Subtyping for Access Control

MyThS REVIEW MEETING

Vladimiro Sassone

University of Sussex,

Group Types for Mobility

Aim: *Resource Access Control*

- Detect and prevent unwanted access to resources.
- We focus on static approaches based on enforcing type disciplines.

Group Types for Mobility

Aim: *Resource Access Control*

- Detect and prevent unwanted access to resources.
- We focus on static approaches based on enforcing type disciplines.

Groups: Sets of processes with common access rights. (Cardelli-Ghelli-Gordon)

Constraints like $k : \mathsf{CanEnter}(n)$ are modelled as:

n belongs to group G

k may cross the border of any ambient of group G.

For instance, the system:

$$k[\,\mathtt{in}\,n \mid l[\,\mathtt{out}\,k\,]\,] \;\mid\; n[\,\_\,]$$

is well-typed under assumptions of the form:

$$k : \mathsf{amb}[\mathtt{K}, \mathsf{cross}(\mathtt{N})]$$

$$l : \mathsf{amb}[\mathtt{L}, \mathsf{cross}(\mathtt{K})] \qquad\qquad n : \mathsf{amb}[\mathtt{N}, \ldots]$$

Indirect Border Crossing in MA

Troyan Horses: The system

$$\mathrm{Odysseus}[\,\mathtt{in}\,\mathrm{Horse}.\mathtt{out}\,\mathrm{Horse}.\mathit{Destroy}\,] \mid \mathrm{Horse}[\,\mathtt{in}\,\mathrm{Troy}\,] \mid \mathrm{Troy}[\,\mathit{Trojans}\,]$$

is well-typed under assumptions:

$$\mathrm{Odysseus} : \mathrm{amb}[\mathtt{Achaean}, \mathrm{cross}(\mathtt{Toy})]$$

$$\mathrm{Horse} : \mathrm{amb}[\mathtt{Toy}, \mathrm{cross}(\mathtt{City})]$$

$$\mathrm{Troy} : \mathrm{amb}[\mathtt{City}, \_]$$

Indirect Border Crossing in MA

Troyan Horses: The system

$$\mathrm{Odysseus}[\,\mathtt{in}\,\mathrm{Horse}.\mathtt{out}\,\mathrm{Horse}.\mathit{Destroy}\,] \mid \mathrm{Horse}[\,\mathtt{in}\,\mathrm{Troy}\,] \mid \mathrm{Troy}[\,\mathit{Trojans}\,]$$

is well-typed under assumptions:

$$\mathrm{Odysseus} : \mathrm{amb}[\mathtt{Achaean}, \mathrm{cross}(\mathtt{Toy})]$$

$$\mathrm{Horse} : \mathrm{amb}[\mathtt{Toy}, \mathrm{cross}(\mathtt{City})]$$

$$\mathrm{Troy} : \mathrm{amb}[\mathtt{City}, \_]$$

However, the system may evolve to

$$\mathrm{Troy}[\,\mathit{Trojans} \mid \mathrm{Horse}[\,\_\,] \mid \mathrm{Odysseus}[\,\mathit{Destroy}\,]\,]$$

where Odysseus got inside Troy's Walls taking by surprise the *Trojans*.

Typed Boxed Ambients: Syntax

η	$::=$	n	names
	$\mid$	$\uparrow$	enclosing amb
	$\mid$	$\star$	local

P	$::=$	$\mathbf{0}$	nil process
	$\mid$	$P_1 \mid P_2$	composition
	$\mid$	$(\nu n{:}A)P$	restriction
	$\mid$	$!P$	replication
	$\mid$	$V[\,P\,]$	ambient
	$\mid$	$V.P$	prefixing
	$\mid$	$(\boldsymbol{x} : \boldsymbol{W})^{\eta}.P$	input
	$\mid$	$\langle \boldsymbol{V} \rangle^{\eta}.P$	output
	$\mid$	$(\nu \mathtt{G})P$	group creation

V, U	$::=$	n	name
	$\mid$	$\mathtt{in}\, V$	may enter V
	$\mid$	$\mathtt{out}\, V$	may exit V
	$\mid$	$V_1.V_2$	path

