Open Positions for Ph.D. candidates and Postdocs in Information-Flow Security and Side-Channel Analysis at TU Darmstadt, Germany

The chair MAIS at TU Darmstadt, led by Prof. Dr. Heiko Mantel, is offering multiple positions. 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. The research focus shall be on software security (information-flow security or side-channel analysis) using formal methods or systematic experiments.

We are offering three positions for Ph.D. candidates and Postdocs in the following areas:

1. information-flow analysis techniques for object-oriented programs at the level of source code and bytecode based on compositional and precise verification techniques
2. experimental analysis of side-channel vulnerabilities in cryptographic implementations and generation of attacks exploiting such vulnerabilities
3. program analysis techniques for detecting side-channel vulnerabilities in cryptographic implementations and for assessing the seriousness of such vulnerabilities

The overall goal of our research at MAIS is to make software-based systems more trustworthy (i.e. secure, safe, and correct) than they are today. As software engineering is a complex and error-prone task, we employ formal methods in combination with experiments for reasoning about software and critical system properties. We investigate software systems on the level of source code, bytecode, and machine code as well as on the level of more abstract system specifications. This allows us to provide support for security at different stages of software development. At MAIS we are offering a productive and collaborative research environment in which you can discuss ideas with other team members working on related topics.

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. For more information and how to apply, see http://www.mais.informatik.tu-darmstadt.de/Positions.html.