Dependent Types for the Verification of Information Flow and Access Control Policies: Online Appendix

Version of May 18, 2012

Aleksandar Nanevski Anindya Banerjee
IMDEA Software Institute
{aleks.nanevski, anindya.banerjee}@imdea.org

Deepak Garg
Max Planck Institute for Software Systems
dg@mpi-sws.org

1 Right Reduction Rules

$$\textsc{val\_ret}\mathrm{V}\ \frac{r\ v\ i}{\mathsf{verify}\, i\, (\mathsf{return}\ @\ v)\, r} \qquad \textsc{bnd\_ret}\mathrm{V}\ \frac{\mathsf{verify}\, i\, (e\ @\ v)\, r}{\mathsf{verify}\, i\, ((\mathsf{return}\ @\ v); e)\, r}$$

$$\textsc{val\_read}\mathrm{V}\ \frac{r\ v\ (\ell \mapsto v \bullet i)}{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, (\mathsf{read}\ @\ l)\, r} \qquad \textsc{bnd\_read}\mathrm{V}\ \frac{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, (e\ @\ v)\, r}{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, ((\mathsf{read}\ @\ l); e)\, r}$$

$$\textsc{val\_write}\mathrm{V}\ \frac{r\ ()\ (\ell \mapsto v \bullet i)}{\mathsf{verify}\, (\ell \mapsto w \bullet i)\, (\mathsf{write}\ @\ (l, v))\, r}$$

$$\textsc{bnd\_write}\mathrm{V}\ \frac{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, (e\ @\ ())\, r}{\mathsf{verify}\, (\ell \mapsto w \bullet i)\, ((\mathsf{write}\ @\ (l, v)); e)\, r} \qquad \textsc{val\_lalloc}\mathrm{V}\ \frac{\forall \ell : ptr. r\ \ell\ (\ell \mapsto v \bullet i)}{\mathsf{verify}\, i\, (\mathsf{lalloc}\ @\ v)\, r}$$

$$\textsc{bnd\_lalloc}\mathrm{V}\ \frac{\forall \ell : ptr. \mathsf{verify}\, (\ell \mapsto v \bullet i)\, (e\ @\ \ell)\, r}{\mathsf{verify}\, i\, ((\mathsf{lalloc}\ @\ v); e)\, r}$$

$$\textsc{val\_halloc}\mathrm{V}\ \frac{\forall \ell : ptr. \mathsf{even}\ \ell \Rightarrow r\ \ell\ (\ell \mapsto v \bullet i)}{\mathsf{verify}\, i\, (\mathsf{alloc}\ @\ v)\, r}$$

$$\textsc{bnd\_halloc}\mathrm{V}\ \frac{\forall \ell : ptr. \mathsf{verify}\, (\ell \mapsto v \bullet i)\, (e\ @\ \ell)\, (\mathsf{fun}\ y\ m.\ \mathsf{even}\ \ell \Rightarrow r\ y\ m)}{\mathsf{verify}\, i\, ((\mathsf{alloc}\ @\ v); e)\, r}$$

$$\textsc{val\_dealloc}\mathrm{V}\ \frac{r\ ()\ i}{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, (\mathsf{dealloc}\ @\ \ell)\, r}$$

$$\textsc{bnd\_dealloc}\mathrm{V}\ \frac{\mathsf{verify}\, i\, (e\ @\ ())\, r}{\mathsf{verify}\, (\ell \mapsto v \bullet i)\, ((\mathsf{dealloc}\ @\ l); e)\, r} \qquad \textsc{val\_inst}\mathrm{V}\ \frac{\mathsf{verify}\, i\, (e_1\ @\ (f a))\, r}{\mathsf{verify}\, i\, (e_1\ @\ f\ @\ a)\, r}$$

$$\textsc{bnd\_push}\mathrm{V}\ \frac{\mathsf{verify}\, i\, ((e_1\ @\ a); (e_2\ @_1\ (\mathsf{fun}\ y.\ (y, a))))\, r}{\mathsf{verify}\, i\, ((e_1; e_2)\ @\ a)\, r} \qquad \textsc{bnd\_inst}\mathrm{V}\ \frac{\mathsf{verify}\, i\, ((e_1\ @\ (f a)); e_2)\, r}{\mathsf{verify}\, i\, ((e_1\ @\ f\ @\ a); e_2)\, r}$$

