

# Input/Output Types for Dynamic Web Data

Svetlana Jakšić

University of Novi Sad

ICTCS 2012, Varese

# Outline

## 1 Motivation

Access control in a distributed system with XML data  
Related Work

## 2 $\text{R}\lambda d\pi$ -calculus

Syntax  
Semantics

## 3 Types

Types  
Subtyping  
Safety

# Outline

## 1 Motivation

Access control in a distributed system with XML data  
Related Work

## 2 $\lambda$ -calculus

Syntax  
Semantics

## 3 Types

Types  
Subtyping  
Safety

# Distributed systems - decentralised peer-to-peer networks

- management of semi-structured and distributed data (XML)
  - different processes 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 (XML)
- different processes 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

- $Xd\pi$  calculus - extension of Active XML - Gardner, Maffeis
  - localised mobile processes
  - distributed, dynamic, semi-structured web data



Philippa Gardner and Sergio Maffeis.

Modelling dynamic web data.

*Theoretical Computer Science*, 342(1):104–131, 2005.

- $Xd\pi$  calculus - features
  - location and processes of  $d\pi$  - Hennessy, Riely
  - capabilities for data migration - Abiteboul et al.; Cardelli, Ghelli

## Related work

- Variety of type systems for  $d\pi$  and related calculi
  - controlling the use of accesses and mobility of processes
- Security types for  $Xd\pi$   
Dezani, Ghilezan, Pantović, Varacca, 2008
  - partially ordered set (with bottom) as security levels
  - control of movements rights
  - network invariant and initial network





Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, and Jovanka Pantovic.  
Security types for dynamic web data.  
*TGC*, volume 4661 of *Lecture Notes in Computer Science*, pages 263–280.  
Springer, 2006.



Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, Jovanka Pantovic, and  
Daniele Varacca.  
Security types for dynamic web data.  
*Theor. Comput. Sci.*, 402(2-3):156–171, 2008.

## Related work

- Security types for  $\textcircled{R}Xd\pi$ -calculus  
Dezani, Ghilezan, Jakšić, Pantović, 2011
  - partially ordered set of roles, RBAC
  - communication, movement and data usage control
-  Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, Svetlana Jakšić, and Jovanka Pantović.  
Types for Role-Based Access Control of Dynamic Web Data.  
In *WFLP'10*, volume 6559 of *LNCS*, pages 1–29. Springer, 2011.
-  Silvia Ghilezan, Svetlana Jakšić, Jovanka Pantović, and Mariangiola Dezani-Ciancaglini.  
Types and Roles for Web Security.  
*Transactions on Advanced Research*, 8(2):16–21, 2012.



# Outline

## 1 Motivation

Access control in a distributed system with XML data  
Related Work

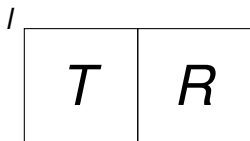
## 2 $\text{R}\lambda d\pi$ -calculus

Syntax  
Semantics

## 3 Types

Types  
Subtyping  
Safety


## Locations and networks



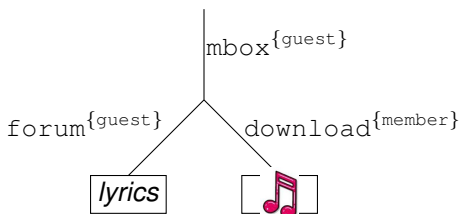
- Each **location** consists of data in a form of a tree and a process
- A well-formed **network** is a parallel composition (  $|$  ) of *locations* with different names.

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

# Data

```
< mbox role = guest >  
  < forum role = guest >  
    lyrics  
  < /forum >  
  < download role = member >  
      
  < /download >  
< /mbox >
```

- $R$ -scripted process
- $p@λ$ -pointer



# Processes

## $\pi$ -calculus

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

# Processes

## $\pi$ -calculus

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

## $d\pi$ -calculus

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

# Processes

## $\pi$ -calculus

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

## $d\pi$ -calculus

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

## $Xd\pi$ -calculus

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

# Processes

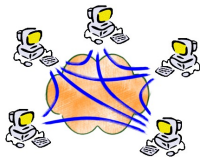
## Ⓜ $\lambda d\pi$ -calculus

- $P ::= \text{enable}(r)_\rho.P$  gives permission to the role  $r$   
to access data on the path  $\rho$
- |  $\text{disable}(r)_\rho.P$  removes the role  $r$  from roles that are  
allowed to access data on the path  $\rho$
- $R ::= P^\top \rho$  single process with roles  $\rho$
- |  $R|R$  parallel composition of processes with roles
- |  $(\nu c^{T\nu})R$  restriction of channel name  $c$

# Operational semantics

## Interactions in the system

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



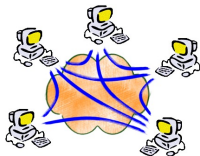
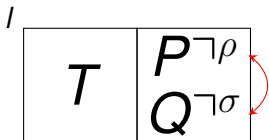
Reduction rules formally describe interactions in the system.



