

# Bisimulation and Unwinding for Verifying Possibilistic Security Properties

---

A. Bossi, R. Focardi, C. Piazza, and S. Rossi

Department of Computer Science  
University Ca' Foscari of Venezia

{bossi,focardi,piazza,srossi}@dsi.unive.it

VMCAI'03 – New York, January 2003

# A Security Problem

---

- ▷ **Data confidentiality** in a **dynamic multilevel** system
  - ▷ **Aim**: assuring that secret **high** level data cannot be inferred by a **low** level user, even with malicious processes running at the high level (internal attacks from, e.g., **Trojan horses**)
  - ▷ **Information Flow**: avoid any **information flow** (direct or indirect) from the high (**classified**) level to the low (**untrusted**) one
  - ▷ **Dynamicity**: a program which is in a secure state for a certain environment might become unprotected if the **environment** suddenly **changes**
- ▷ **Problem**: **verify**, **rectify**, **incrementally build secure** processes

## Plan of the Talk

---

- ▷ The **SPA** Language: syntax and semantics
- ▷ Information Flow Security as **BNDC**
- ▷ Sufficient Conditions: **P\_BNDC**, **SBNDC**, **CP\_BNDC**
- ▷ **Bisimulation** Characterizations: to **verify** security
- ▷ **Unwinding** Characterizations: to **rectify** non-secure processes
- ▷ **Refinement** Operators: to **build** secure processes

# The SPA syntax

---

$E$	$::=$	$\mathbf{0}$	<i>empty process</i>
		$a.E$	<i>input</i>
		$\bar{a}.E$	<i>output</i>
		$\tau.E$	<i>internal action</i>
		$E + E$	<i>non-det. choice</i>
		$E \mid E$	<i>parallel composition</i>
		$E \setminus v$	<i>restriction</i>
		$E[f]$	<i>relabelling</i>
		$Z$	<i>constant</i>

- ▷  $H$  high actions and  $L$  low actions
- ▷  $\mathcal{E}_H$  processes with only high level actions

# The SPA semantics - Transitions

---

Semantics given through transition relations

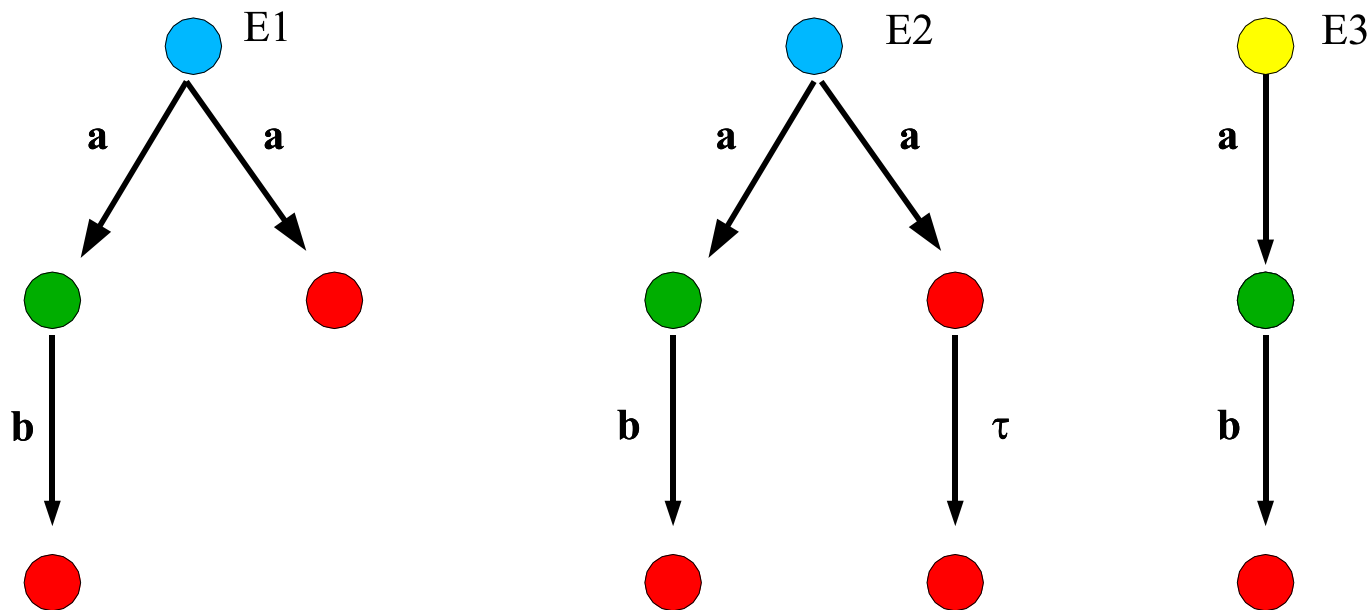
Input		Output	
	$a.E \xrightarrow{a} E$		$a.E \xrightarrow{\bar{a}} E$
Parallel	$E_1 \xrightarrow{a} E'_1$		$E_1 \xrightarrow{a} E'_1 \quad E_2 \xrightarrow{\bar{a}} E'_2$
	$E_1   E_2 \xrightarrow{a} E'_1   E_2$		$E_1   E_2 \xrightarrow{\tau} E'_1   E'_2$

