Nichtinterferenz in relationalen Datenbanksystemen

(Am Lehrstuhl Prof. Dr. Beckert)

Die Geheimhaltung von Informationen in modernen IT Systemen gewinnt auf Grund von immer wachsender Mengen an Daten stets an Wichtigkeit. Um diese Eigenschaft in Web-basierten Anwendungen garantieren zu können haben sich Methoden etabliert, die den Fluss von Informationen durch Programme analysieren. Typischerweise wird hierbei Untersucht, inwiefern geheimzuhaltende Eingaben in ein Programm öffentliche Ausgaben beeinflussen. Beeinflussen geheime Eingaben die öffentlichen Ausgaben gar nicht, so ist das Programm nichtinterferent.

In den letzten Jahren wurden große Fortschritte in der Spezifikation und Analyse von verteilten Systemen bezüglich solcher Nichtinterferenzeigenschaften gemacht. Allerdings wurden dabei zentrale Technologien von Webanwendungen, insbesondere relationale Datenbanken, bisher nicht betrachtet. Das Verhalten von relationalen Datenbanken ist typischerweise definiert durch SQL-Anfragen, die wiederum durch relationale Algebra formal beschrieben werden können. Dadurch bieten relationale Datenbanken alle Voraussetzungen, die notwendig sind, um Nichtinterferenz auch in diesen Systemen zu analysieren und formal nachzuweisen.

Ziel dieser Projektgruppe ist es bestehende Nichtinterferenzbegriffe für verteilte Programme auf relationale Datenbanksysteme anzuwenden. Hierfür soll der Nichtinterfernzbegriff geeignet formalisiert werden und eine geeignete Methode zur Spezifikation von Geheimnissen und öffentlichen Informationen in Datenbanken entworfen werden. Abschließend soll aufbauend auf Beweissysteme (z. B. SMT Beweiser) eine Methode entwickelt werden, die für ein bestehendes relationales Datenbanksystem und den dazugehörigen Schnittstellendefinitionen untersuchen kann, ob der Datenbankentwurf die spezifizierten Sicherheitseigenschaften erfüllt.

Voraussetzungen: Interesse an Formalen Systemen, Logik, relationaler Algebra und theoretischen Arbeiten

Kontakt und Betreuer:

Simon Greiner (Simon.Greiner@kit.edu)