Types for Role-based Access Control of Dynamic Web Data

Mariangiola Dezani-Ciancaglini [1] Silvia Ghilezan[2]
Svetlana Jakšić [2] Jovanka Pantović[2]

[1]Università di Torino

[2]University of Novi Sad

SVARM 2010, Edinburgh

Outline

Outline

Distributed systems - decentralised peer-to-peer networks

- management of semi-structured and distributed data
- processes with different roles have different access rights
- different access policies in different locations
- exchange between data and processes preserving access control
- dynamic changes of access rights

- One solution - typed models
  - control of access
  - control of movements rights

Distributed systems - decentralised peer-to-peer networks

- management of semi-structured and distributed data
- processes with different roles have different access rights
- different access policies in different locations
- exchange between data and processes preserving access control
- dynamic changes of access rights

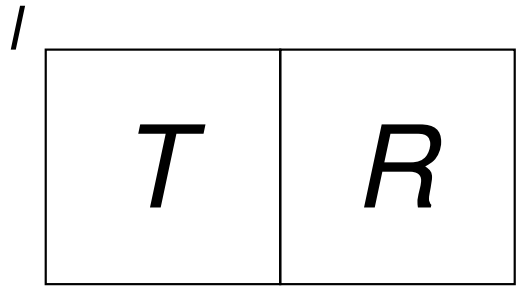
- One solution - typed models
  - control of access
  - control of movements rights

Related work

- X$d\pi$ calculus - extension of Active XML - Gardner, Maffeis
  - localised mobile processes
  - distributed, dynamic, semi-structured web data
- Variety of type systems for $d\pi$ and related calculi
  - controlling the use of accesses and mobility of processes
- Security types for X$d\pi$
  Dezani, Ghilezan, Pantovic, Varacca, 2008
  - partially ordered set (with bottom) as security levels
  - control of movements rights
  - network invariant and initial network

Distributed Network

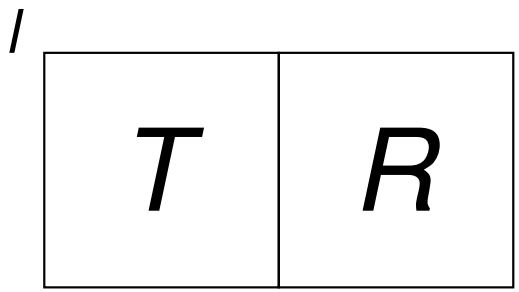
Location

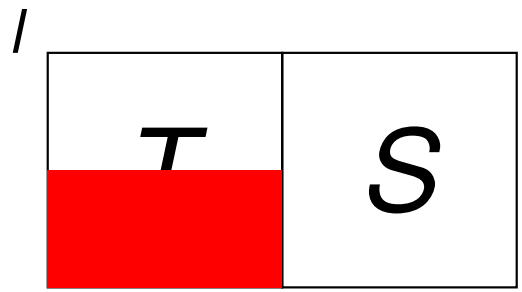


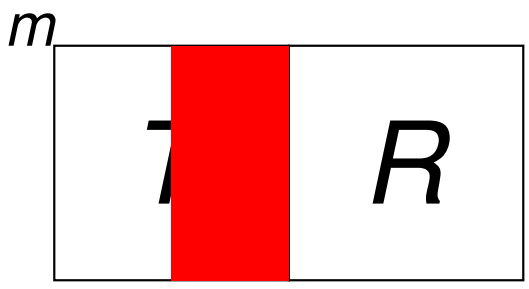
Location

A peer or a location is represented with data and a process.

Access Rights







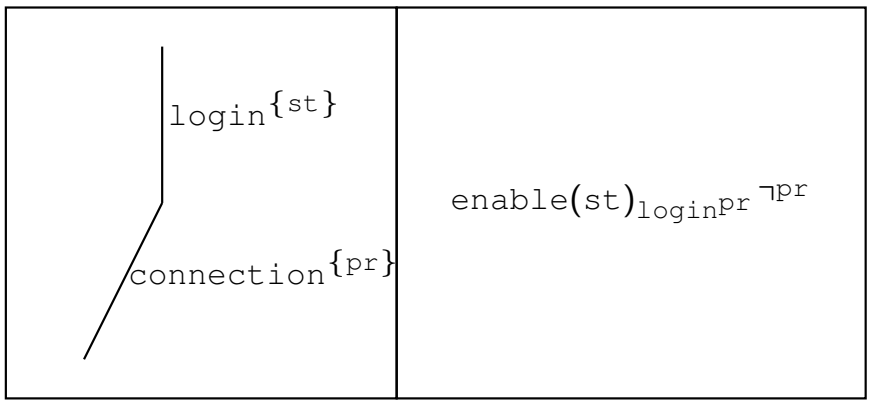
Security conditions

- not all data is visible to all processes
- different locations with different access policies