Two processes are equivalent if they are **weak bisimilar**:  $E \approx F$

# Bisimulation

▷ **Idea:** mutual step-by-step simulation.

▷  $E1 = a.b.0 + a.0$       $E2 = a.b.0 + a.\tau.0$       $E3 = a.b.0$



▷ **Note:**  $E3$  cannot simulate the rightmost  $a$  of  $E1$ !

# The SPA semantics - Bisimulation

---

$$E \xRightarrow{\hat{a}} E' = E(\overrightarrow{\tau})^* \xrightarrow{a} (\overrightarrow{\tau})^* E'$$

## Weak Bisimulation

$\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$  over SPA processes such that if  $(E, F) \in \mathcal{S}$  then:

$E \xrightarrow{a} E'$  implies  $F \xRightarrow{\hat{a}} F'$  and  $(E', F') \in \mathcal{S}$

$F \xrightarrow{a} F'$  implies  $E \xRightarrow{\hat{a}} E'$  and  $(E', F') \in \mathcal{S}$

$E \approx F$  if there exists a weak bisimulation  $\mathcal{S}$  containing  $(E, F)$

# Information Flow Security

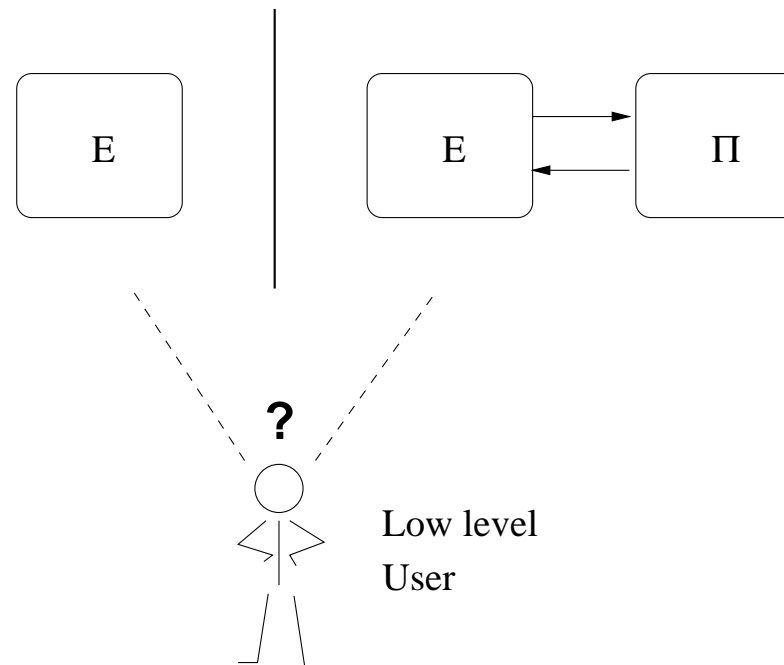
---

- ▶ **Aim**: capture information flow from a **high** (classified) level to a **low** (untrusted) one, even with malicious processes running at the high level (internal attacks from, e.g., **Trojan Horses**)
- ▶ **Non-Interference** [Goguen-Meseguer'82]: **No information flow** is possible **from high to low** if what is done at the high level *cannot interfere* in any way with the low level
- ▶ **BNDC** [Focardi-Gorrieri'94]: formalized non-interference as Bisimulation-based Non Deducibility on Compositions (**BNDC**)

