Karlsruher Institut für Technologie

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

Combining Graph-Based and Deductive Information-Flow Analysis for Proving Non-Interference

Projektgruppe "Praxis der Forschung"
Wintersemester 2015/16

1 Abstract

Modern systems are getting more and more complex. This is especially crucial for security-critical systems, as with increasing complexity, also errors/bugs are more likely to occur. Information flow control (IFC) is a category of techniques for enforcing information flow properties and thus for ensuring that systems are secure. An approach that uses a combination of automatic and interactive techniques for IFC has been developed. This approach still needs a lot of user interactions and program modifications.

In this work, we present the combined approach that works without any program modifications. It minimizes the user interaction by running a graph-based information flow analysis first. Due to over-approximation, this step can generate false positives. We use a theorem-prover to check that there does not exist any path from a secret input to a public output and thus non-interference holds.

Finally, the new approach is evaluated based on a number of examples, showing that it can automatically prove non-interference for complex programs, i.e., is more precise than the dependency graph-based approaches and handles larger programs better than theorem-provers.

2 Contact

Mihai Herda herda@kit.edu, Raum 227 (Geb. 50.34)
Michael Kirsten kirsten@kit.edu, Raum 228 (Geb. 50.34)