Reduction Semantics

Mobility:

$$n[\,\mathtt{in}\,m.P|Q\,] \;\mid\; m[\,R\,] \;\rightarrow m[\,n[\,P \mid Q\,] \mid R\,] \qquad \text{(In)}$$

$$m[\,n[\,\mathtt{out}\,m.P \mid Q\,] \mid R\,] \;\rightarrow n[\,P \mid Q\,] \;\mid\; m[\,R\,] \qquad \text{(Out)}$$

Reduction Semantics

Mobility:

$$n[\,\mathtt{in}\,m.P|Q\,] \;\mid\; m[\,R\,] \;\rightarrow m[\,n[\,P \mid Q\,] \mid R\,] \qquad \text{(In)}$$

$$m[\,n[\,\mathtt{out}\,m.P \mid Q\,] \mid R\,] \;\rightarrow n[\,P \mid Q\,] \mid m[\,R\,] \qquad \text{(Out)}$$

Communication:

$$(\boldsymbol{x}).P \mid \langle \boldsymbol{V} \rangle.Q \;\rightarrow P\{\boldsymbol{V}/\boldsymbol{x}\} \mid Q \qquad \text{(Comm Local)}$$

$$(\boldsymbol{x})^n.P \mid n[\,\langle \boldsymbol{V} \rangle.Q \mid R\,] \;\rightarrow P\{\boldsymbol{V}/\boldsymbol{x}\} \mid n[\,Q \mid R\,] \qquad \text{(Comm Input } n\text{)}$$

$$(\boldsymbol{x}).P \mid n[\,\langle \boldsymbol{V} \rangle^{\uparrow}.Q \mid R\,] \;\rightarrow P\{\boldsymbol{V}/\boldsymbol{x}\} \mid n[\,Q|R\,] \qquad \text{(Comm Output } \uparrow\text{)}$$

$$\langle \boldsymbol{V} \rangle^n.P \mid n[\,(\boldsymbol{x}).Q \mid R\,] \;\rightarrow P \mid n[\,Q\{\boldsymbol{V}/\boldsymbol{x}\} \mid R\,] \qquad \text{(Comm Output } n\text{)}$$

$$\langle \boldsymbol{V} \rangle.P \mid n[\,(\boldsymbol{x})^{\uparrow}.Q \mid R\,] \;\rightarrow P \mid n[\,Q\{\boldsymbol{V}/\boldsymbol{x}\} \mid R\,] \qquad \text{(Comm Input } \uparrow\text{)}$$

Types

Groups: $\mathtt{G}, \mathtt{H}, \ldots$

Sets of groups: $\mathscr{G}, \mathscr{D}, \mathscr{S}, \ldots$ $\quad \mathscr{U}$ The universal set of groups

Ambients types:

$A \quad ::= \quad \mathrm{amb}_{\chi}[\mathtt{G}, M, C]$ amb of group $\mathtt{G}$, good for actions $\chi \subseteq \{\mathtt{i}, \mathtt{o}, \mathtt{c}, \mathtt{r}, \mathtt{w}\}$, with mobility type M, and communication type C

Process types:

$\Pi \quad ::= \quad \mathrm{proc}[\mathtt{G}, M, C]$ process that can be enclosed in an ambient of group $\mathtt{G}$, may drive to ambients whose groups are in M, and communicates as described by type C

Capability types:

$K \quad ::= \quad \mathrm{cap}[\mathtt{G}, M, F]$ capability that can appear in an ambient of group $\mathtt{G}$, may drive it to ambients whose groups are in M, with exchange type F for local communication

Types (cont.)

Mobility types:

$$M \;::=\; \mathsf{mob}[\mathscr{G}]$$ mobility specs

Communication types:

$$C \;::=\; \mathsf{com}[E, F]$$ E for local and F for upward exchange

Exchange types:

$$E, F \;::=\; \mathsf{rw}[I, O]$$ read/write values (valid if $O \prec I$)

Message types:

$$I, O \;::=\; \bot \;\mid\; W_1 \times \ldots \times W_k \;\mid\; \top$$ bottom, tuple, top

Value types:

$$W, Y \;::=\; A$$ ambient name

$$\mid\; K$$ capability

Subtyping

(sAmb)
$$\frac{\chi_1 \subseteq \chi_0 \subseteq \{\mathtt{i}, \mathtt{o}, \mathtt{c}, \mathtt{r}, \mathtt{w}\}}{\mathsf{amb}_{\chi_0}[\mathtt{G}, M, C] \prec \mathsf{amb}_{\chi_1}[\mathtt{G}, M, C]}$$