# BNDC Bisimulation based Non Deducibility on Composition

---

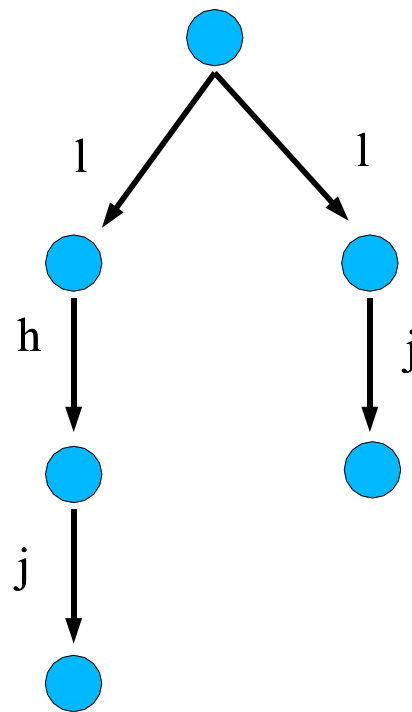
- ▷ **Idea:** check the system against all high level (potentially malicious) processes



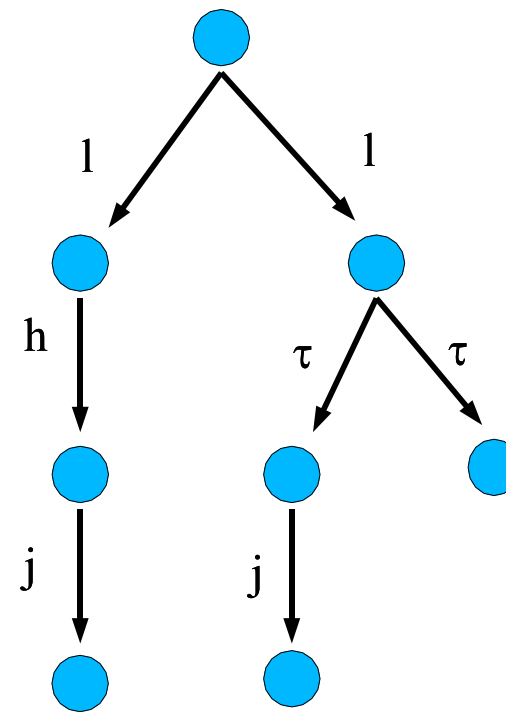
- ▷ **BNDC:**  $\forall \Pi \in \mathcal{E}_H, E \setminus H \approx (E|\Pi) \setminus H$

# Example

---



**Not BNDC**



**BNDC**

$\Pi = \bar{h}.0$  generates a deadlock when in parallel with the one on the left

## BNDC: some problems...

---

- ▷ **Decidability**: the decidability of BNDC is still an **open** problem
- ▷ **Compositionality**:  $E$  and  $F$  are BNDC but  $E|F$  is not BNDC  
(state **explosion** problem)
- ▷ **Persistency**:  $E$  is BNDC but  $E$  reaches  $E'$  and  $E'$  is not BNDC  
(not suitable for **dynamic** contexts)

