Secure Compilation
Lecture 2

Renate Robin Eilers Cristina Matache Baber Rehman

June 24, 2019

This is the second talk presented by Amal Ahmed in OPLSS 2019, University of Oregon, USA.

1 Introduction

1.1 Source Language

1.1.1 Types

We just have integers and functions in source language.

$\sigma ::= \text{int} \mid \sigma_1 \to \sigma_2$

1.1.2 Terms

1.2 Target Language

Theorem 1.1 (Type Preservation)**.** *If* $\Gamma \vdash e_S : \sigma$ *and* $\Gamma \vdash e_S : \alpha \rightsquigarrow e_T$ *then* $\Gamma_S^+ \vdash e_T : \sigma^+$

For correctness, we want to show $e_S \approx e_T$. This is not contexual equivalance because source language and target language are two different languages. There are many ways to prove compiler correction. We want to say that when:

$$e_S \approx e_T \text{ then } \sigma \approx \sigma^+$$

$\mathrm{V}[\![\sigma]\!] = \{ (V_S , V_T)\ j\ .\ \vdash V_S : \sigma \wedge .\ ;\ .\ \vdash V_T : \sigma^+ \ldots\ldots \}$
$\mathrm{V}[\![\text{ints}]\!] = \{ (n_S , n_T) \}$
$\mathrm{V}[\![\sigma_1 \to \sigma_2]\!] = \{ (\lambda \mathrm{x}{:}\sigma_1\ .\ e_S \}$