(sProc)
$$\frac{M_0 \prec M_1; \quad C_0 \prec C_1}{\mathsf{proc}[\mathtt{G}, M_0, C_0] \prec \mathsf{proc}[\mathtt{G}, M_1, C_1]}$$

(sCap)
$$\frac{M_0 \prec M_1; \quad F_0 \prec F_1}{\mathsf{cap}[\mathtt{G}, M_0, F_0] \prec \mathsf{cap}[\mathtt{G}, M_1, F_1]}$$

(sMob)
$$\frac{\mathscr{G}_0 \subseteq \mathscr{G}_1}{\mathsf{mob}[\mathscr{G}_0] \prec \mathsf{mob}[\mathscr{G}_1]}$$

(sCom)
$$\frac{E_0 \prec E_1; \quad F_0 \prec F_1}{\mathsf{com}[E_0, F_0] \prec \mathsf{com}[E_1, F_1]}$$

(sExc)
$$\frac{I_1 \prec I_0; \quad O_0 \prec O_1}{\mathsf{rw}[I_0, O_0] \prec \mathsf{rw}[I_1, O_1]}$$

(sMsg)
$$\frac{-}{\bot \prec W_1 \times \ldots \times W_k \prec \top}$$

(sTuple)
$$\frac{W_i \prec T_i; \quad i \in 1..k}{W_1 \times \ldots \times W_k \prec T_1 \times \ldots \times T_k}$$

Good Values

(Val n)
$$\frac{\Gamma, n : W, \Gamma' \vdash \diamond}{\Gamma, n : W, \Gamma' \vdash n : W}$$

(Val pfx)
$$\frac{\Gamma \vdash V_0 : K; \;\; \Gamma \vdash V_1 : K}{\Gamma \vdash V_0.V_1 : K}$$

(Val in)
$$\frac{\Gamma \vdash V : \mathsf{amb_i}[\mathtt{G}, M, \mathsf{com}[E, F]]}{\Gamma \vdash \mathtt{in}\, V : \mathsf{cap}[\mathtt{H}, \mathsf{mob}[\{\mathtt{G}\}], E]}\ \mathtt{H} \in \Gamma$$

(Val sub)
$$\frac{\Gamma \vdash V : W; \quad W \prec W'}{\Gamma \vdash V : W'}$$

(Val out)
$$\frac{\Gamma \vdash V : \mathsf{amb_o}[\mathtt{G}, M, \mathsf{com}[E, F]]}{\Gamma \vdash \mathtt{out}\, V : \mathsf{cap}[\mathtt{H}, M, F]}\ \mathtt{H} \in \Gamma$$

Good Processes – Mobility

(Pro pfx)
$$\frac{\Gamma \vdash V{:}\mathrm{cap}[\mathtt{G}, M, F];\quad \Gamma \vdash P{:}\mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, F]]}{\Gamma \vdash V.P{:}\mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, F]]}$$

(Pro amb)
$$\frac{\Gamma \vdash V{:}\mathrm{amb_c}[\mathtt{H}, \mathrm{mob}[\mathscr{S}], \mathrm{com}[E, F]];\ \Gamma \vdash P{:}\mathrm{proc}[\mathtt{H}, \mathrm{mob}[\mathscr{S}], \mathrm{com}[E, F]]}{\Gamma \vdash V[\,P\,]{:}\mathrm{proc}[\mathtt{G}, \mathrm{mob}[\emptyset], \mathrm{com}[F, \mathrm{zero}]]}\ \mathtt{G} \in \mathscr{S}$$

(Pro res)
$$\frac{\Gamma, n : A \vdash P : \Pi}{\Gamma \vdash (\nu n : A)P : \Pi}$$

(Pro gres)
$$\frac{\Gamma, \mathtt{G} \vdash P : \Pi}{\Gamma \vdash (\nu \mathtt{G})P : \Pi}\ \mathtt{G} \notin \mathsf{fg}(\Pi)$$

(Pro $\mathbf{0}$)
$$\frac{\mathtt{G} \in \mathsf{dom}(\Gamma)}{\Gamma \vdash \mathbf{0} : \mathrm{proc}[\mathtt{G}, \mathrm{mob}[\emptyset], \mathrm{com}[\mathrm{zero}, \mathrm{zero}]]}$$