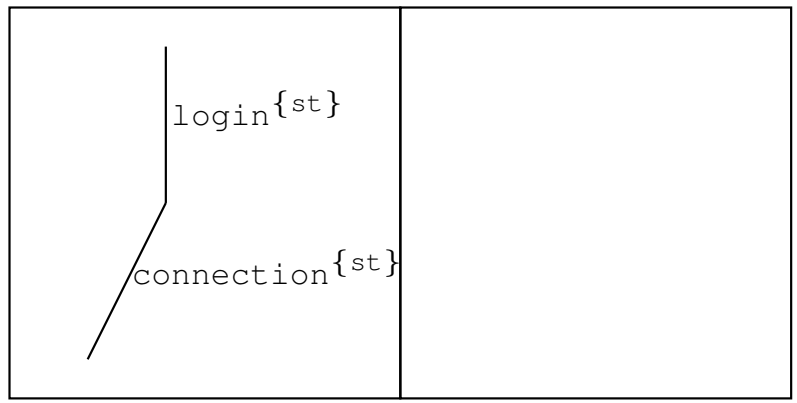
Roles

$$st \sqsubseteq pr$$

CLASSROOM



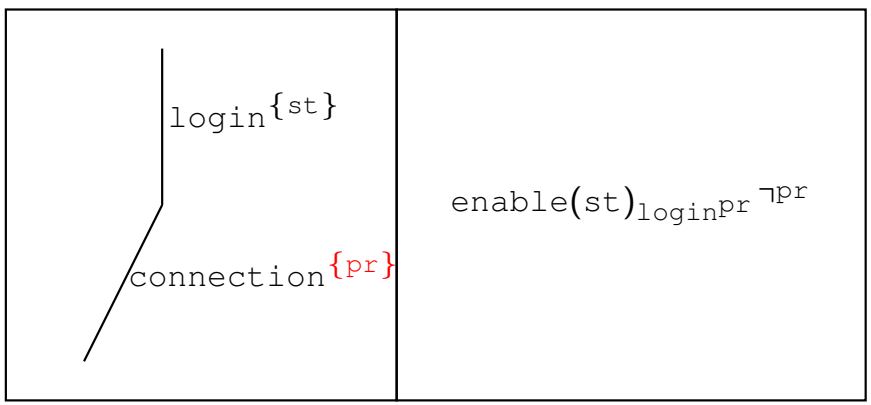
PUBLIC



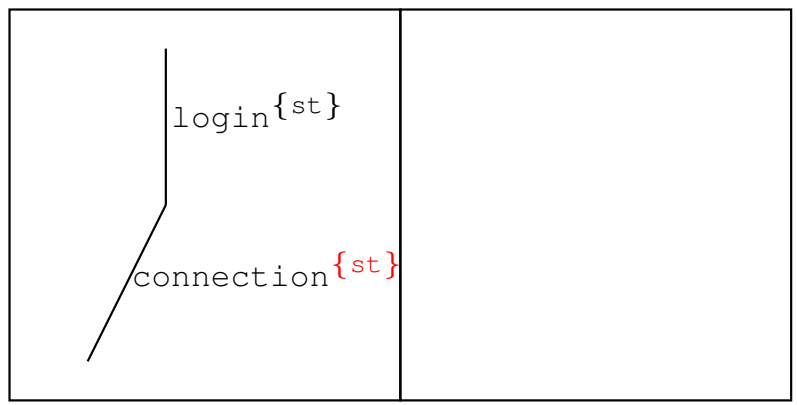
Roles

$$st \sqsubseteq pr$$

CLASSROOM



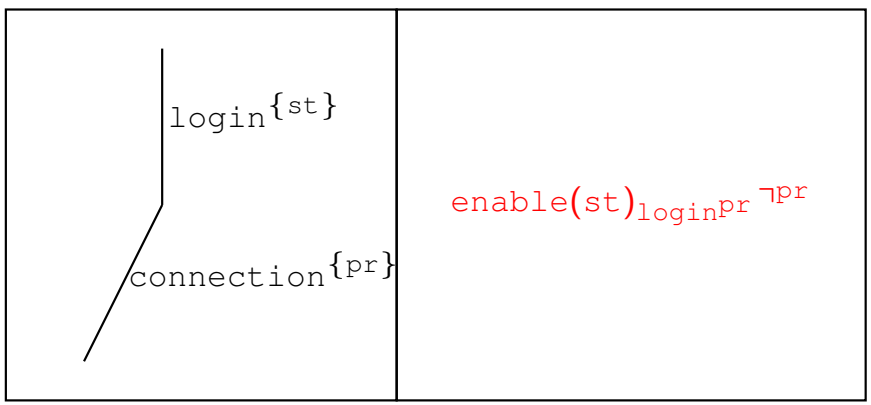
PUBLIC



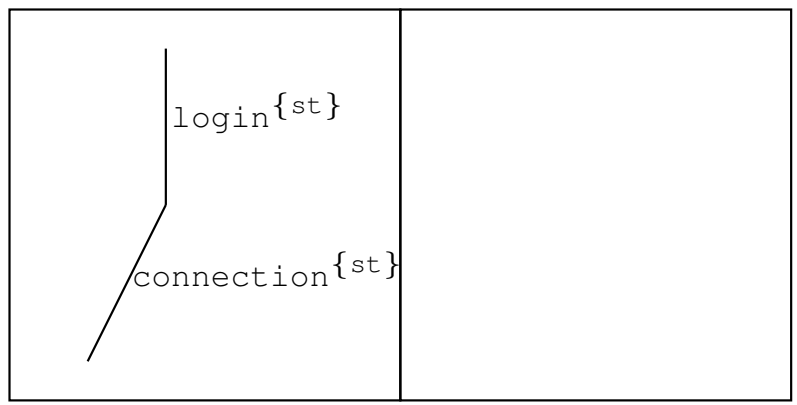
Roles

$$st \sqsubseteq pr$$

CLASSROOM

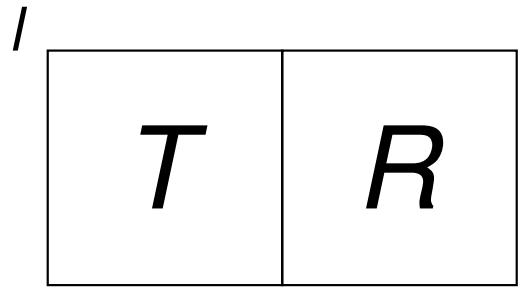


PUBLIC



Outline

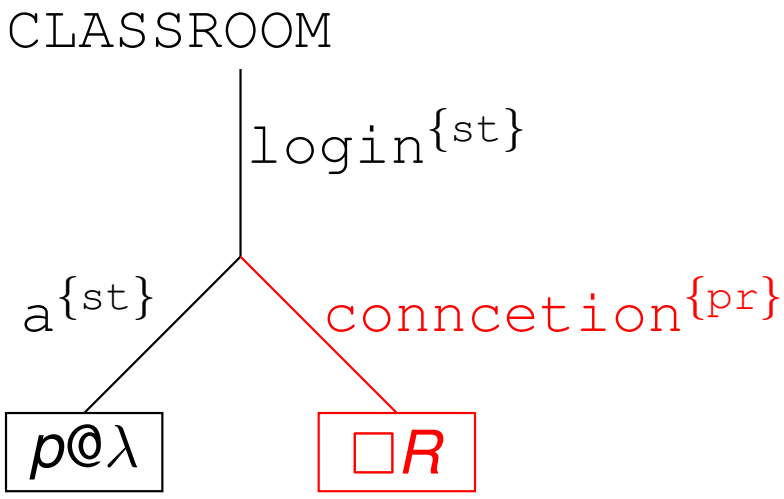
Locations, Networks

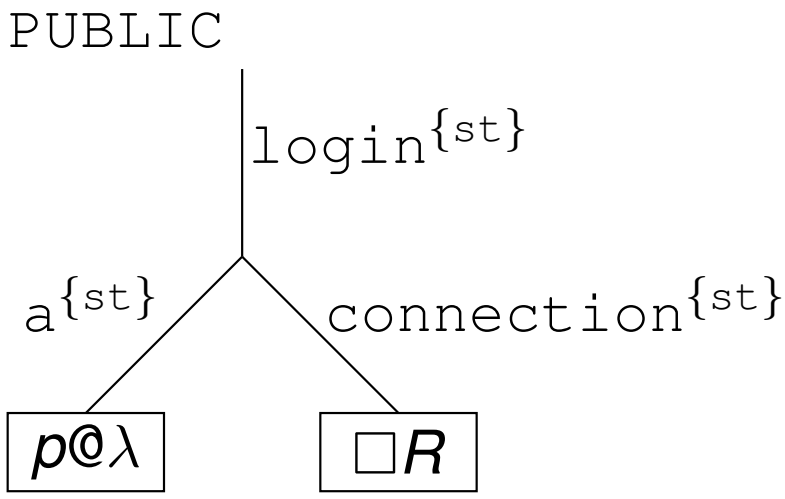


- Each location consists of data in a form of a tree and a process
- A well-formed network is a parallel composition (|) of *locations* with different names.

$$\mathbf{N} ::= \mathbf{0} \mid \mathbf{N} \mid \mathbf{N} \mid l[T \parallel R] \mid (\nu c^{Tv})\mathbf{N}$$

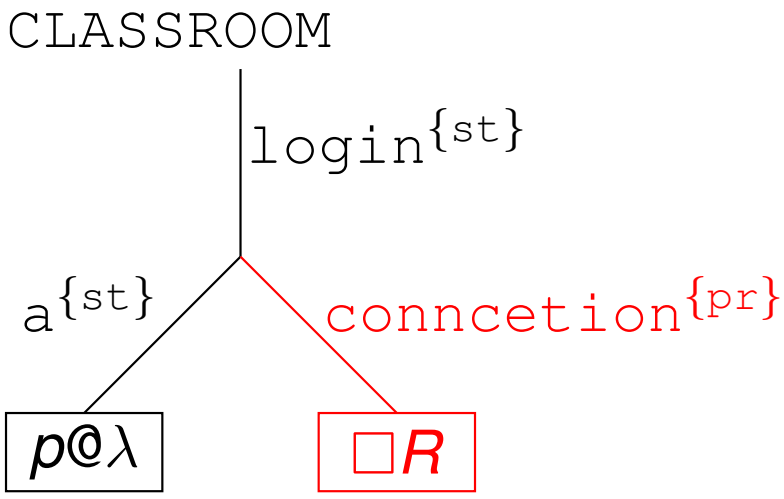
Data

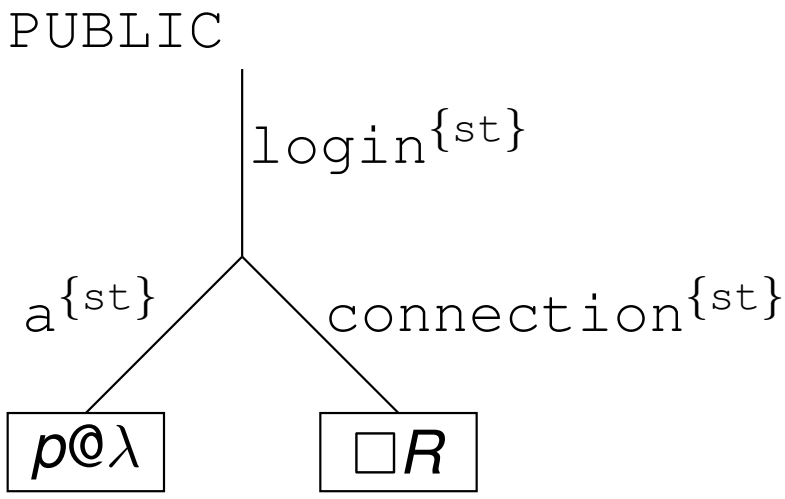




- □*R*-scripted process
- *p*-path
- *p*@λ-pointer
- run, read, change
- dynamic changes of access rights

Data





- $\square R$-scripted process
- p-path
- $p@\lambda$-pointer
- `run`, `read`, `change`
- dynamic changes of access rights

Processes

π-calculus

P	$::=$	0	the nil process
	$\mid$	$P \mid P$	composition of processes
	$\mid$	$\bar{c}^{Tv}\langle v \rangle$	output value v on a channel c
