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

2 Preservation Proof

Theorem 2.1 (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:

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

V$[\![\ \sigma \ ]\!] = \{ \ (V_S \ , V_T) \ j \cdot \vdash V_S : \sigma \wedge \cdot \ ; \cdot \vdash V_T : \sigma^+ \ ..... \ \}$
V$[\![$ ints $]\!] = \{ \ (n_S \ , n_T) \ \}$
V$[\![\ \sigma_1 \to \sigma_2 \ ]\!] = \{ \ (\lambda \text{x:}\sigma_1 \cdot e_S$ `pack` $(\tau_{env} \ , \langle \ \lambda \ (\text{Z} : \tau \ , x_T : \sigma_1^+) \cdot e_T \ , V_{env} \ \rangle \ )$
$j \ \forall \ (v_S \ , v_T) \ \mathcal{E} \text{ V} \ [\![\ \sigma_1 \ ]\!] \ . \ (e_S[v_s \ / \ x_s] \ , e_T \ [v_{env} \ / \ \text{z} \ , v_T \ / \ x_T]) \in \mathcal{E} \ [\![\ \sigma_2 \ ]\!] \ \}$

3 Logical Relations

In logical relations we map related input to related outputs. Same source value and target value are related.