(Pro par)
$$\frac{\Gamma \vdash P : \Pi;\ \Gamma \vdash Q : \Pi}{\Gamma \vdash P \mid Q : \Pi}$$

(Pro rep)
$$\frac{\Gamma \vdash P : \Pi}{\Gamma \vdash\, !P : \Pi}$$

(Pro sub)
$$\frac{\Gamma \vdash P : \Pi \quad \Pi \prec \Pi'}{\Gamma \vdash P : \Pi'}$$

Good Processes – Communication

(inp $\star$)

$$\frac{\Gamma, \boldsymbol{x} : \boldsymbol{W} \vdash P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[\mathrm{rw}[I, O], F]]}{\Gamma \vdash (\boldsymbol{x} : \boldsymbol{W}).P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[\mathrm{rw}[I, O], F]]}\ I \prec \boldsymbol{W}$$

(out $\star$)

$$\frac{\Gamma \vdash \boldsymbol{V} : \boldsymbol{W}; \quad \Gamma \vdash P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[\mathrm{rw}[I, \boldsymbol{W}], F]]}{\Gamma \vdash \langle \boldsymbol{V} \rangle.P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[\mathrm{rw}[I, \boldsymbol{W}], F]]}$$

(inp $\uparrow$)

$$\frac{\Gamma, \boldsymbol{x} : \boldsymbol{W} \vdash P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, \mathrm{rw}[I, O]]]}{\Gamma \vdash (\boldsymbol{x} : \boldsymbol{W}_k)^{\uparrow}.P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, \mathrm{rw}[I, O]]]}\ I \prec \boldsymbol{W}$$

(output $\uparrow$)

$$\frac{\Gamma \vdash \boldsymbol{V} : \boldsymbol{W}; \quad \Gamma \vdash P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, \mathrm{rw}[I, \boldsymbol{W}]]]}{\Gamma \vdash \langle \boldsymbol{V} \rangle^{\uparrow}.P : \mathrm{proc}[\mathtt{G}, M, \mathrm{com}[E, \mathrm{rw}[I, \boldsymbol{W}]]]}$$

...and so on analogously

Properties

Communication properties:

- If $\Gamma \vdash (\boldsymbol{x} : \boldsymbol{W}).P \mid \langle \boldsymbol{V} \rangle.Q : \Pi$ then $\Gamma \vdash \boldsymbol{V}{:}\boldsymbol{Y}$ with $\boldsymbol{Y} \prec \boldsymbol{W}$.

Properties

Communication properties:

- If $\Gamma \vdash (\boldsymbol{x} : \boldsymbol{W}).P \mid \langle \boldsymbol{V} \rangle.Q : \Pi$ then $\Gamma \vdash \boldsymbol{V}{:}\boldsymbol{Y}$ with $\boldsymbol{Y} \prec \boldsymbol{W}$.

Mobility properties:

- If $\Gamma \vdash n[\,\mathtt{in}\, m.P \mid Q\,] \mid m[\,R\,] : \Pi$, then

$$\Gamma \vdash m : \mathtt{amb}_{\chi_0}[\mathtt{M}, \_, \_] \quad \text{and} \quad \Gamma \vdash n : \mathtt{amb}_{\chi_1}[\_, \mathtt{mob}[\mathscr{S}], \_]$$

  with $\mathtt{M} \in \mathscr{S}$, $\mathtt{i}, \mathtt{c} \in \chi_0$ and $\mathtt{c} \in \chi_1$.

- If $\Gamma \vdash m[\,n[\,\mathtt{out}\, m.P \mid Q\,] \mid R\,] : \Pi$, then

$$\Gamma \vdash m : \mathtt{amb}_{\chi_0}[\mathtt{M}, \mathtt{mob}[\mathscr{S}_m], \_] \text{ and } \Gamma \vdash n : \mathtt{amb}_{\chi_1}[\mathtt{N}, \mathtt{mob}[\mathscr{S}_n], \_]$$

  with $\mathtt{o}, \mathtt{c} \in \chi_0$, $\mathtt{c} \in \chi_1$, $\mathtt{M} \in \mathscr{S}_n$ and $\mathscr{S}_m \subseteq \mathscr{S}_n$.