	$\mid$	$c^{Tv}(x).P$	input parameterized by a variable x
	$\mid$	$!c^{Tv}(x).P$	replication of an input process

Processes

π-calculus

P	$::=$	0	the nil process
	$\mid$	$P \mid P$	composition of processes
	$\mid$	$\bar{c}^{Tv}\langle v \rangle$	output value v on a channel c
	$\mid$	$c^{Tv}(x).P$	input parameterized by a variable x
	$\mid$	$!c^{Tv}(x).P$	replication of an input process

$d\pi$-calculus

P	$::=$	$\texttt{go}\ \lambda.R$	migrate to location λ, continue as R

X$d\pi$-calculus

P	$::=$	$\texttt{run}_p$	run command
	$\mid$	$\texttt{read}_p(\chi).P$	read command
	$\mid$	$\texttt{change}_p(\chi, V).P$	change command

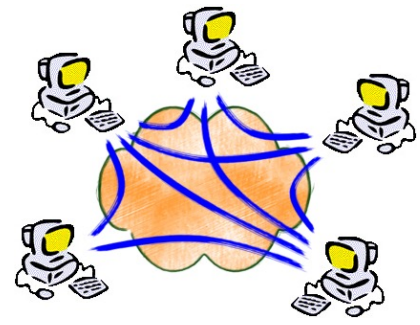
Processes

®X$d\pi$-calculus

P	$::=$	$\texttt{enable}(r)_p.P$	gives permission to the role r to access data on the path p
	$\mid$	$\texttt{disable}(r)_p.P$	removes the role $r$from roles that are allowed to access data on the path p
R	$::=$	$P^{\urcorner\rho}$	single process with roles ρ
	$\mid$	$R \mid R$	parallel composition of processes with roles
	$\mid$	$(\nu c^{Tv})R$	restriction of channel name c

Interactions in the System

- Communication
- Movement
- Interaction with local data
- Permission change



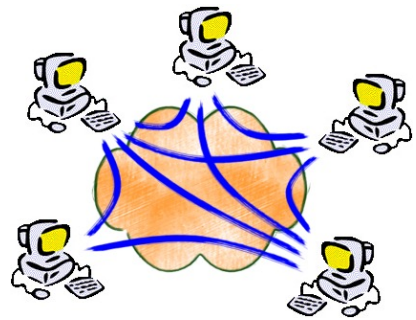
Reduction rules formally describe interactions in the system.

