Information Flow in Boxed Ambient

I. Salvo

a joint work (**in progress**) with:
M. Bugliesi, G. Castagna, S. Crafa

journees “methode formelle pour la mobilitè”,
Paris, December 6, 2002

Outline of the talk

- From Mobile Ambients to NBA
- Information Flow in Distributed Systems
- A Type System for Information Flow in Boxed Ambients
- Conclusions and Future Work

Ambient Calculus

[Cardelli & Gordon 98]

- Main Motivation:
  - Define a calculus to model mobile computations (**programming the Web**)
- Formalize:
  - Named places (ambients) where computations happen
  - **Hierarchical** structure
  - **Movement** between places
  - Asyncronous communication among processes running in parallel inside the same ambient

Operational Semantics

A process may:

- communicate locally in an asyncronous way:

$$\langle M \rangle \mid (x).P \ \longrightarrow \ P\{x := M\}$$

- cause the enclosing ambient to move inside or outside another ambient:

$$n[\mathbf{in}\ m.P \mid Q] \mid m[R] \longrightarrow m[n[P \mid Q] \mid R]$$

$$m[n[\mathbf{out}\ m.P \mid Q] \mid R] \longrightarrow n[P \mid Q] \mid m[R]$$

- destroy the boundary of a sub-ambient:

$$\mathbf{open}\ n.P \mid n[Q] \ \longrightarrow \ P \mid Q$$

“Boxing” Ambients

[Bugliesi, Castagna & Crafa, 01]

- open is essential for communication, but:
  - Dangerous for security:

    $$m[\mathbf{in}\ n.\mathsf{bad}] \mid n[\mathbf{open}\ m.P] \longrightarrow n[P \mid \mathsf{bad}]$$

  - Complicates type systems

- Drop the open capability

- Introduce parent-child communication for expressivess

Boxed Ambient

$$
\begin{array}{llcl}
\text{(Local)} & (x)P \mid \langle M \rangle Q & \longrightarrow & P\{x := M\} \mid Q \\
\text{(Input } n\text{)} & (x)^n P \mid n[\langle M \rangle \mid Q] & \longrightarrow & P\{x := M\} \mid n[Q] \\
\text{(Output } n\text{)} & \langle M \rangle^n \mid n[(x)P \mid Q] & \longrightarrow & n[P\{x := M\} \mid Q] \\
\text{(Input } \uparrow\text{)} & \langle M \rangle \mid n[(x)^{\uparrow} P \mid Q] & \longrightarrow & n[P\{x := M\} \mid Q] \\
\text{(Output } \uparrow\text{)} & (x)P \mid n[\langle M \rangle^{\uparrow} \mid Q] & \longrightarrow & P\{x := M\} \mid n[Q]
\end{array}
$$

Boxed Ambient: Discussion

- Powerful Communication Mechanism

  Example: **Broadcast**

  $$n[!\langle M\rangle \mid m[(x)^{\uparrow} \mid \ldots] \mid \ldots \mid p[(x)^{\uparrow} \mid \ldots]]$$

- Source of grave **interference**

$$m[\ (x)^{n}\ .P \mid n[\ \langle M\rangle\ \mid\ (x)\ .Q \mid k[\ (x)^{\uparrow}\ .R]]]$$

Boxed Ambient (II)

[Bugliesi, Castagna & Crafa, 02]

- two **non-interfering** channels for **local** and **upward** communication:

$$\begin{array}{lrcl} \text{(Local)} & (x)P \mid \langle M \rangle Q & \longrightarrow & P\{x := M\} \mid Q \\ \text{(Input } n\text{)} & (x)^n P \mid n[\langle M \rangle^{\uparrow} \mid Q] & \longrightarrow & P\{x := M\} \mid n[Q] \\ \text{(Output } n\text{)} & \langle M \rangle^n \mid n[(x)^{\uparrow} P \mid Q] & \longrightarrow & n[P\{x := M\} \mid Q] \end{array}$$

NBA Calculus

[Bugliesi, Crafa, Merro & Sassone 02]

- **Expressiveness:**
  - Ambients must statically know their children
  - do not learn about incoming ambients

