Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Praxis der Forschung

Semantische Datenminimierung

```
int foo(int a, int b) {
  int x = a - a;
  if (x == 0) return 2*a;
  else return 2*b;
}
```

Hintergrund. Mit der zunehmenden Digitalisierung der Gesellschaft wird der Schutz privater Daten immer wichtiger. In der Datenschutzgrundverordnung der Europäischen Union wird deshalb der Grundsatz der *Datenminimierung* festgelegt: „Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein."

Im Rahmen einer Bachelorarbeit entstand an unserem Lehrstuhl ein Werkzeug, das ein Programm in einen projizierenden Teil, der die eingehenden persönlichen Daten auf das Notwendigste reduziert, und einen berechnenden Teil, der aus den minimierten Informationen die ursprüngliche Ausgabe berechnet, aufteilt. So erhält man ein Programm, das dieselbe Aufgabe erfüllt, aber weniger Daten erhebt. Da dieses Werkzeug bisher aber nur auf syntaktischer statt auf semantischer Ebene arbeitet, kann es manchmal ausgetrickst werden. Im Beispiel oben könnten z. B. die persönlichen Daten a, b in der Eingabe auf a reduziert werden, da der Fall, in dem das Ergebnis von b abhängt, nie auftritt. Trotzdem reduziert das Werkzeug die Eingabe hier nicht.

Aufgabe. Ihre Aufgabe ist es, basierend auf dieser Arbeit ein Werkzeug zu entwickeln, das die oben erläuterte Aufteilung anhand der Semantik des Programms statt anhand seiner Syntax vornimmt. Hierbei können verschiedene Werkzeuge der (quantitativen) Informationsflussanalyse wie z. B. Slicing und Bitabhängigkeitsgraphen eingesetzt werden. Außerdem kann man auf Methoden der relationalen Verifikation – also Methoden, die das Verhalten mehrerer Programme vergleichen – aufbauen.

Ansprechpartner.

- Florian Lanzinger, lanzinger@kit.edu, Büro 50.34R203
- Dr. Alexander Weigl, weigl@kit.edu, Büro 50.34R225