Properties

Communication properties:

- If $\Gamma \vdash (\boldsymbol{x} : \boldsymbol{W}).P \mid \langle \boldsymbol{V} \rangle.Q : \Pi$ then $\Gamma \vdash \boldsymbol{V}{:}\boldsymbol{Y}$ with $\boldsymbol{Y} \prec \boldsymbol{W}$.

Mobility properties:

- If $\Gamma \vdash n[\,\mathtt{in}\, m.P \mid Q\,] \mid m[\,R\,] : \Pi$, then

$$\Gamma \vdash m : \mathtt{amb}_{\chi_0}[\mathtt{M}, \_, \_] \quad \text{and} \quad \Gamma \vdash n : \mathtt{amb}_{\chi_1}[\_, \mathtt{mob}[\mathscr{S}], \_]$$

  with $\mathtt{M} \in \mathscr{S}$, $\mathtt{i}, \mathtt{c} \in \chi_0$ and $\mathtt{c} \in \chi_1$.

- If $\Gamma \vdash m[\,n[\,\mathtt{out}\, m.P \mid Q\,] \mid R\,] : \Pi$, then

$$\Gamma \vdash m : \mathtt{amb}_{\chi_0}[\mathtt{M}, \mathtt{mob}[\mathscr{S}_m], \_] \text{ and } \Gamma \vdash n : \mathtt{amb}_{\chi_1}[\mathtt{N}, \mathtt{mob}[\mathscr{S}_n], \_]$$

  with $\mathtt{o}, \mathtt{c} \in \chi_0$, $\mathtt{c} \in \chi_1$, $\mathtt{M} \in \mathscr{S}_n$ and $\mathscr{S}_m \subseteq \mathscr{S}_n$.

Subject reduction:

- If $\Gamma \vdash P : \Pi$ and $P \equiv Q$ or $P \rightarrow Q$, then there exist groups $\mathtt{G}_0, \ldots \mathtt{G}_k$ such that $\mathtt{G}_0, \ldots, \mathtt{G}_k, \Gamma \vdash Q : \Pi$.

Detecting Odysseus' intentions

Now, in order to assign a type to

$$\mathtt{Odysseus}[\,\mathtt{in}\,\mathtt{Horse}.\mathtt{out}\,\mathtt{Horse}.\mathit{Destroy}\,] \mid \mathtt{Horse}[\,\mathtt{in}\,\mathtt{Troy}\,] \mid \mathtt{Troy}[\,\mathit{Trojans}\,]$$

we need assumptions of the form:

$$\mathtt{Odysseus} : \mathtt{amb_c}[\mathtt{Achaean}, \mathtt{mob}[\{\mathtt{Ground}, \mathtt{Toy}, \mathtt{City}\}], \_]$$

$$\mathtt{Horse} : \mathtt{amb_{ioc}}[\mathtt{Toy}, \mathtt{mob}[\{\mathtt{Ground}, \mathtt{City}\}], \_]$$

$$\mathtt{Troy} : \mathtt{amb_{ioc}}[\mathtt{City}, \_, \_]$$

representing that Odysseus is an Achaean intentioned to move into a City!

Detecting Odysseus' intentions

Now, in order to assign a type to

$$\mathtt{Odysseus}[\,\mathtt{in}\,\mathtt{Horse}.\mathtt{out}\,\mathtt{Horse}.\mathit{Destroy}\,] \mid \mathtt{Horse}[\,\mathtt{in}\,\mathtt{Troy}\,] \mid \mathtt{Troy}[\,\mathit{Trojans}\,]$$

we need assumptions of the form:

$$\mathtt{Odysseus} : \mathtt{amb}_{\mathtt{c}}[\mathtt{Achaean}, \mathtt{mob}[\{\mathtt{Ground}, \mathtt{Toy}, \mathtt{City}\}], \_]$$

$$\mathtt{Horse} : \mathtt{amb}_{\mathtt{ioc}}[\mathtt{Toy}, \mathtt{mob}[\{\mathtt{Ground}, \mathtt{City}\}], \_]$$

$$\mathtt{Troy} : \mathtt{amb}_{\mathtt{ioc}}[\mathtt{City}, \_, \_]$$

representing that Odysseus is an Achaean intentioned to move into a City!
On the other hand, under assumptions of the form

$$\mathtt{Odysseus} : \mathtt{amb}_{\mathtt{c}}[\mathtt{Achaean}, \mathtt{mob}[\{\mathtt{Ground}, \mathtt{Toy}\}], \_]$$

the *Trojans* should not fear any attack from Odysseus.