# Operational semantics

## Interactions in the system

- Communication



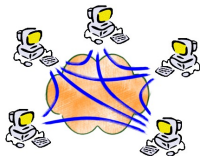
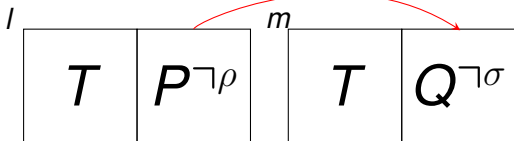
- Movement
- Interaction with local data
- Permission change

Reduction rules formally describe interactions in the system.

# Operational semantics

Interactions in the system

- Communication
- Movement



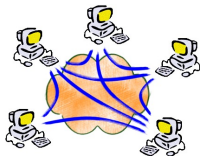
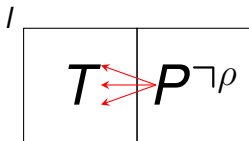
- Interaction with local data
- Permission change

Reduction rules formally describe interactions in the system.

# Operational semantics

## Interactions in the system

- Communication
- Movement
- Interaction with local data



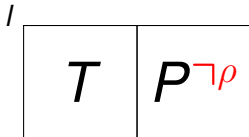
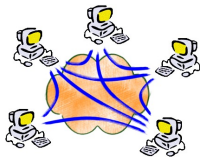
- Permission change

Reduction rules formally describe interactions in the system.

# Operational semantics

## Interactions in the system

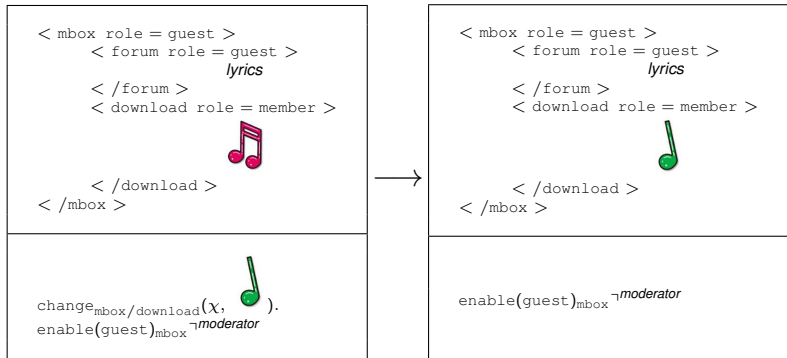
- Communication
- Movement
- Interaction with local data
- Permission change



Reduction rules formally describe interactions in the system.

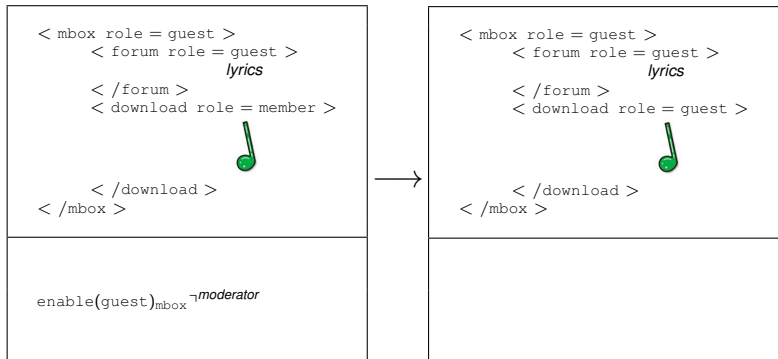
# Operational semantics

## Example



# Operational semantics

## Example



# Outline

## 1 Motivation

Access control in a distributed system with XML data  
Related Work

## 2 $\text{R}\lambda d\pi$ -calculus

Syntax  
Semantics

## 3 Types

Types  
Subtyping  
Safety

# 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

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

- $\sigma$ : 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

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

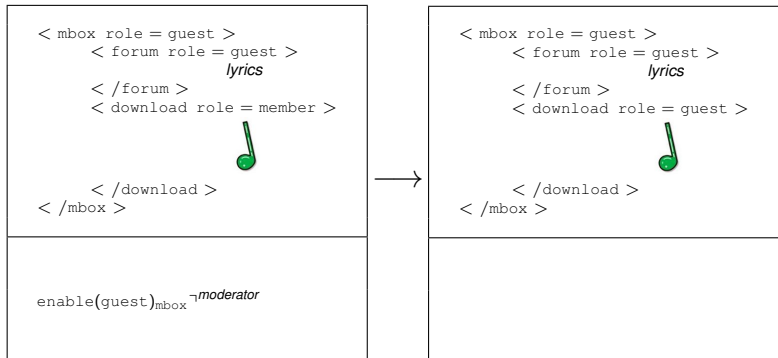
- $\sigma$ : set of minimal roles which can access data
- $\mathcal{E}$ : policy for role enabling
- $\mathcal{D}$ : policy for role disabling

# Music Box

## Policy

Roles:  $\text{guest} \sqsubseteq \text{member} \sqsubseteq \text{moderator}$

Policy:  $((\text{guest}), \{(\text{moderator}), \text{guest}\}), \{(\text{moderator}), \text{member}\})$