## ... some solutions

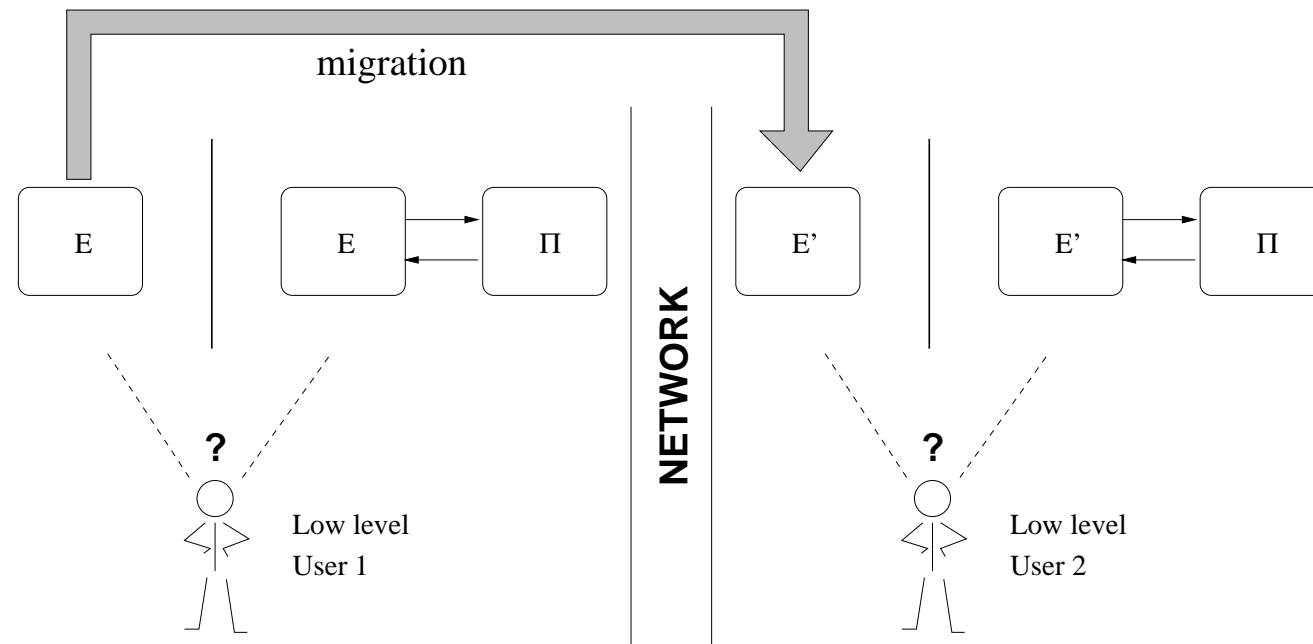
---

- ▷ **Idea**: **Study** different security properties which **imply** BNDC and which are **compositional** and **persistent**
- ▷ **SBNDC** [Focardi-Gorrieri'94]: Strong BNDC proposed as a **decidable** sufficient condition for BNDC
- ▷ **P\_BNDC** [Focardi-Rossi'02]: Persistent BNDC proved to be suitable in **dynamic** contexts
- ▷ **CP\_BNDC** [here]: Compositional Persistent BNDC introduced in this paper

**Study** means: **verify**, **rectify**, **incrementally build**, ...

# P\_BNDC: Persistent BNDC

- ▷ **Idea:** check the system against all high level (potentially malicious) processes which can be dynamically reconfigured



- ▷ **P\_BNDC:**

$$\forall E' \text{ reachable from } E, \forall \Pi \in \mathcal{E}_H, E' \setminus H \approx (E' | \Pi) \setminus H$$

## Bisimulation Characterization of P\_BNDC

---

$$E \xRightarrow{\hat{a}}_{\setminus H} E' = \begin{cases} E \xRightarrow{\hat{a}} E' & \text{if } a \notin H \\ E \xRightarrow{\hat{a}} E' \text{ or } E \xRightarrow{\hat{\tau}} E' & \text{if } a \in H \end{cases}$$

### Weak Bisimulation up to $H$

$\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$  over SPA processes such that if  $(E, F) \in \mathcal{S}$  then:

$E \xrightarrow{a} E'$  implies  $F \xRightarrow{\hat{a}}_{\setminus H} F'$  and  $(E', F') \in \mathcal{S}$

$F \xrightarrow{a} F'$  implies  $E \xRightarrow{\hat{a}}_{\setminus H} E'$  and  $(E', F') \in \mathcal{S}$

$E \approx_{\setminus H} F$ , if there exists  $\mathcal{S}$  w. b. up to  $H$  containing  $(E, F)$

# Bisimulation Characterization of P\_BNDC

---

## Theorem

$$E \text{ is P\_BNDC} \quad \text{iff} \quad E \setminus H \approx_{\setminus H} E$$

This is a **global condition**: **efficiently** verify P\_BNDC [VMCAI'02]

**Intuition:**

$E \setminus H$  simulates the high actions of  $E$  with **0 or more**  $\tau$ 's