Interactions in the System

- Communication

l

T	$P \urcorner \rho$ $Q \urcorner \sigma$

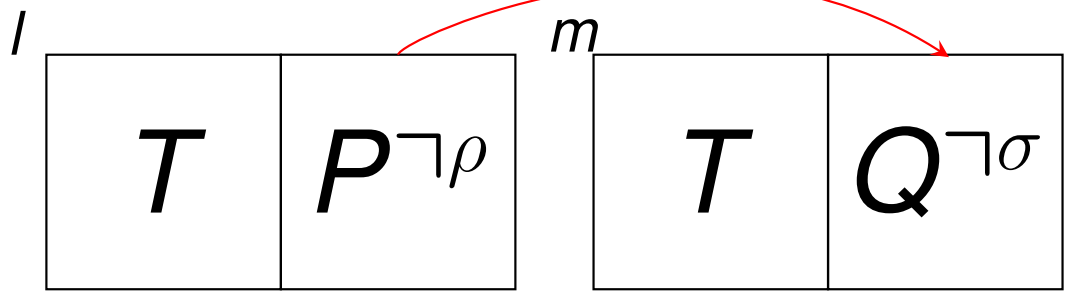


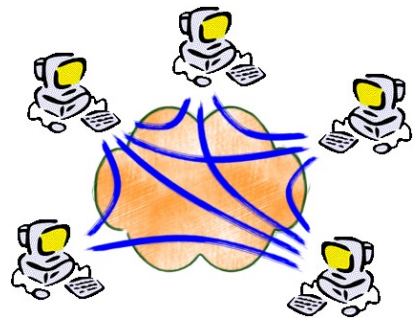
- Movement
- Interaction with local data
- Permission change

Reduction rules formally describe interactions in the system.

Interactions in the System

- Communication
- Movement



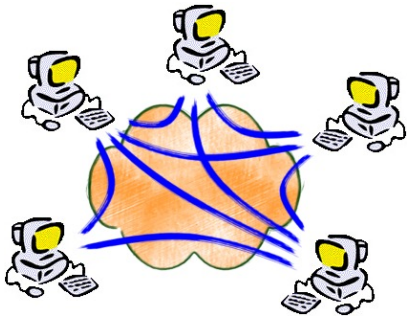


- Interaction with local data
- Permission change

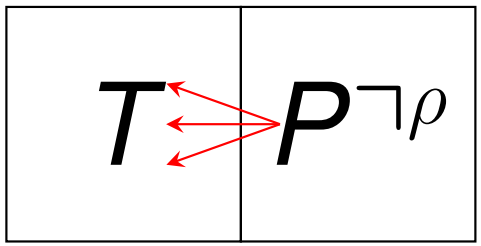
Reduction rules formally describe interactions in the system.

Interactions in the System

- Communication
- Movement
- Interaction with local data



l

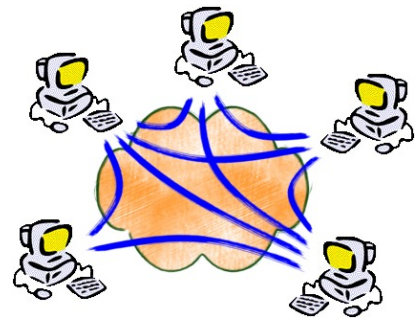


- Permission change

Reduction rules formally describe interactions in the system.

Interactions in the System

- Communication
- Movement
- Interaction with local data
- Permission change

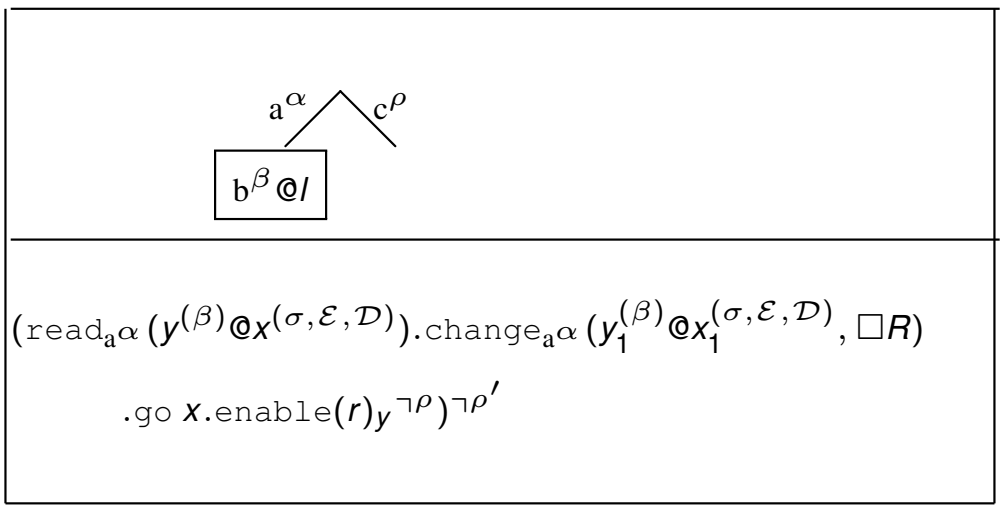


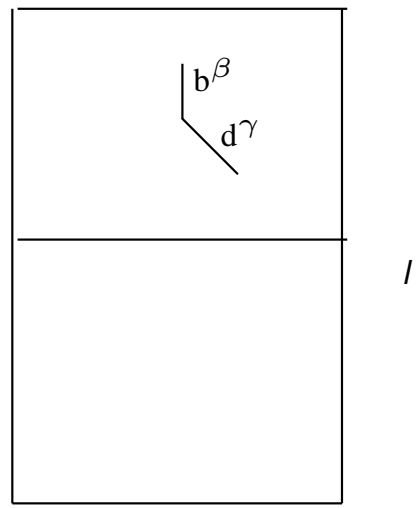
l

T	$P^{\neg\rho}$

Reduction rules formally describe interactions in the system.

