Certificate Translation*

Gilles Barthe

IMDEA Software, Madrid, Spain
gilles.barthe@imdea.org

Abstract

Program verification techniques based on programming logics and verification condition generators provide a powerful means to reason about programs. Whereas these techniques have very often been employed in the context of high-level languages in order to benefit from their structural nature, it is often required, especially in the context of mobile code, to prove the correctness of compiled programs. Thus it is highly desirable to have a means of bringing the benefits of source code verification to code consumers.

Certificate translation is a general method to transfer to code consumers evidence gained through verification of source code; it relies on the notion of certificate, used in Proof-Carrying Code to convey to the code consumer independently verifiable evidence that programs respect policies. The talk provides sufficient conditions of existence for algorithms that transform certificates of source programs into certificates of compiled programs, and show that many common transformations comply with these conditions.

* Joint work with Benjamin Grégoire, César Kunz, and Tamara Rezk