- Introduce coaction as **binder**:

$$n[\mathbf{enter}\langle m, k\rangle.P \mid Q] \mid m[\overline{\mathbf{enter}}(x, k).R \mid S] \\ \longrightarrow m[n[P \mid Q] \mid R\{x := n\} \mid S]$$

$$n[m[\mathbf{exit}\langle n, k\rangle.P \mid Q] \mid R] \mid \overline{\mathbf{exit}}(x, k).S \\ \longrightarrow m[P \mid Q] \mid n[R] \mid S\{x := m\}$$

NBA: Discussion

- Expressiveness: using guarded choice allow to encode the first version of BA
- Nice equational laws: **LTS sematics**
- Barbs:

$$P \downarrow_n \text{ iff } P \equiv (\nu \vec{m})(n[\overline{\mathbf{enter}}(x,k).Q \mid R] \mid S)$$

$$P \Downarrow_n \text{ iff } \exists Q \text{ and } P \longrightarrow^* Q, Q \downarrow_n$$

- It is equivalent to observe $\langle \cdot \rangle^{\uparrow}$

NBA Type System

- **Types:**

Message Types	W	$::=$	$\mathsf{N}[E]$	ambient/password
		$\mid$	$\mathsf{C}[E]$	capability
Exchange Types	E, F	$::=$	Shh	silent process
		$\mid$	$W_1 \ldots W_k$	Tuples, $k \geq 0$
Process Types	T	$::=$	$[E, F]$	local/upward exchange

NBA Typing Rules

$$\frac{\Gamma \vdash M : \mathsf{N}[E] \quad \Gamma \vdash N : \mathsf{N}[F]}{\Gamma \vdash \mathbf{exit}\langle M, N\rangle : \mathsf{C}[F]} \text{ (Exit)} \qquad \frac{\Gamma \vdash M : \mathsf{N}[F] \quad \Gamma \vdash P : [E, F]}{\Gamma \vdash M[P] : T} \text{ (Amb)}$$

$$\frac{\Gamma \vdash M : \mathsf{N}[\tilde{W}] \quad \Gamma, \tilde{x} : \tilde{W} \vdash P : T}{\Gamma \vdash (\tilde{x} : \tilde{W})^{M}.P : T} \text{ (Input M)}$$

$$\frac{\Gamma, \tilde{x} : \tilde{W} \vdash P : [E, \tilde{W}]}{\Gamma \vdash (\tilde{x} : \tilde{W})^{\uparrow}P : [E, \tilde{W}]} \text{ (Input } \uparrow\text{)} \qquad \frac{\Gamma \vdash M : \tilde{W} \quad \Gamma \vdash P : [\tilde{W}, E]}{\Gamma \vdash \langle M\rangle.P : [\tilde{W}, E]} \text{ (Output)}$$

$$\frac{\Gamma \vdash M : \mathsf{N}[\tilde{W}] \quad \Gamma, x : \mathsf{N}[\tilde{W}] \vdash P : [E, F]}{\Gamma \vdash \overline{\mathbf{exit}}(x, M).P : [E, F]} \text{ (Co-Exit)}$$

Outline of the talk

- From Mobile Ambients to NBA ✓
- Information Flow in Distributed Systems
- A Type System for Information Flow in Boxed Ambients
- Conclusions and Future Work

MAC Security Policy in NBA

- Each Ambient has a security clearance (types)
- Consider a set of subjects (Processes) and of objects (Ambients)
- Define a security policy (e.g no read-up, no write-down)
- Read Access: $m[(x)^n P \mid n[\langle M \rangle^{\uparrow} Q \mid R] \mid S]$
- Write Access: $m[\langle M \rangle^n P \mid n[(x)^{\uparrow} Q \mid R] \mid S]$

Implicit Information Flows

- The behavior of a low level entity depends indirectly from high level ones

- Example: testing the existence of a high level process maybe a relevant information

- Information flow is difficult to formalize: **non interference** **(Goguen, Meseguer 82)**

Example: e-commerce

- Consider an agent P that visits sites that offer a given service
- P stores the offer in its private aerea H
- We do not want a new offer depends on previously stored data and the vendors know the agent visited other sites

$$P \equiv l[!\overline{\mathbf{enter}}(x,k).\langle \mathbf{enter}\langle h,k'\rangle\rangle \mid Q \\ \mid h[!\overline{\mathbf{enter}}(x,k').R \mid S]]$$

What the Example Shows

- The secret component contains low-level subcomponents
- Testing the presence of the secret component is a relevant information
- To enter the secret component a capability is communicated (low level information)
- Information inside H will be inside other secrets components

What has been done so far...