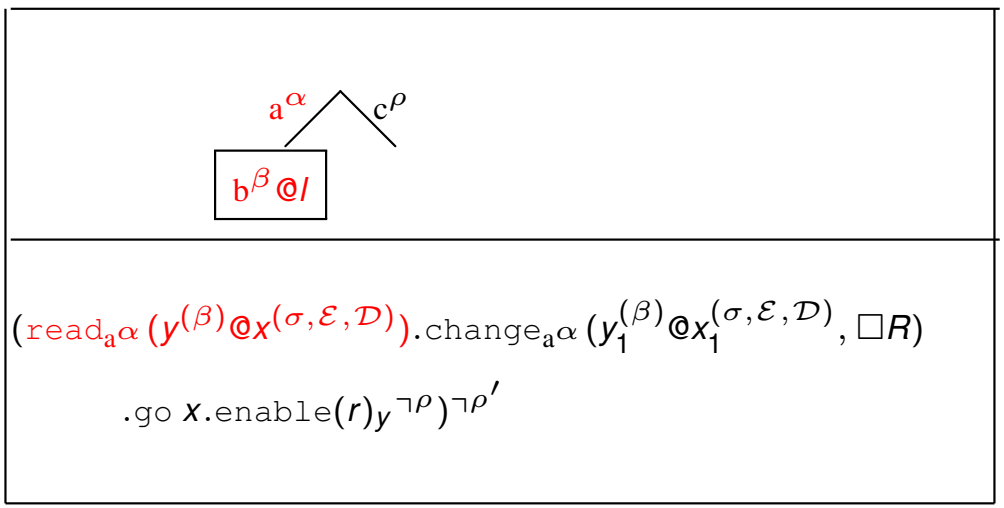
Operational Semantics - Example

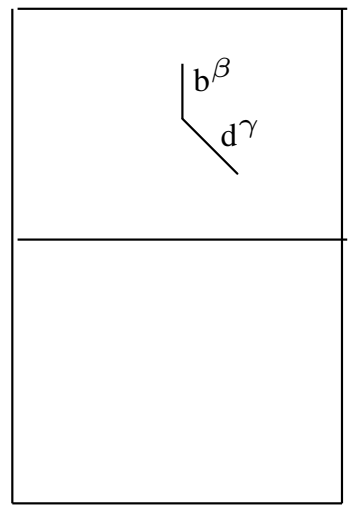




l

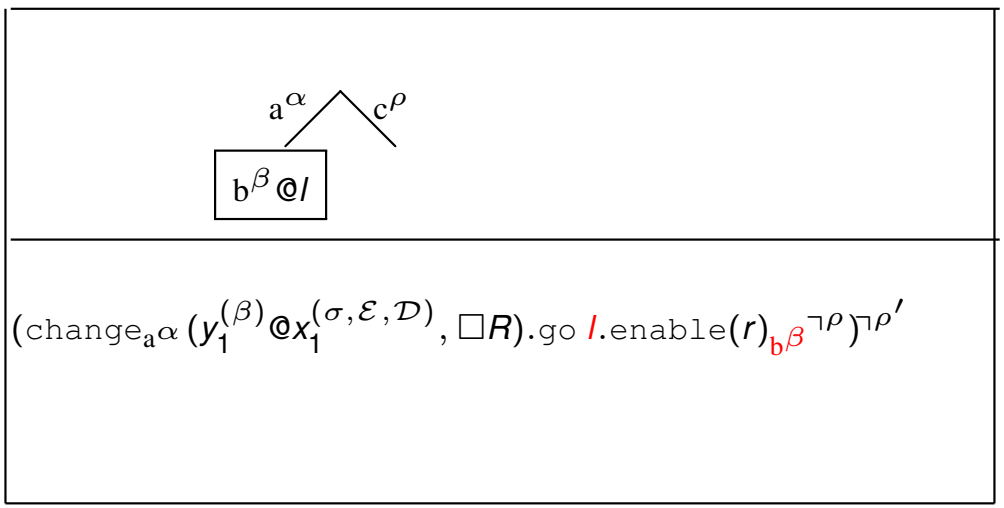
Operational Semantics - Example

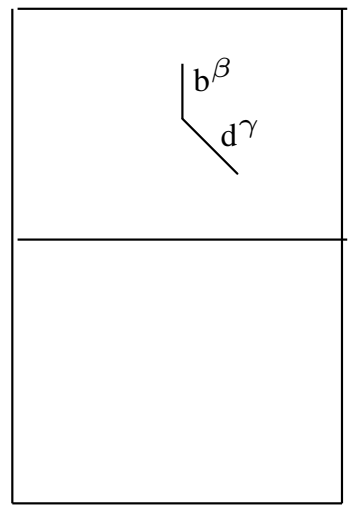




l

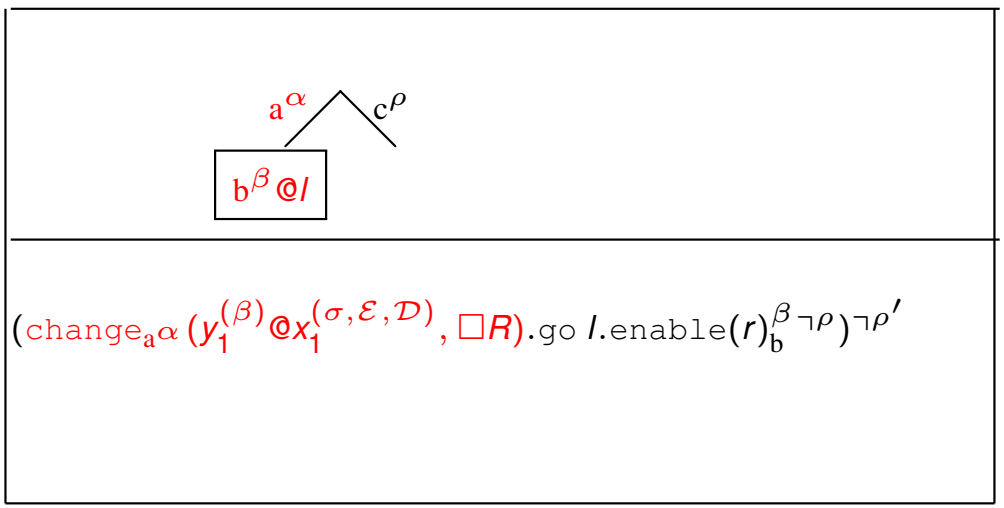
Operational Semantics - Example

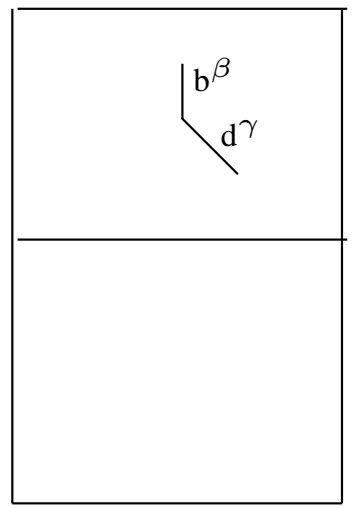




l

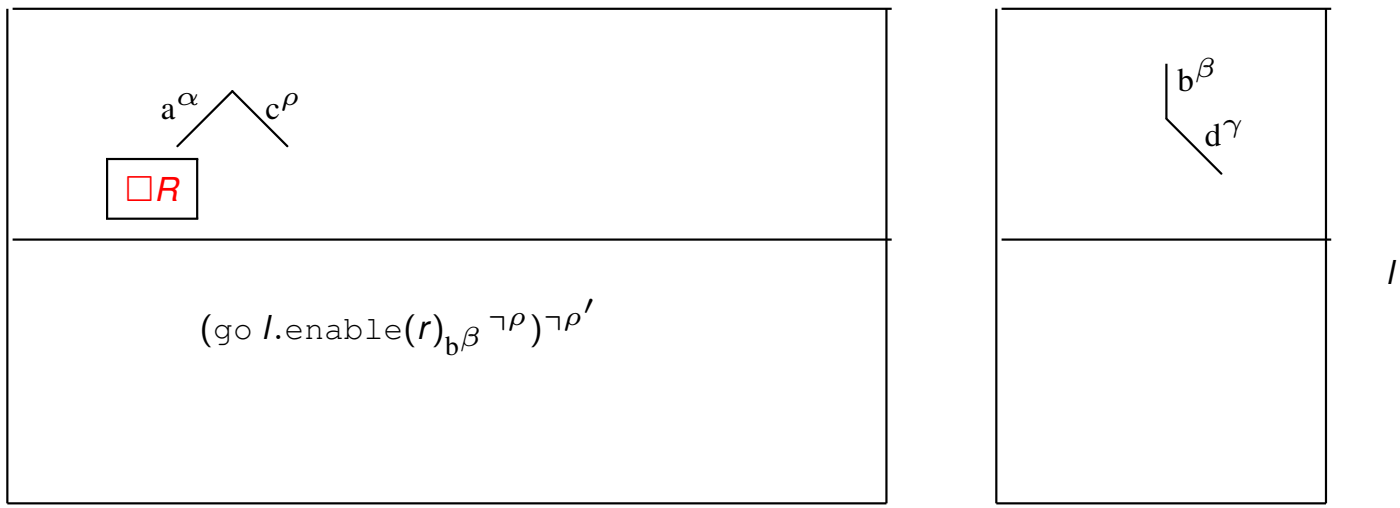
Operational Semantics - Example



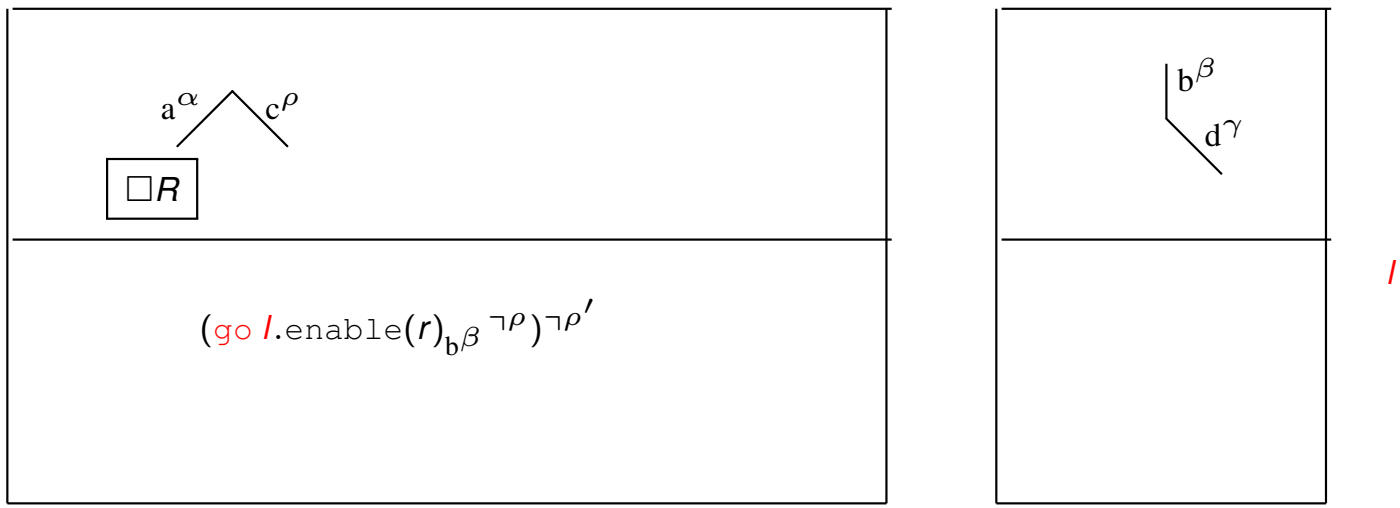


l

Operational Semantics - Example



Operational Semantics - Example



Operational Semantics - Example

Operational Semantics - Example

Operational Semantics - Example

Outline

Type System

Main goals

- to control communication of values
- to control migration and activation of processes
- to control access to data and their modification

Location Policy

$$(\sigma, \mathcal{E}, \mathcal{D})$$

- σ: set of minimal roles which can access data
- $\mathcal{E}$: policy for role enabling
- $\mathcal{D}$: policy for role disabling

Type System

Main goals

- to control communication of values
- to control migration and activation of processes
- to control access to data and their modification

Location Policy

$$(\sigma, \mathcal{E}, \mathcal{D})$$

- σ: set of minimal roles which can access data
- $\mathcal{E}$: policy for role enabling
- $\mathcal{D}$: policy for role disabling

Type System - Example

$\mathtt{st} \sqsubseteq \mathtt{st}_{\mathtt{i}} \sqsubseteq \mathtt{as} \sqsubseteq \mathtt{prof} \sqsubseteq \mathtt{dean}$ where $\mathtt{i} \in I$.