Figure 1: Right reduction rules

2 Both Ways Reduction Rules

$$\text{VAL\_RET}\ \frac{r(v_1, v_2)(i_1, i_2)}{\mathsf{verify2}\, i_1\, i_2\, (\mathsf{return}\ @\ v_1)\, (\mathsf{return}\ @\ v_2)\, r}$$

$$\text{BND\_RET}\ \frac{\mathsf{verify2}\, i_1\, i_2\, (e_1\ @\ v_1)\, (e_2\ @\ v_2)\, r}{\mathsf{verify2}\, i_1\, i_2\, ((\mathsf{return}\ @\ v_1); e_1)\, ((\mathsf{return}\ @\ v_2); e_2)\, r}$$

$$\text{VAL\_READ}\ \frac{r\ (v_1, v_2)\ (l_1 \mapsto v_1 \bullet i_1, l_2 \mapsto v_2 \bullet i_2)}{\mathsf{verify2}\, (l_1 \mapsto v_1 \bullet i_1)\, (l_2 \mapsto v_2 \bullet i_2)\, (\mathsf{read}\ @\ l_1)\, (\mathsf{read}\ @\ l_2)\, r}$$

$$\text{BND\_READ}\ \frac{\mathsf{verify2}\, (l_1 \mapsto v_1 \bullet i_1)\, (l_2 \mapsto v_2 \bullet i_2)\, (e_1\ @\ v_1)\, (e_2\ @\ v_2)\, r}{\mathsf{verify2}\, (l_1 \mapsto v_1 \bullet i_1)\, (l_2 \mapsto v_2 \bullet i_2)\, ((\mathsf{read}\ @\ l_1); e_1)\, ((\mathsf{read}\ @\ l_2); e_2)\, r}$$

$$\text{VAL\_WRITE}\ \frac{r\ ((), ())\ (l_1 \mapsto v_1 \bullet i_1, l_2 \mapsto v_2 \bullet i_2)}{\mathsf{verify2}\, (l_1 \mapsto w_1 \bullet i_1)\, (l_2 \mapsto w_2 \bullet i_2)\, (\mathsf{write}\ @\ (l_1, v_1))\, (\mathsf{write}\ @\ (l_2, v_2))\, r}$$

$$\text{BND\_WRITE}\ \frac{\mathsf{verify2}\, (l_1 \mapsto v_1 \bullet i_1)\, (l_2 \mapsto v_2 \bullet i_2)\, (e_1\ @\ ())\, (e_2\ @\ ())\, r}{\mathsf{verify2}\, (l_1 \mapsto v_1 \bullet i_1)\, (l_2 \mapsto v_2 \bullet i_2)\, ((\mathsf{write}\ @\ (l_1, v_1)); e_1)\, ((\mathsf{write}\ @\ (l_2, v_2)); e_2)\, r}$$

$$\text{VAL\_LALLOC}\ \frac{\begin{array}{c}\forall \ell_1, \ell_2 : ptr. i_1 \cong i_2 \Rightarrow (\ell_1 = \ell_2)\ \wedge\ (\ell_1 \mapsto v_1 \bullet i_1 \cong \ell_2 \mapsto v_2 \bullet i_2) \\ \forall \ell_1, \ell_2 : ptr. r\ (\ell_1, \ell_2)\ (\ell_1 \mapsto v_1 \bullet i_1, \ell_2 \mapsto v_2 \bullet i_2)\end{array}}{\mathsf{verify2}\, i_1\, i_2\, (\mathsf{lalloc}\ @\ v_1)\, (\mathsf{lalloc}\ @\ v_2)\, r}$$