# Unwinding Characterization of P\_BNDC

---

## Theorem

$E$  is P\_BNDC iff for all  $E'$  reachable from  $E$

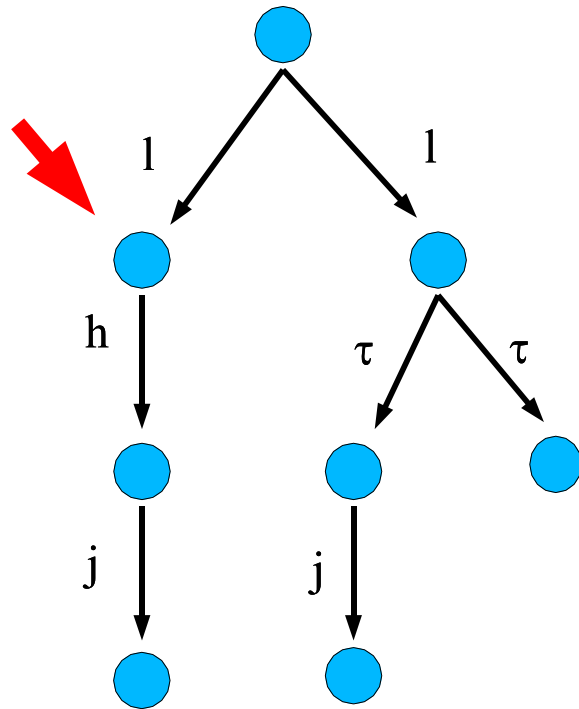
$$E' \xrightarrow{h} E'' \text{ implies } E' \xrightarrow{\hat{\tau}} E''' \text{ and } E'' \setminus H \approx E''' \setminus H$$

$E'$  reaches through 0 or more  $\tau$ 's a state equiv. to  $E''$  for the low level user

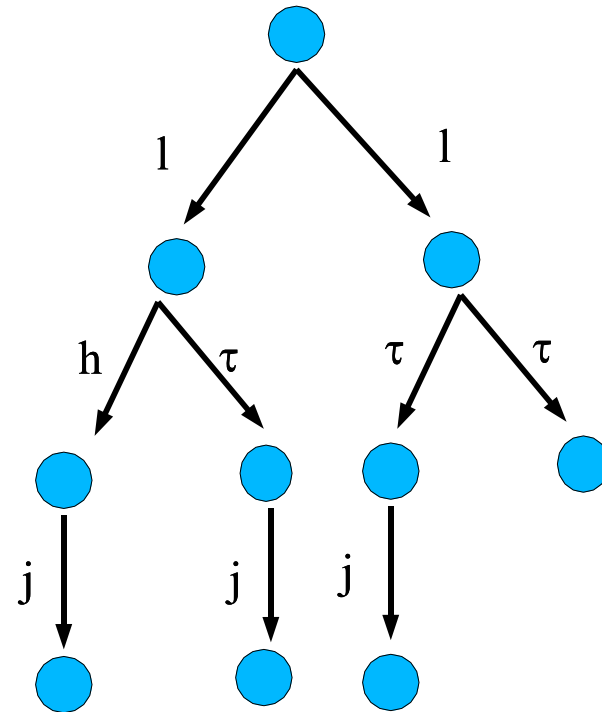
This is a **local condition**:

- ▷ **rectify** non P\_BNDC processes [AMAST'02]
- ▷ **incrementally build** P\_BNDC processes [LOPSTR'02]

# Example



**BNDC not P\_BNDC**



**P\_BNDC**

# Unwinding Definition of SBND C

---

## Definition

$E$  is SBND C iff for all  $E'$  reachable from  $E$

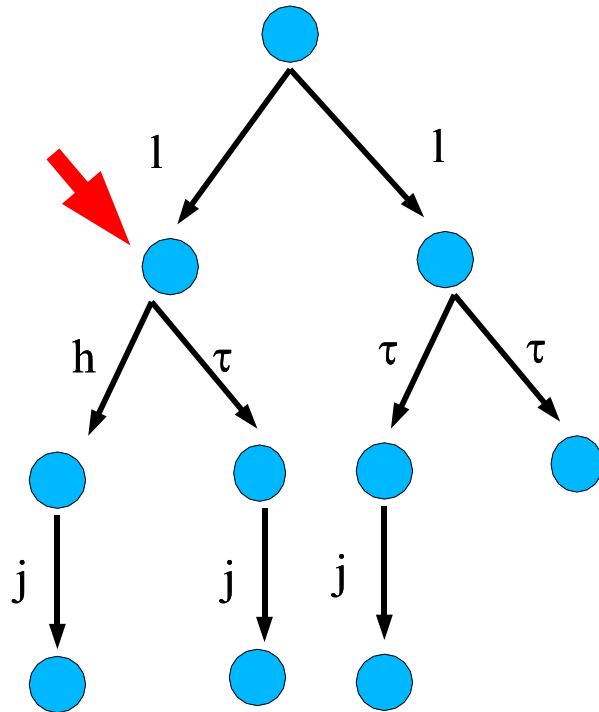
$$E' \xrightarrow{h} E'' \text{ implies } E'' \setminus H \approx E' \setminus H$$