Type System - Example

$\texttt{st} \sqsubseteq \texttt{st}_\texttt{i} \sqsubseteq \texttt{as} \sqsubseteq \texttt{prof} \sqsubseteq \texttt{dean}$ where $\texttt{i} \in I$.

$$\texttt{FACULTY} : (\sigma_\texttt{F}, \mathcal{E}_\texttt{F}, \mathcal{D}_\texttt{F})$$

$$\sigma_\texttt{F} = \{\texttt{st}_\texttt{i}\} \quad \mathcal{E}_\texttt{F} = (\{\texttt{prof}\}, \texttt{as}) \quad \mathcal{D}_\texttt{C} = (\{\texttt{dean}\}, \texttt{st}_\texttt{i})$$

FACULTY

Type System - Example

$\mathtt{st} \sqsubseteq \mathtt{st}_i \sqsubseteq \mathtt{as} \sqsubseteq \mathtt{prof} \sqsubseteq \mathtt{dean}$ where $\mathtt{i} \in I$.

$$\mathtt{FACULTY} : (\sigma_F, \mathcal{E}_F, \mathcal{D}_F)$$

$$\sigma_F = \{\mathtt{st}_i\} \quad \mathcal{E}_F = (\{\mathtt{prof}\}, \mathtt{as}) \quad \mathcal{D}_C = (\{\mathtt{dean}\}, \mathtt{st}_i)$$

FACULTY

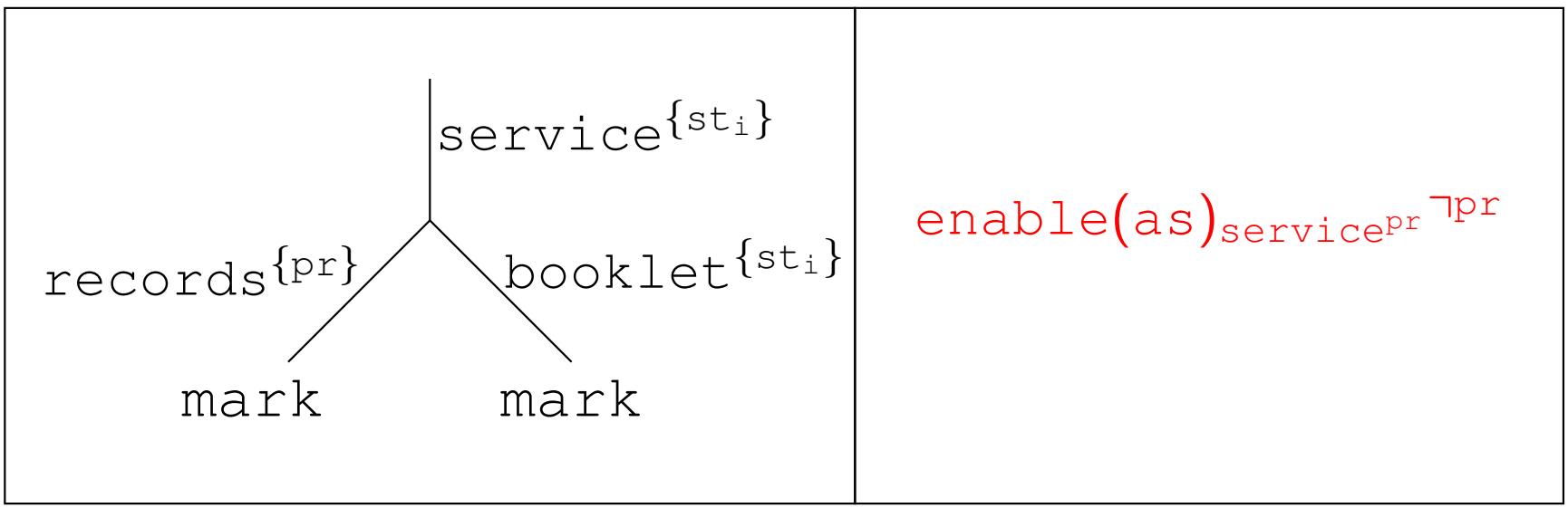
Type System - Example

$\mathtt{st} \sqsubseteq \mathtt{st_i} \sqsubseteq \mathtt{as} \sqsubseteq \mathtt{prof} \sqsubseteq \mathtt{dean}$ where $\mathtt{i} \in I$.

$$\mathtt{FACULTY} : (\sigma_{\mathtt{F}}, \mathcal{E}_{\mathtt{F}}, \mathcal{D}_{\mathtt{F}})$$

$$\sigma_{\mathtt{F}} = \{\mathtt{st_i}\} \quad \mathcal{E}_{\mathtt{F}} = (\{\mathtt{prof}\}, \mathtt{as}) \quad \mathcal{D}_{\mathtt{C}} = (\{\mathtt{dean}\}, \mathtt{st_i})$$

