Featherweight Breeze: Step 4/4

Cătălin Hriţcu, Benoît Montagu, Benjamin C. Pierce, and the Breeze team

December 14, 2011

1 Syntax

$L,\ H,\ pc$	::=			label
	|	$\top$	M	top secret
	|	$\bot$	M	unclassified
	|	$L_1 \vee L_2$	M	label join
	|	(L)	S	
c	::=			constants
	|	$()$	M	unit
	|	true	M	true
	|	false	M	false
	|	L		label
t	::=			terms
	|	c		constant
	|	x		variable
	|	$\lambda x.t$	bind x in t	abstraction
	|	$t_1\ t_2$		application
	|	$t_1 == t_2$		equality on constants
	|	$t_1\langle t_2\rangle$		executes t_2, labels result with t_1, restores pc
	|	labelOf t		returns the label of t
	|	getPc ()		returns the current pc
	|	valueOf t		labels t with $\bot$ if pc high enough
	|	raisePc t		only construct that raises the pc (by t)
	|	(t)	S	
v	::=			values
	|	c		constants
	|	$\langle \rho,\ \lambda x.\ t\rangle$	bind x in t	closures

a	$::=$		atoms
	$\vert$	$v@L$	labeled value
ρ	$::=$		environments
	$\vert$	$empty$	
	$\vert$	$\rho, x \mapsto a$	
	$\vert$	(ρ)	S

2 Evaluation with Dynamic IF Control

$\boxed{\rho \vdash t, pc \Downarrow a, pc'}$

$$\frac{}{\rho \vdash c, pc \Downarrow c@\bot, pc} \quad \textsc{Eval\_Const}$$

$$\frac{\rho(x) = a}{\rho \vdash x, pc \Downarrow a, pc} \quad \textsc{Eval\_Var}$$

$$\frac{}{\rho \vdash (\lambda x.t), pc \Downarrow \langle \rho,\ \lambda x.\ t\rangle@\bot, pc} \quad \textsc{Eval\_Abs}$$

$$\frac{\begin{array}{l}\rho \vdash t', pc \Downarrow \langle \rho',\ \lambda x.\ t\rangle@L', pc' \\ L' \sqsubseteq pc' \\ \rho \vdash t'', pc' \Downarrow a'', pc'' \\ (\rho', x \mapsto a'') \vdash t, pc'' \Downarrow a, pc'''\end{array}}{\rho \vdash (t'\ t''), pc \Downarrow a, pc'''} \quad \textsc{Eval\_App}$$

$$\frac{\begin{array}{l}\rho \vdash t', pc \Downarrow c'@L', pc' \\ \rho \vdash t'', pc' \Downarrow c''@L'', pc'' \\ v \triangleq c' = c''\end{array}}{\rho \vdash (t' == t''), pc \Downarrow v@(L' \vee L''), pc''} \quad \textsc{Eval\_Eq}$$

$$\frac{\begin{array}{l}\rho \vdash t', pc \Downarrow L@L', pc' \\ L' \sqsubseteq pc' \\ \rho \vdash t'', pc' \Downarrow v@L'', pc'' \\ L'' \sqsubseteq L \vee pc' \\ pc'' \sqsubseteq L \vee pc'\end{array}}{\rho \vdash t'\langle t''\rangle, pc \Downarrow v@L, pc'} \quad \textsc{Eval\_Bracket}$$

$$\frac{\rho \vdash t, pc \Downarrow v@L, pc'}{\rho \vdash \mathsf{labelOf}\, t, pc \Downarrow L@\bot, pc'} \quad \textsc{Eval\_LabelOf}$$

$$\frac{}{\rho \vdash \mathsf{getPc}\,(), pc \Downarrow pc@\bot, pc} \quad \textsc{Eval\_GetPc}$$

$$\frac{\begin{array}{l}\rho \vdash t, pc \Downarrow v@L, pc' \\ L \sqsubseteq pc'\end{array}}{\rho \vdash \mathsf{valueOf}\, t, pc \Downarrow v@\bot, pc'} \quad \textsc{Eval\_ValueOf}$$

$$\frac{\rho \vdash t, pc \Downarrow L@L', pc' \quad L' \sqsubseteq pc'}{\rho \vdash \mathsf{raisePc}\ t, pc \Downarrow ()@\bot, (pc' \vee L)} \quad \text{EVAL\_RAISEPC}$$

3 Changes wrt Step 3

- Removed all constructs that can be faithfully Church encoded: let, pairs and projections, booleans and conditionals, classification, unit. Exercise: try out some of these encodings.
- Added new construct for manually raising the *pc*.
- Made all constructs that used to raise the *pc* expect that the *pc* was manually raised before. Affects rules: EVAL_APP, EVAL_BRACKET, and EVAL_VALUEOF.

4 Termination-insensitive Non-interference

Lemma 1 (Monotonous PC)**.** *If* $\rho \vdash t, pc \Downarrow a, pc'$ *then* $pc \sqsubseteq pc'$.

Definition 1 (Low Equivalence)**.**

$$\frac{\textit{if } pc_1 \sqsubseteq L \vee pc_2 \sqsubseteq L \textit{ then } X_1 \simeq_L X_2 \wedge pc_1 = pc_2}{X_1, pc_1 \simeq_L X_2, pc_1}$$

$$\frac{\textit{if } L' \sqsubseteq L \textit{ then } v_1 \simeq_L v_2}{v_1@L' \simeq_L v_2@L'}$$

$$L' \simeq_L L'$$

$$\frac{\rho_1 \simeq_L \rho_2}{\langle \rho_1, \lambda x.\, t\rangle \simeq_L \langle \rho_2, \lambda x.\, t\rangle}$$

$$\textit{empty} \simeq_L \textit{empty}$$

$$\frac{\rho_1 \simeq_L \rho_2 \quad a_1 \simeq_L a_2}{\rho_1, x \mapsto a_1 \simeq_L \rho_2, x \mapsto a_2}$$

Theorem 2 (Non-interference)**.** *If* $\rho_1 \vdash t, pc_1 \Downarrow a_1, pc_1'$, *and* $\rho_2 \vdash t, pc_2 \Downarrow a_2, pc_2'$, *and* $\rho_1, pc_1 \simeq_L \rho_2, pc_2$, *then* $a_1, pc_1' \simeq_L a_2, pc_2'$.