Securing Interactive Programs

Willard Rafnsson Daniel Hedin Andrei Sabelfeld

Department of Computer Science and Engineering
Chalmers University of Technology
Gothenburg, Sweden

May 31, 2012

Abstract

This talk studies the foundations of information-flow security for interactive programs. Previous research assumes that the environment is total, that is, it must always be ready to feed new inputs into programs. However, programs secure under this assumption can leak the presence of input. Such leaks can be magnified to whole-secret leaks in the concurrent setting. We propose a framework that generalizes previous research along two dimensions: first, the framework breaks away from the totality of the environment and, second, the framework features fine-grained security types for communication channels, where we distinguish between the security level of message presence and message content. We show that the generalized framework features appealing compositionality properties: parallel composition of secure programs results in a secure thread pool. We also show that modeling environments as strategies leads to strong compositionality: various types of composition (with and without scoping) follow from our general compositionality result. Further, we propose a type system that supports enforcement of security via fine-grained security types.