FACULTY



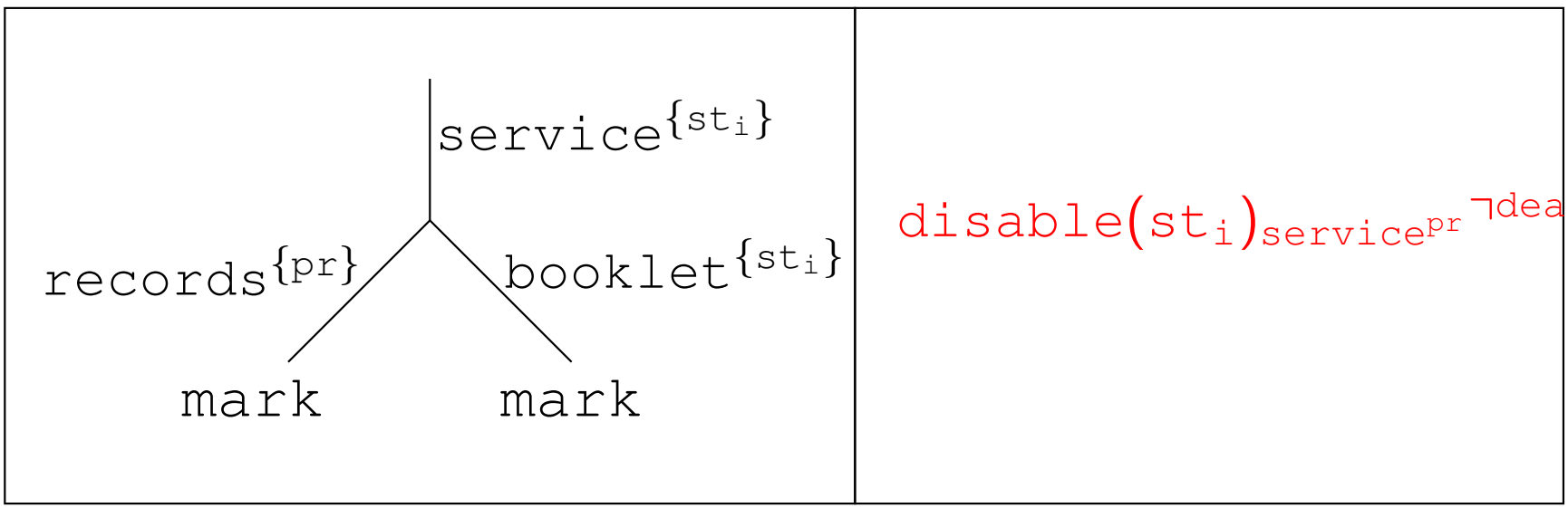
Type System - Example

$\mathtt{st} \sqsubseteq \mathtt{st}_i \sqsubseteq \mathtt{as} \sqsubseteq \mathtt{prof} \sqsubseteq \mathtt{dean}$ where $\mathtt{i} \in I$.

$$\mathtt{FACULTY} : (\sigma_F, \mathcal{E}_F, \mathcal{D}_F)$$

$$\sigma_F = \{\mathtt{st}_i\} \quad \mathcal{E}_F = (\{\mathtt{prof}\}, \mathtt{as}) \quad \mathcal{D}_C = (\{\mathtt{dean}\}, \mathtt{st}_i)$$

FACULTY



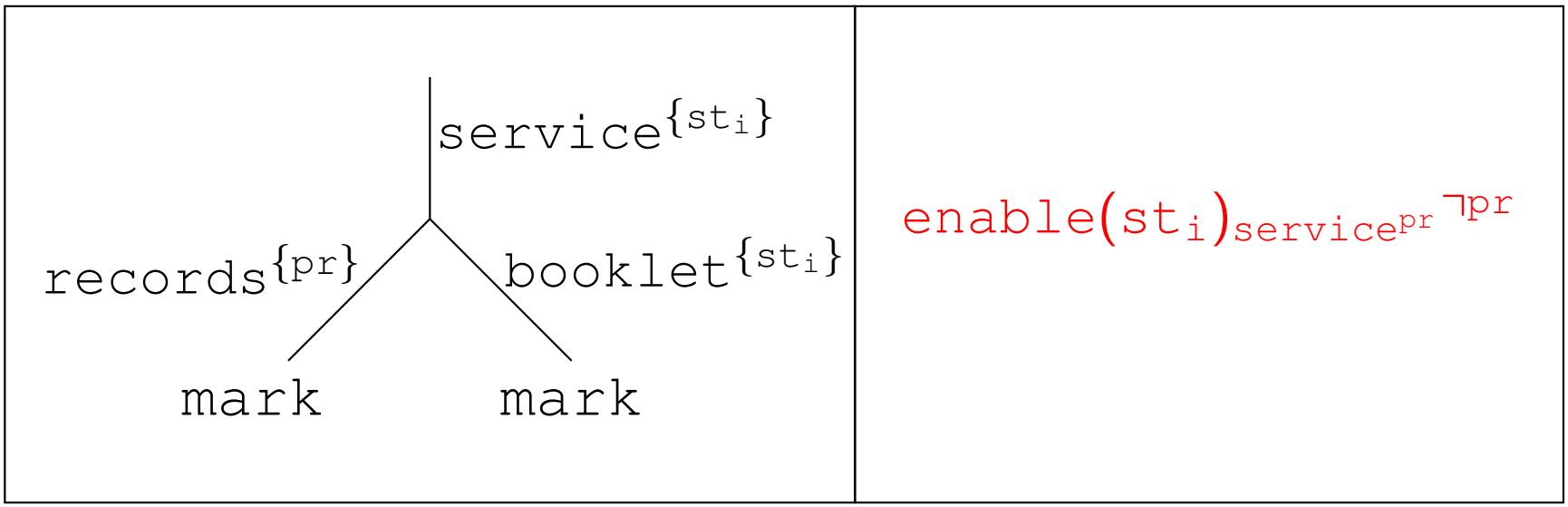
Type System - Example

$\mathtt{st} \sqsubseteq \mathtt{st}_i \sqsubseteq \mathtt{as} \sqsubseteq \mathtt{prof} \sqsubseteq \mathtt{dean}$ where $\mathtt{i} \in I$.

$$\mathtt{FACULTY} : (\sigma_F, \mathcal{E}_F, \mathcal{D}_F)$$

$$\sigma_F = \{\mathtt{st}_i\} \quad \mathcal{E}_F = (\{\mathtt{prof}\}, \mathtt{as}) \quad \mathcal{D}_C = (\{\mathtt{dean}\}, \mathtt{st}_i)$$

FACULTY



Safety properties

- (Subject reduction) If $\vdash \mathbf{N} : \mathit{Net}$ and $\mathbf{N} \rightarrow \mathbf{N}'$, then $\vdash \mathbf{N}' : \mathit{Net}$.

- Properties of location policies and communication:
  - **P0** All trees and processes in a location agree with the location policy;
  - **P1** A process with roles can communicate only values with characteristic roles accessible to the process.
- Properties of migration between locations:
  - **P2** A process with roles can migrate to another location only if it is well typed for that location.
- Properties of access of processes to local data trees:
  - **P3** A process with roles looks for a path in the local tree only if the path is accessible to the process.

Safety properties

- Properties of manipulation of local data trees by processes:
  - **P4** A script is activated in a location only if the corresponding process with roles can stay in that location;
  - **P5** A process with roles generated by a read command in a location can stay in that location;
  - **P6** A process with roles can erase a subtree of data only if it can access all data;
  - **P7** A tree built by a change command in a location can stay in that location;
  - **P8** A process with roles can add a role to an edge in the local tree only if this is allowed by the location policy;
  - **P9** A tree built by an enable command in a location can stay in that location;
  - **P10** A process with roles can erase a role from an edge in the local tree only if this is allowed by the location policy;
  - **P11** A tree built by a disable command in a location can stay in that location.

RDP 2011

Announcement

May 29 to June 3, 2011
Novi Sad, Serbia
http://www.rdp2011.uns.ac.rs/