But what if Odysseus is lying about his intentions (i.e. type)?

BSA: Adding co-capabilities

Reduction Semantics:

$$n[\,\mathtt{in}\,m.P \mid Q\,] \mid m[\,\overline{\mathtt{in}}\,\alpha.R \mid S\,] \;\rightarrow m[\,n[\,P \mid Q\,] \mid R \mid S\,] \quad \text{for } \alpha \in \{\star, n\}$$

$$m[\,n[\,\mathtt{out}\,m.P \mid Q\,] \mid R\,] \mid \overline{\mathtt{out}}\,\alpha.S \;\rightarrow n[\,P \mid Q\,] \mid m[\,R\,] \mid S \quad \text{for } \alpha \in \{\star, n\}$$

Mobility Types: (extended: $\mathscr{C}$ tells which processes are allowed.)

$$M \quad ::= \quad \mathsf{mob}[\mathscr{S}, \mathscr{C}]$$

Subtyping Relation: (extended)

$$(\mathsf{sMob}) \quad \frac{\mathscr{G}_0 \subseteq \mathscr{G}_1, \quad \mathscr{C}_0 \subseteq \mathscr{C}_1}{\mathsf{mob}[\mathscr{G}_0, \mathscr{C}_0] \prec \mathsf{mob}[\mathscr{G}_1, \mathscr{C}_1]}$$

Good Values in BSA

(Val in)
$$\frac{\Gamma \vdash V{:}\mathrm{amb_i}[\mathtt{G}, M, \mathrm{com}[E, F]]}{\Gamma \vdash \mathtt{in}\, V{:}\mathrm{cap}[\mathtt{H}, \mathrm{mob}[\{G\}, \emptyset], E]}$$

(Val out)
$$\frac{\Gamma \vdash V{:}\mathrm{amb_o}[\mathtt{G}, \mathrm{mob}[\mathscr{S}, \mathscr{C}], \mathrm{com}[E, F]]}{\Gamma \vdash \mathtt{out}\, V{:}\mathrm{cap}[\mathtt{H}, \mathrm{mob}[\mathscr{S}, \emptyset], F]}$$

(Val coin)
$$\frac{\Gamma \vdash V{:}\mathrm{amb_i}[\mathtt{G}, M, \mathrm{com}[E, F]]}{\Gamma \vdash \overline{\mathtt{in}}\, V{:}\mathrm{cap}[\mathtt{H}, \mathrm{mob}[\emptyset, \{\mathtt{G}\}], F]}$$

(Val coout)
$$\frac{\Gamma \vdash V{:}\mathrm{amb_o}[\mathtt{G}, M, \mathrm{com}[E, F]]}{\Gamma \vdash \overline{\mathtt{out}}\, V{:}\mathrm{cap}[\mathtt{H}, \mathrm{mob}[\emptyset, \{\mathtt{G}\}], F]}$$

(Val coin $\star$)
$$\frac{\mathtt{G} \in \mathrm{dom}(\Gamma)}{\Gamma \vdash \overline{\mathtt{in}}\, \star{:}\mathrm{cap}[\mathtt{G}, \mathrm{mob}[\emptyset, \mathscr{U}], \mathrm{zero}]}$$

(Val coout $\star$)
$$\frac{\mathtt{G} \in \mathrm{dom}(\Gamma)}{\Gamma \vdash \overline{\mathtt{out}}\, \star{:}\mathrm{cap}[\mathtt{G}, \mathrm{mob}[\emptyset, \mathscr{U}], \mathrm{zero}]}$$

In (Val in), (Val out), (Val coin), (Val coin), assume $\mathtt{H} \in \Gamma$

Good Processes – Mobility in BSA

(Pro $\mathbf{0}$)

$$\frac{\mathtt{G} \in \mathsf{dom}(\Gamma)}{\Gamma \vdash \mathbf{0}{:}\mathsf{proc}[\mathtt{G}, \mathsf{mob}[\emptyset, \emptyset], \mathsf{com}[\mathsf{zero}, \mathsf{zero}]]}$$