[HR98, BCC02, ...]

- **Usual approaches:** Consider $\Gamma \vdash H$ a high level process
- **Only well-typed contexts** wrt a type system which discards "dangerous" flows of information
- **Interference Free Processes** P is interference free if, for all high level sources H,

$$P \mid H \cong_L P$$

$$P \cong_L Q \text{ iff } \forall C(), C(P) \Downarrow_l \Longleftrightarrow C(Q) \Downarrow_l$$

Our (forthcoming) approach

- Consider processes typed in a lightweight type system without information flow constraints
- Define the set of interference free process
- Define a type system that accepts only interference free processes

Non Interference (revisited)

- **High Level Sources** H is a high level source if

$$(\nu\vec{h})H \cong 0,$$

where $\vec{h}$ is the set of high free names of H

- **Interference Free Processes** P is interference free if, for all high level sources H,

$$(\nu\vec{h})(P \mid H) \cong (\nu\vec{h})P,$$

where $\vec{h}$ is the set of high free names of H and P

Outline of the talk

- **From Mobile Ambients to NBA** ✓
- **Information Flow in Distributed Systems** ✓
- **A Type System for Information Flow in Boxed Ambients**
- **Conclusions and Future Work**

Security Types for NBA

- **Types**:

Message Types	W	$::=$	$\mathsf{N}[\sigma, E]$	ambient/password
		$\mid$	$\mathsf{C}[\sigma, E]$	capability
Exchange Types	E, F	$::=$	Shh	silent process
		$\mid$	$W_1 \ldots W_k$	Tuples, $k \geq 0$
Process Types	T	$::=$	$[\sigma, E, F]$	local/upward exchange

Security Types for NBA

Clearence of types:

$$\alpha(\mathsf{N}[\sigma, E]) = \sigma$$

$$\alpha(\mathsf{C}[\sigma, E]) = \bot$$

$$\alpha(W_1 \ldots W_k) = \mathsf{max}_i\ \alpha(W_i)$$

Type formation rules:

$$\frac{\Gamma \vdash E \quad \Gamma \vdash \alpha(E) \leq \sigma}{\Gamma \vdash \mathsf{N}[\sigma, E]} \text{(Type Amb)} \qquad \frac{\Gamma \vdash E_i \quad \Gamma \vdash \alpha(E_i) \leq \sigma}{\Gamma \vdash [\sigma, E_1, E_2]} \text{(Type Proc)}$$

“Information Flow” Types for NBA

- Message types becomes: $\mathsf{N}[\sigma, \tau, E]$

- Judgement has the shape:

  $\Gamma \vdash_{\phi} P : [\sigma, E, F]$

“Information Flow” Types Rules

$$\frac{\Gamma \vdash M : \mathsf{N}[\tau, \rho, E] \quad \Gamma, x : \mathsf{N}[\tau, -, \tilde{W}] \vdash_{\tau} P : [\sigma, E, F]}{\Gamma \vdash_{\phi} \overline{\mathbf{exit}}(x, M).P : [\sigma, E, F]} \text{ (CoExit)}$$

provided $\mathsf{Safe}(\sigma, \phi, \tau) \quad \rho = H \ \& \ \tau = L \Rightarrow \sigma = H$

$$\frac{\Gamma \vdash M : \mathsf{N}[\tau, -, \tilde{W}] \quad \Gamma, \tilde{x} : \tilde{W} \vdash_{\tau} P : [\sigma, E, F] \quad \mathsf{Safe}(\sigma, \phi, \tau)}{\Gamma \vdash (\tilde{x} : \tilde{W})^{M}.P : [\sigma, E, F]} \text{ (Input M)}$$

Outline of the talk

- **From Mobile Ambients to NBA** ✓
- **Information Flow in Distributed Systems** ✓
- **A Type System for Information Flow in Boxed Ambients** ✓
- **Conclusions and Future Work**

Conclusion and Future Work

- Main achievement: “type indepedent” definition of interference free process
- Study less restrictive type system
- Apply this approach to π-calculus and compare with previous work

Outline of the talk

- From Mobile Ambients to NBA ✓

- Information Flow in Distributed Systems ✓

- A Type System for Information Flow in Boxed Ambients ✓

- Conclusions and Future Work ✓