"LITTLE" SECURE TYPE SYSTEM DRAFT

A. Russo

Andrei:

- All variables are fresh ones
- $\tau_1 \sim \tau_2$ means: τ_1 and τ_2 must unify.
- $\tau_1 \leq \tau_2$ means: τ_1 has a lower security level than τ_2.
- $\tau_1 := max\ \tau_2\ \tau_3$ means: τ_1 is the maximum secure level between τ_2 and τ_3.

$$\text{(INT)} \quad \emptyset \mid \Gamma \vdash_{\mathrm{W}} n : \hat{0}$$

$$\text{(VAR)} \quad \frac{(v : \tau) \in \Gamma}{\emptyset \mid \Gamma \vdash_{\mathrm{W}} v : \tau}$$

$$\text{(SKIP)} \quad t \leq \hat{1} \mid \Gamma \vdash_{\mathrm{W}} \mathbf{skip} : t$$

$$\text{(PLUS)} \quad \frac{\Delta_1 \mid \Gamma \vdash_{\mathrm{W}} e_1 : \tau_1 \quad \Delta_2 \mid \Gamma \vdash_{\mathrm{W}} e_2 : \tau_2}{t := \max \tau_1\, \tau_2, \Delta_1, \Delta_2 \mid \Gamma \vdash_{\mathrm{W}} e_1 \oplus e_2 : t}$$

$$\text{(ASSGN)} \quad \frac{\begin{array}{c}\Delta_v \mid \Gamma \vdash_{\mathrm{W}} v : \tau_v \\ \Delta_e \mid \Gamma \vdash_{\mathrm{W}} e : \tau_e\end{array}}{\tau_e \leq \tau_v, t \leq \tau_v, \Delta_v, \Delta_e \mid \Gamma \vdash_{\mathrm{W}} v := e : t}$$

$$\text{(IF)} \quad \frac{\begin{array}{c}\Delta_e \mid \Gamma \vdash_{\mathrm{W}} e : \tau_e \\ (\Delta_i \mid \Gamma \vdash_{\mathrm{W}} e_i : \tau_i)_{i \in \{1,2\}}\end{array}}{\tau_e \sim \tau_1, \tau_1 \sim \tau_2, t \leq \tau_e, \Delta_e, \Delta_1, \Delta_2 \mid \Gamma \vdash_{\mathrm{W}} \mathbf{if}\ e\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2 : t}$$

$$\text{(WHILE)} \quad \frac{\begin{array}{c}\Delta_e \mid \Gamma \vdash_{\mathrm{W}} e : \tau_e \\ \Delta_{e'} \mid \Gamma \vdash_{\mathrm{W}} e' : \tau_{e'}\end{array}}{\tau_e \sim \tau_{e'}, t \leq \tau_e, \Delta_e, \Delta_{e'} \mid \Gamma \vdash_{\mathrm{W}} \mathbf{while}\ e\ e' : t}$$

$$\text{(SEQ)} \quad \frac{\Delta_1 \mid \Gamma \vdash_{\mathrm{W}} e_1 : \tau_1 \quad \Delta_2 \mid \Gamma \vdash_{\mathrm{W}} e_2 : \tau_2}{\tau_1 \sim \tau_2, \Delta_1, \Delta_2 \mid \Gamma \vdash_{\mathrm{W}} e_1 ; e_2 : \tau_1}$$

Figure 1: Princital Secure Type System