(Pro pfx)

$$\frac{\Gamma \vdash V{:}\mathsf{cap}[\mathtt{G}, M, F]; \quad \Gamma \vdash P{:}\mathsf{proc}[\mathtt{G}, M, \mathsf{com}[E, F]]}{\Gamma \vdash V.P{:}\mathsf{proc}[\mathtt{G}, M, \mathsf{com}[E, F]]}$$

(Pro amb)

$$\frac{\begin{array}{l}\Gamma \vdash V{:}\mathsf{amb}_{\mathsf{c}}[\mathtt{H}, \mathsf{mob}[\mathscr{S}, \mathscr{C}], \mathsf{com}[E, F]] \\ \Gamma \vdash P{:}\mathsf{proc}[\mathtt{H}, \mathsf{mob}[\mathscr{S}, \mathscr{C}], \mathsf{com}[E, F]]\end{array}}{\Gamma \vdash V[\,P\,]{:}\mathsf{proc}[\mathtt{G}, \mathsf{mob}[\emptyset, \{\mathtt{H}\}], \mathsf{com}[F, \mathsf{zero}]]} \; \mathtt{G} \in \mathscr{S}$$

Control Properties in BSA

Access Control Theorem:

Whenever

$$\Gamma \vdash m[\,\overline{\mathtt{in}}\,\alpha.P \mid Q\,] : \Pi \quad \text{or} \quad \Gamma \vdash m[\,\overline{\mathtt{out}}\,\alpha.P \mid Q\,] : \Pi,$$

with $\alpha \in \{\star, n\}$, then

- $\Gamma \vdash m : \mathsf{amb}_{\chi_0}[\_, \mathsf{mob}[\_, \mathscr{C}], \_]$, and
  - either $\alpha = \star$ and $\mathscr{C} = \mathscr{U}$,
  - or $\alpha = n$ with $\Gamma \vdash n : \mathsf{amb}_{\chi_1}[\mathtt{N}, \_, \_]$ and $\mathtt{N} \in \mathscr{C}$.

Using co-capabilities to defend Troy

Our running example in BSA:

$$\mathit{The\ Trojan\ War} \triangleq \mathtt{Odysseus}[\,\mathtt{in}\,\mathtt{Horse}.\mathtt{out}\,\mathtt{Horse}.\mathit{Destroy}\,]$$
$$\mid \mathtt{Horse}[\,\overline{\mathtt{in}}\,\star.\mathtt{in}\,\mathtt{Troy}\,]$$
$$\mid \mathtt{Troy}[\,\overline{\mathtt{in}}\,\mathtt{Horse}.\mathit{Trojans} \mid \overline{\mathtt{out}}\,\mathtt{Odysseus}.\mathit{Sinon}\,]$$

which can be well-typed only if

$$\Gamma \vdash \mathtt{Troy} : \mathtt{amb}_{\mathtt{ioc}}[\mathtt{City}, \mathtt{mob}[\_, \{\mathtt{Toy}, \mathtt{Achaean}\}], \_]$$

That is if Troy (in suicidal mood) allowed Achaeans in.

Using co-capabilities to defend Troy (ctd)

Consider now the system:

$$\mathit{The\ Trojan\ Trap} \triangleq \mathrm{Odysseus}[\,\mathtt{in}\,\mathrm{Horse}.\mathtt{out}\,\mathrm{Horse}.\mathit{Destroy}\,]$$
$$\mid \mathrm{Horse}[\,\overline{\mathtt{in}}\,\star.\mathtt{in}\,\mathrm{Troy}\,]$$
$$\mid \mathrm{Troy}[\,\overline{\mathtt{in}}\,\mathrm{Horse}.\mathit{Trojans}\,]$$

This situation would be perfectly safe for Troy (but dangerous for Odysseus!) provided we can type it under the assumptions of the form

$$\mathrm{Odysseus} : \mathrm{amb}_{\mathtt{c}}[\mathtt{Achaean}, \_, \_]$$
$$\mathrm{Horse} : \mathrm{amb}_{\mathtt{ioc}}[\mathtt{Toy}, \_, \mathrm{com}[E, \mathbf{0}]]$$
$$\mathrm{Troy} : \mathrm{amb}_{\mathtt{ioc}}[\mathtt{City}, \mathrm{mob}[\emptyset, \mathscr{C}], \_]$$

with $\mathtt{Achaean} \notin \mathscr{C}$.