## Masterarbeit „Weiterentwicklung und Evaluation eines Werkzeugs zur Sicherheitsanalyse von Java-Software“

Software Security ist ein immer relevanter werdendes Teilgebiet der Informationssicherheit. Die Relevanz ist durch die zunehmende Digitalisierung, insbesondere durch die vermehrte Einführung von mobilen und IoT-Anwendungen, begründet. Sicherheitslücken in der Software können zu entsprechenden Risiken der Anwendungen führen, was letztendlich das Vertrauen untergräbt.

Ein Weg, Sicherheitslücken in Software zu identifizieren, sind **statische Programmanalysen** (mit Compilerbau-ähnlichen Techniken). Diese durchsuchen den Quelltext automatisiert nach Sicherheitslücken auf Programmzeilenebene. Nachteil dieses Ansatzes ist jedoch die hohe Anzahl an Fehlalarmen (gemeldete Sicherheitslücken, die in Wirklichkeit keine sind). Komplementär wird in dieser Masterarbeit ein anderer Ansatz auf Basis statischer Programmanalysen verfolgt: Es werden mit Hilfe der Slicing-Technik für die Security relevante Programmstellen automatisiert extrahiert und dem Entwickler/Sicherheitsauditor in benutzerfreundlicher Form, z.B. in einer IDE, dargestellt. Der Auditor kann dann selbst die entsprechenden Programmstellen bzgl. der Security einschätzen, so dass dieser wieder mehr in den Analyseprozess eingebunden ist.

Es existieren bereits Demonstratoren für ein solches **Sicherheitsaudit-Werkzeug** für die Android-Plattform und Java-Anwendungen (vorrangig Java-Krypto-Funktionalität). Diese Demonstratoren sollen in der Masterarbeit miteinander integriert und anschließend weiterentwickelt werden; insbesondere sind Zeigeranalysen umzusetzen, welche die Analyseergebnisse verbessern. Die Arbeiten werden auf dem Java-Programmanalyse-Framework **WALA** von IBM basieren. Die Ergebnisse sollen mit Sicherheitsexperten, im Idealfall z.B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), diskutiert und als Open Source publiziert werden.

**Voraussetzungen:**

1. Informationssicherheit (z.B. iSec oder andere Vorlesungen aus diesem Bereich)
2. Kenntnisse in der Softwaretechnik sind wünschenswert, aber nicht notwendig
3. Eigenmotivation, an einem forschungsnahen Thema zu arbeiten

**Literatur:**


1. WALA-Website, http://wala.sourceforge.net/wiki/index.php/Main_Page
2. Jürgen Graf. Information Flow Control with System Dependence Graphs - Improving Modularity, Scalability and Precision for Object Oriented Languages. Dissertation Karlsruhe Institute of Technology, 2016, https://publikationen.bibliothek.kit.edu/1000068211/4090558
3. Jens Krinke. Slicing, Chopping, and Path Conditions with Barriers. In: Software Quality Journal 12 (2004), Nr. 4, S. 339–360
4. Tanveer Mustafa, Karsten Sohr: Understanding the Implemented Access Control Policy of Android System Services with Slicing and Extended Static Checking, International Journal of Information Security (IJIS), Springer-Verlag, Berlin, 2014.
5. Ggf. geeignete Abschlussarbeiten an der Universität Bremen


**Kontakt:**


Dr. Karsten Sohr, TZI der Universität Bremen, Leitthema „Empowering Digital Media“

E-Mail: sohr@tzi.de

Tel.: 218 63922