# Syntax of $\textcircled{R}Xd\pi$ types

$Ch(Tv)$	type of channels communicating values of type $Tv$
$Ch^!(Tv)$	type of channels emitting values of type $Tv$
$Ch^?(Tv)$	type of channels receiving values of type $Tv$
$Loc(\mathcal{P})$	type of locations with the policy $\mathcal{P}$
$Script(\mathcal{P})$	type of scripts which can be activated at locations with the policy $\mathcal{P}$
$Path(\alpha)$	type of paths having the last edge with the set of roles $\alpha$
$Pointer(\alpha)$	type of pointers whose path is typed by $Path(\alpha)$
$Tree(\mathcal{P}, \tau, \zeta)$	type of trees, which can stay at locations with the policy $\mathcal{P}$ , with initial branches asking $\tau$ and which can be completely accessed by processes with at least one role of $\zeta$
$Proc(\mathcal{P}, \rho)$	type of pure processes, which can stay at locations with the policy $\mathcal{P}$ and which can be assigned roles $\rho$
$ProcRole(\mathcal{P})$	type of processes with roles which can stay at locations with the policy $\mathcal{P}$

## Typing rules

$$\Gamma \vdash p : \text{Path}(\alpha) \quad \Gamma \vdash P : \text{Proc}(\mathcal{P}, \rho) \quad \alpha \leq \rho$$
$$\Gamma \cup \Gamma_\chi \vdash \begin{cases} V : \text{Script}(\mathcal{P}) \text{ or} \\ V : \text{Pointer}(\beta) \text{ or} \\ V : \text{Tree}(\mathcal{P}, \tau', \zeta') \quad \alpha \leq \tau' \end{cases} \quad (\text{Change})$$

if  $\chi = x^{(\mathcal{P}, \tau, \zeta)}$  then  $\zeta \leq \rho$

---

$$\Gamma \vdash \text{change}_\rho(\chi, V).P : \text{Proc}(\mathcal{P}, \rho)$$
$$\frac{\vdash I : \text{Loc}(\mathcal{P}) \quad \vdash T : \text{Tree}(\mathcal{P}, \tau, \zeta) \quad \vdash R : \text{ProcRole}(\mathcal{P})}{\vdash I \llbracket T \parallel R \rrbracket : \text{Net}} \quad (\text{NetLoc})$$

# Subtyping relation

## Channels

$$Ch(Tv) \prec Ch^!(Tv)$$

$$Ch(Tv) \prec Ch^?(Tv)$$

$$\frac{Tv_1 \prec Tv_2}{Ch^?(Tv_1) \prec Ch^?(Tv_2)}$$

$$\frac{Tv_1 \prec Tv_2}{Ch^!(Tv_2) \prec Ch^!(Tv_1)}$$

$$\frac{Tv_1 \prec Tv_2 \quad Tv_2 \prec Tv_1}{Ch(Tv_1) \prec Ch(Tv_2)}$$

# Subtyping relation

Data

$$\frac{\mathcal{P}_1 = (\sigma_1, \mathcal{E}_1, \mathcal{D}_1) \quad \mathcal{P}_2 = (\sigma_2, \mathcal{E}_2, \mathcal{D}_2) \quad \text{Loc}(\mathcal{P}_1) \prec \text{Loc}(\mathcal{P}_2)}{\text{Script}(\mathcal{P}_1) \prec \text{Script}(\mathcal{P}_2)}$$

$$\frac{\alpha_1 \preceq \alpha_2}{\text{Path}(\alpha_1) \prec \text{Path}(\alpha_2)}$$

$$\frac{\tau_1 \preceq \tau_2 \quad \zeta_1 \preceq \zeta_2}{\text{Tree}(\mathcal{P}, \tau_2, \zeta_2) \prec \text{Tree}(\mathcal{P}, \tau_1, \zeta_1)}$$

# Subtyping relation

Location

$$\frac{\mathcal{P}_1 = (\sigma_1, \mathcal{E}_1, \mathcal{D}_1) \quad \mathcal{P}_2 = (\sigma_2, \mathcal{E}_2, \mathcal{D}_2) \quad \sigma_2 \leq \sigma_1 \quad \mathcal{E}_1 \subseteq^* \mathcal{E}_2 \quad \mathcal{D}_1 \subseteq^* \mathcal{D}_2}{\text{Loc}(\mathcal{P}_1) \prec \text{Loc}(\mathcal{P}_2)}$$

## Subtyping rule

$$\frac{\Gamma \vdash v : Tv_1 \quad Tv_1 < Tv_2}{\Gamma \vdash v : Tv_2}$$

$\bar{b}\langle \text{new}\{\text{guest}\}[\dots] \rangle^{\{\text{guest}\}} \mid \bar{b}\langle \text{new}\{\text{member}\}[\dots] \rangle^{\{\text{member}\}}$   
 $\mid !b(y).\text{change}_{\text{forum}\{\text{moderator}\}}(x, x|y)^{\{\text{moderator}\}}$



# 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.

