Master thesis
Vulnerabilities specifications for Android apps analysis

Android apps are an easy entry point for attackers. To ensure secure code, developers can check their apps against known vulnerabilities using different static analysis tools or by writing their own custom analyses. However, not many developers are familiar with the static analysis methods in order to write their own analyses. In addition, it is not an easy task to configure the existing tools in order to find some custom vulnerability. The goal of this master thesis is to propose a domain specific language that can help the developers to specify different vulnerabilities transparently from the static analysis expertise. The DSL should have a default support for the top 25 software errors selected by the SANS institute [1].

Your tasks
- Assess the applicability of taint analysis in detecting the SANS top 25 vulnerabilities
- Propose an automatic detection of relevant API Android methods and their classification to the selected vulnerabilities (relevant tool is SuSi [4])
- Elicit requirements for a DSL for customized vulnerabilities specifications
- Develop a prototype of the DSL

Prerequisites:
- Programming experience (preferably in Java)
- Prior knowledge in static analysis methods (e.g. data flow analysis)
- Experience with Soot framework [2] (optional)
- Experience with machine learning techniques (optional)

Contact
Goran Piskachev
Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM, Software engineering department
Zukunftsmelie 1, 33102 Paderborn
Telefon: +49 5251 5465-168, Room ZM1.02-47
goran.piskachev@iem.fraunhofer.de

References: