Ph.D. Candidate and Postdoc Positions in Side-Channel Analysis

We are looking for researchers who are interested in addressing foundational problems that will be of practical relevance or in addressing practical problems based on solid foundations. We are offering two positions that aim at trustworthy software implementations of cryptographic algorithms. The research focus shall be on the security of cryptographic implementations against side-channel attacks. More concretely, the research foci of the positions shall be on:

1. experimental techniques against side-channel attacks
2. program analysis against side-channel attacks

In a side-channel attack, an attacker observes characteristics of a program run, (e.g., the running time) and exploits the observation to deduce secrets (e.g., cryptographic keys). Such attacks target concrete implementations and might succeed even against programs whose underlying algorithm was proven to be secure. The overall goal of the research project is to increase the trustworthiness of cryptographic implementations by a framework for the systematic analysis of code for side-channel vulnerabilities.

TECHNISCHE UNIVERSITÄT DARMSTADT

MAIS Modeling and Analysis of Information Systems

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 .

As a researcher on the first position, you will address the problem of side-channel attacks to cryptographic implementations using experiments and statistical methods. Your research shall be based on information theory and could result, e.g., in foundational insights, in experimental analysis techniques, in attack generation techniques, and in corresponding tool support. As a researcher on the second position, you will contribute to the security of cryptographic implementations against side-channel attacks using program analysis. Your research shall be based on solid theoretical foundations and could result, e.g., in foundational insights, in program analysis techniques, in program transformation techniques, and in corresponding tool support. Our research project is associated with the DFG collaborative research center CROSSING.

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.

The positions are available immediately and applications will be considered until the positions are taken. These are positions 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 preferred.

Prerequisites

You should be highly motivated to tackle challenging research projects and be open minded. For both positions, a background in information theory is a plus. For the first position, a background in statistics, software development, or side-channel attacks will be helpful. For the second position, a background in formal methods, logic, or program analysis will be helpful. 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), you 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.