# Precise Enforcement of Progress-Sensitive Security

Scott Moore, Aslan Askarov, and Stephen Chong

Harvard School of Engineering and Applied Science
{sdmoore,aslan,chong}@seas.harvard.edu

### Abstract

Program progress (or termination) is a covert channel that may leak sensitive information. To control information leakage on this channel, semantic definitions of security should be *progress sensitive* and enforcement mechanisms should restrict the channel's capacity. However, most state-of-the-art language-based information-flow mechanisms are progress insensitive—allowing arbitrary information leakage through this channel—and current progress-sensitive enforcement techniques are overly restrictive.

We propose a type system and instrumented semantics that together enforce progress-sensitive security more precisely than existing approaches. Our system is permissive in that it is able to accept programs in which the termination behavior depends only on low-security (e.g., public or untrusted) information. Our system is parameterized on a termination oracle, and controls the progress channel precisely, modulo the ability of the oracle to determine the termination behavior of a program based on low-security information. We have instantiated the oracle for a simple imperative language with a logical abstract interpretation that uses an SMT solver to synthesize linear rank functions.

In addition, we extend the system to permit controlled leakage through the progress channel, with the leakage bound by an explicit budget.