideas with other team members working on related topics. Our international connections and our involvement in leading-edge research projects (CRISP, CROSSING, and Software-Factory 4.0) provide further opportunities for collaborations.

TU Darmstadt is one of Germany's top technical universities with an outstanding reputation in research and education in Computer Science.

The chair MAIS is led by Prof. Dr. Heiko Mantel. The overall research objective of MAIS is to increase the trustworthiness and reliability of software-based systems.

<http://www.mais.informatik.tu-darmstadt.de>

The position is available immediately and applications will be considered until the position is taken. The position is with regular salary and social benefits based on TV-TUD. TU Darmstadt is an equal-opportunities employer and encourages applications from women. In case of equal qualifications, applicants with a degree of disability of at least 50% will be given preference.

Prerequisites

You should be highly motivated to tackle challenging research projects and be open minded. You should have a solid background in formal methods, logic, or other mathematical foundations of Computer Science. Prior knowledge in any of the following areas is a plus (but not required): concurrency, Dalvik bytecode or Java source code, information-flow security, and proof assistants like Isabelle/HOL. You need very good language skills in English, both in talking and writing. Prior knowledge of German is not expected, but you should be willing to obtain basic skills within a year. For a Postdoc position, you need to hold a Ph.D. (or to have completed all requirements upon start of appointment), should aim for scientific leadership, and have organizational skills. For a Ph.D. position, you need to hold a Master's degree in Computer Science or Mathematics (or to have completed all requirements upon start of appointment).

How to apply?

Please submit your application, including your detailed CV with language skills, complete transcripts with lists of courses and grades, all theses that you have completed so far, a description of your background and research interests, and, if possible, references whom we may contact for letters of recommendation to recruiting@mais.informatik.tu-darmstadt.de.