$$\text{BND\_LALLOC}\ \frac{\begin{array}{c}\forall \ell_1, \ell_2 : ptr. \mathsf{verify2}\, (\ell_1 \mapsto v_1 \bullet i_1)\, (\ell_2 \mapsto v_2 \bullet i_2)\, (e_1\ @\ \ell_1)\, (e_2\ @\ \ell_2)\, r' \\ r' = \mathsf{fun}\ y\ m.\ (i_1 \cong i_2\ \wedge\ \ell_1 = \ell_2\ \wedge\ \ell_1 \mapsto v_1 \bullet i_1 \cong \ell_2 \mapsto v_2 \bullet i_2) \Rightarrow r\ y\ m\end{array}}{\mathsf{verify2}\, i_1\, i_2\, ((\mathsf{lalloc}\ @\ v_1); e_1)\, ((\mathsf{lalloc}\ @\ v_2); e_2)\, r}$$

Figure 2: Both ways reduction rules: 1 of 2

$$\textsc{val\_halloc}\ \frac{\forall \ell_1, \ell_2 : ptr.\mathsf{even}\ \ell_1\ \wedge\ \mathsf{even}\ \ell_2 \Rightarrow r\ (\ell_1, \ell_2)\ (\ell_1 \mapsto v_1 \bullet i_1, \ell_2 \mapsto v_2 \bullet i_2)}{\mathsf{verify2}\, i_1\, i_2\, (\mathsf{alloc}\ @\ v_1)\, (\mathsf{alloc}\ @\ v_2)\, r}$$

$$\textsc{bnd\_halloc}\ \frac{\begin{array}{c}\forall \ell_1, \ell_2 : ptr.\mathsf{verify2}\, (\ell_1 \mapsto v_1 \bullet i_1)\, (\ell_2 \mapsto v_2 \bullet i_2)\, (e_1\ @\ \ell_1)\, (e_2\ @\ \ell_2)\, r' \\ r' = \mathsf{fun}\ yy\ mm.\ (\mathsf{even}\ \ell_1 \wedge \mathsf{even}\ \ell_2) \Rightarrow r\ yy\ mm\end{array}}{\mathsf{verify2}\, i_1\, i_2\, ((\mathsf{alloc}\ @\ v_1); e_1)\, ((\mathsf{alloc}\ @\ v_2); e_2)\, r}$$

$$\textsc{val\_dealloc}\ \frac{r\ ((), ())\ (i_1, i_2)}{\mathsf{verify2}\, (\ell_1 \mapsto v_1 \bullet i_1)\, (\ell_2 \mapsto v_2 \bullet i_2)\, (\mathsf{dealloc}\ @\ \ell_1)\, (\mathsf{dealloc}\ @\ \ell_2)\, r}$$

$$\textsc{bnd\_dealloc}\ \frac{\mathsf{verify2}\, i_1\, i_2\, (e_1\ @\ ())\, (e_2\ @\ ())\, r}{\mathsf{verify2}\, (\ell_1 \mapsto v_1 \bullet i_1)\, (\ell_2 \mapsto v_2 \bullet i_2)\, ((\mathsf{dealloc}\ @\ \ell_1); e_1)\, ((\mathsf{dealloc}\ @\ \ell_2); e_2)\, r}$$

$$\textsc{val\_inst}\mathrm{R}\ \frac{\mathsf{verify2}\, i\, j\, e_2\, (e_1\ @\ (f\ a))\, r}{\mathsf{verify2}\, i\, j\, e_2\, (e_1\ @\ f\ @\ a)\, r}$$

$$\textsc{bnd\_push}\mathrm{R}\ \frac{\mathsf{verify2}\, i\, j\, e_3\, ((e_1\ @\ a); (e_2\ @_1\ (\mathsf{fun}\ y.\ (y, a))))\, r}{\mathsf{verify2}\, i\, j\, e_3\, ((e_1; e_2)\ @\ a)\, r}$$

$$\textsc{bnd\_inst}\mathrm{R}\ \frac{\mathsf{verify2}\, i\, j\, e_3\, ((e_1\ @\ (f\ a)); e_2)\, r}{\mathsf{verify2}\, i\, j\, e_3\, ((e_1\ @\ f\ @\ a); e_2)\, r}$$

Figure 3: Both ways reduction rules: 2 of 2