Practical, Flexible Programming with Information Flow Control

Niklas Broberg

Defense will be held in room HB4,
Hörsalsvägen 8, Chalmers University of Technology,
on **Tuesday August 30, 2011** at **10:00**.

Opponent: **Stephan Zdancewic**, University of Pennsylvania

The thesis is available at the Department of Computer Science and Engineering, Chalmers University of Technology and Göteborg University.

Department of Computer Science and Engineering
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg, Sweden
Telephone + 46 (0)31-772 1000

Abstract

Mainstream mechanisms for protection of information security are not adequate. Most vulnerabilities today do not arise from deficiencies in network security or encryption mechanisms, but from software that fails to provide adequate protection for the information it handles. Programs are not prevented from revealing too much of their information to actors who can legitimately interact with them, and restricting access to the data is not a viable solution. What is needed is mechanisms that can control not only what information a program has access to, but also how the program handles that information once access is given.

This thesis describes Paralocks, a language for building expressive but statically verifiable fine-grained information flow policies, and Paragon, an extension of Java supporting the enforcement of Paralocks policy specifications. Our contributions can be categorised along three axes:

- The design of a policy specification language, Paralocks, that is expressive enough to model a large number of different mechanisms for information flow control.
- The development of a formal semantic information flow model for Paralocks that can be used to prove properties about programs and enforcement mechanisms.
- The development of Paragon, an extension of Java with support for enforcement of Paralocks information flow policies.

Together these components provide a complete framework for programming with information flow control. It is the first framework to bring together all aspects of information flow control including dynamically changing policies such as declassification, making it both theoretically sound as well as usable for solving practical programming problems.