$E'$  reaches through **zero**  $\tau$ 's a state equivalent to  $E''$  for the low level user

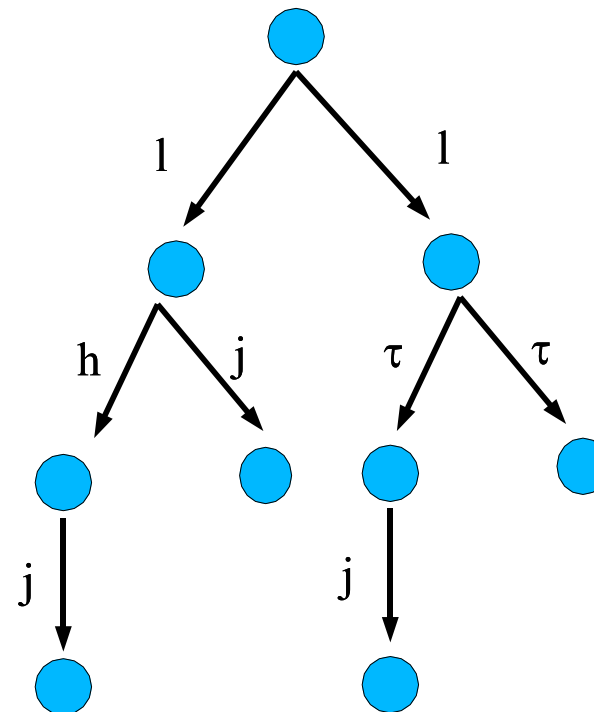
The low level user cannot tell whether any high level action has been performed on the system

This is a **local condition**: **rectify** and **incrementally build**

# Example



**P\_BNDC not SBNDC**



**SBNDC**

# Bisimulation Characterization of SBNDC

---

$$E \xrightarrow{\hat{a}}_{\setminus H}^0 E' = \begin{cases} E \xrightarrow{\hat{a}} E' & \text{if } a \notin H \\ E \xrightarrow{\hat{a}} E' \text{ or } E \xrightarrow{\tau} E' & \text{if } a \in H \end{cases}$$

## Theorem

$$E \text{ is SBNDC} \quad \text{iff} \quad E \setminus H \approx_{\setminus H}^0 E$$

This is a **global condition** useful to **efficiently** verify SBNDC

**Intuition:**

$E \setminus H$  simulates the high actions of  $E$  with  $\tau$ 's

## Properties of SBNDC and P\_BNDC

---

- ▷  $\text{SBNDC} \subseteq \text{P\_BNDC} \subseteq \text{BNDC}$
- ▷ SBNDC and P\_BNDC are
  - ▷ persistent
  - ▷ compositional w.r.t. parallel

SBNDC and P\_BNDC are **not compositional** w.r.t. **non deterministic choice** operator

## Bisimulation Definition of CP\_BNDC

---

$$E \xrightarrow{\hat{a}}^+_H E' = \begin{cases} E \xrightarrow{\hat{a}} E' & \text{if } a \notin H \\ E \xrightarrow{\hat{a}} E' \text{ or } E \xrightarrow{\tau} E' & \text{if } a \in H \end{cases}$$

### Definition

$$E \text{ is CP\_BNDC} \quad \text{iff} \quad E \setminus H \approx^+_H E$$

### Intuition:

$E \setminus H$  simulates the high actions of  $E$  with **at least one**  $\tau$

CP\_BNDC is **compositional** also w.r.t. the **non deterministic choice** operator

## Unwinding Characterization of CP\_BNDC

---

### Theorem

$E$  is CP\_BNDC iff for all  $E'$  reachable from  $E$

$$E' \xrightarrow{h} E'' \text{ implies } E' \xrightarrow{\tau} E''' \text{ and } E'' \setminus H \approx E''' \setminus H$$

$E'$  reaches through **at least one**  $\tau$  a state equiv. to  $E''$  for the low level user

The low level user cannot distinguish whether the system has been moved by a high level action or by internal actions

# Refinement Operators

---

- ▷ **Abstraction** and **Decomposition** to **develop** large systems
- ▷ **Refinement** [Jacob'89]: an abstract specification  $A$  is **refined** by a specification  $C$  if all behaviors allowed by  $C$  are allowed by  $A$ , i.e., **removal of non determinism**

A **refinement operator** can be seen as a **function**

$$ref : \mathcal{E} \longrightarrow \mathcal{E}$$

We consider only refinement operators **preserving the low level view**

$$E \setminus H \approx F \setminus H \text{ implies } ref(E) \setminus H \approx ref(F) \setminus H$$

# CP\_BNDC, SBND, P\_BNDC and Refinement

---

When does a **refinement preserve** P\_BNDC (SBND, CP\_BNDC)?

