Semantic Models for the Security of Sequential and Concurrent Programs

Andrei Sabelfeld
Department of Computing Science
Chalmers University of Technology and Göteborg University

Abstract

The present thesis investigates *confidentiality*, i.e., the problem of determining whether a given program (possibly acquired from an untrusted source) has *secure information flow*. In a setting of *extensional* security, whether or not a difference in a program's behaviour is detectable by a low-level observer as the sensitive data is varied, determines whether or not the program is insecure. Such a view induces an *equivalence relation* on program behaviours in the low-level observer's (or attacker's) view.

We present a formalisation of the attacker's view: this is done via the mathematical machinery of partial equivalence relations in the case of sequential programs (covering nondeterminism and probabilistic covert channels) and bisimulations in the case of concurrent programs (arguing for scheduler-independent security and covering synchronisation, timing and probabilistic covert channels). In both cases, we arrive at compositional security specifications; this facilitates straightforward soundness proofs for compositional security analyses, such as type-based analyses. By such a formalisation of secure information flow, we contribute to a rigorous understanding of potential threats and a higher confidence in security certification based on formal definitions.

We further concentrate on integrating the formalisation of the security of computation at the level of specific programming languages (sequential and concurrent as considered in this thesis) into the security of complex systems at a more abstract level. With this objective in mind, we propose a sound and complete translation of a timing-sensitive security specification for simple multi-threaded programs into a more general security framework.

Keywords: semantics-based security, information flow control, noninterference, confidentiality, probabilistic covert channels, partial equivalence relations, powerdomains, probabilistic bisimulation, multi-threadedness.