**Unwinding** characterizations suggest:

if  $E$  reaches  $E'$  and  $E''$  with  $E' \setminus H \approx E'' \setminus H$  and we refine  $E'$ ,  
then we have to refine also  $E''$

Let  $ref$  be a refinement operator

$$refine(E, ref, S)$$

is the refinement operator obtained by applying  $ref$  only to the  
 $E' \in S$  reachable from  $E$

# CP\_BNDC, SBNDC, P\_BNDC and Refinement

---

## Theorem

Let  $S$  be a set s.t. for all  $E', E''$  reachable from  $E$   
if  $E' \in S$  and  $E' \setminus H \approx E'' \setminus H$  then  $E'' \in S$  (\*\*)

If  $E$  is P\_BNDC (CP\_BNDC, SBNDC) then  $refine(E, ref, S)$  is  
P\_BNDC (CP\_BNDC, SBNDC)

## Corollary

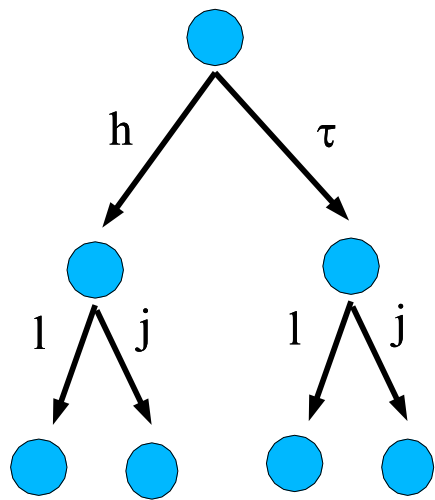
Let  $S^+$  be the smallest set s.t.  $S \subseteq S^+$  and  $S^+$  satisfies (\*\*)

Let  $S^-$  be the largest set s.t.  $S^- \subseteq S$  and  $S^-$  satisfies (\*\*)

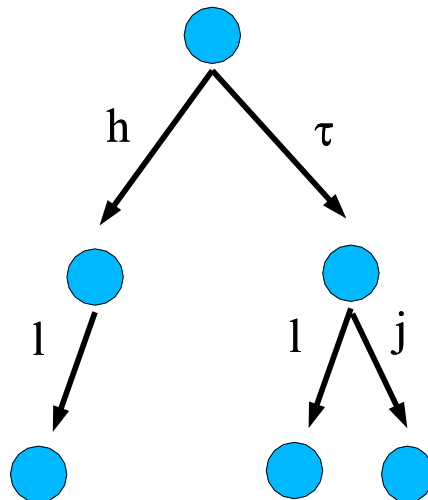
If  $E$  is P\_BNDC (CP\_BNDC, SBNDC) then  $refine(E, ref, S^+)$  and  
 $refine(E, ref, S^-)$  are P\_BNDC (CP\_BNDC, SBNDC)

# Example

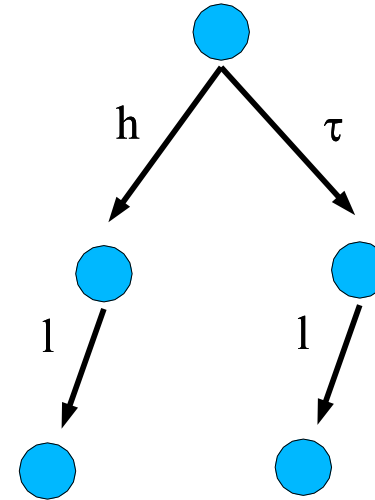
---



**P\_BNDC**



**wrong ref**



**right ref**

## Conclusions

---

- ▷ a strong **connection** between **bisimulation** characterizations and **unwinding** conditions has been pointed out
- ▷ a **fully compositional and persistent bisimulation based security property** has been defined
- ▷ **preservation** under **refinement** of properties that are characterized through unwinding conditions has been analysed