

Ensuring Information Flow Security

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

MyThS, Bertinoro, September 2002

Plan of the Talk

- ▷ A Security Problem
- ▷ Information Flow Security as **P_BNDC**
- ▷ Properties of P_BNDC: **unwinding condition** and **compositionality**
- ▷ A **transformation** to ensure P_BNDC
- ▷ A **proof system** for P_BNDC

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
 - ▷ **Non-Interference** [Goguen-Meseguer'82]: what is done at the high level **cannot interfere** in any way with the low level
 - ▷ **Dynamicity**: a program which is in a secure state for a certain environment might become unprotected if the **environment** suddenly **changes**

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	$\frac{E_1 \xrightarrow{a} E'_1}{E_1 E_2 \xrightarrow{a} E'_1 E_2}$	$\frac{E_1 \xrightarrow{a} E'_1 \quad E_2 \xrightarrow{\bar{a}} E'_2}{E_1 E_2 \xrightarrow{\tau} E'_1 E'_2}$

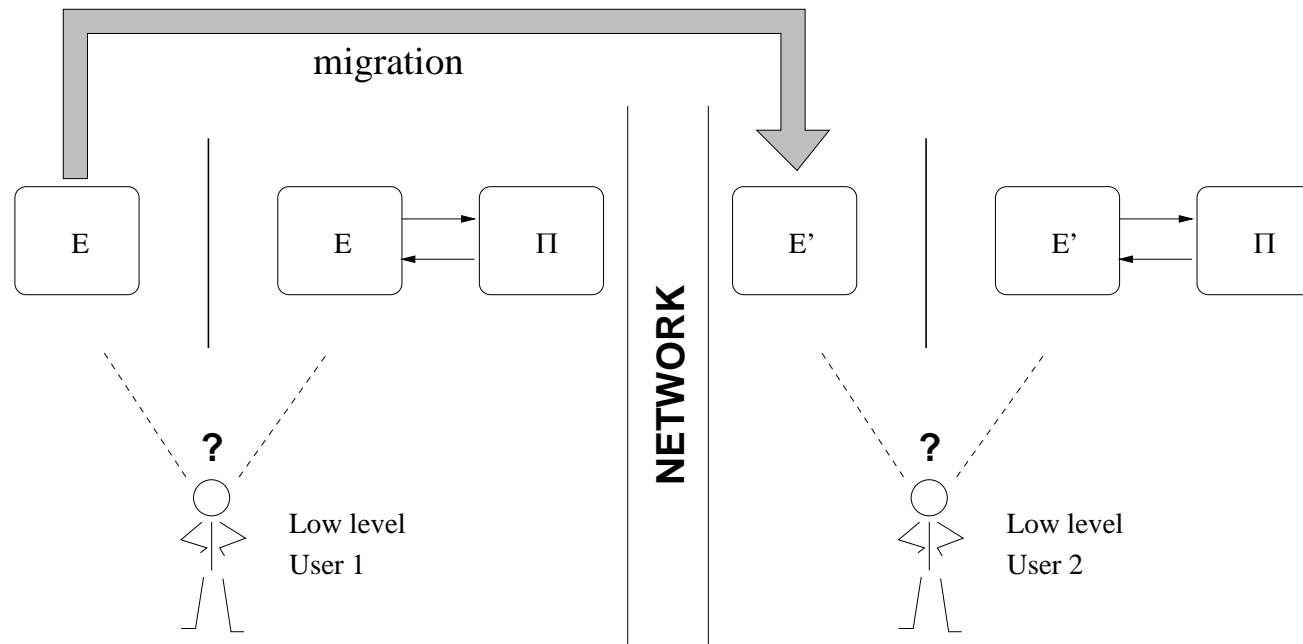
Two processes are equivalent if they are **weak bisimilar**: $E \approx F$

Information Flow Security as P_BNDC

- ▷ **P_BNDC** (Persistent Bisimulation-based Non Deducibility on Compositions) [Focardi-Rossi'02]
 - ▷ is a generalization of (**BNDC**) [Focardi-Gorrieri'94]
 - ▷ formalizes the concept of **Non-Interference** [Goguen-Meseguer'82] for processes running in dynamic contexts.

P_BNDC Persistent Bisimulation Non Deducibility on Composition

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



- ▷ **P_BNDC:**

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

Weak bisimulation up to H

$$E \xRightarrow{\hat{a}}_{\setminus H} E' = \begin{cases} E(\overrightarrow{\tau})^* (\overrightarrow{a}) (\overrightarrow{\tau})^* E' & \text{if } a \notin H \\ E(\overrightarrow{\tau})^* (\overrightarrow{a})^{\{0,1\}} (\overrightarrow{\tau})^* E' & \text{if } a \in H \end{cases}$$

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)

A first characterization

Theorem

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

- ▷ **Intuition:** $E \setminus H$ simulates the high actions of E with 0 or more τ transitions

Recent works

- ▷ How to **transform** a process to **ensure** P_BNDC?
- ▷ How to use transformations to **check** P_BNDC?
- ▷ How to **compose** P_BNDC processes?
- ▷ How to **incrementally build** P_BNDC processes?

Unwinding condition

Theorem

Let $E \in \mathcal{E}$ be a process.

$$E \in P_BNDC$$

iff

if $E \rightsquigarrow E_i \xrightarrow{h} E_j$, then $E_i \xrightarrow{\hat{\tau}} E_k$ and $E_j \setminus H \approx E_k \setminus H$

Checking the unwinding condition: example 1

Let E be $h.E_1 + \tau.E_1$.

Then

$$E \rightsquigarrow E \xrightarrow{h} E_1$$

but also

$$E \xrightarrow{\tau} E_1$$

and clearly:

$$E_1 \setminus H \approx E_1 \setminus H.$$

A Transformation to Ensure P_BNDC

Let E be a process of the form

$$E = \sum_{i \in I} l_i.F_i + \sum_{j \in J} h_j.F_j$$

with $l_i \in L \cup \{\tau\}$ and $h_j \in H$

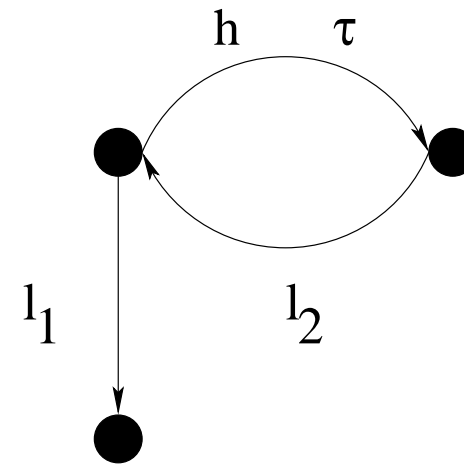
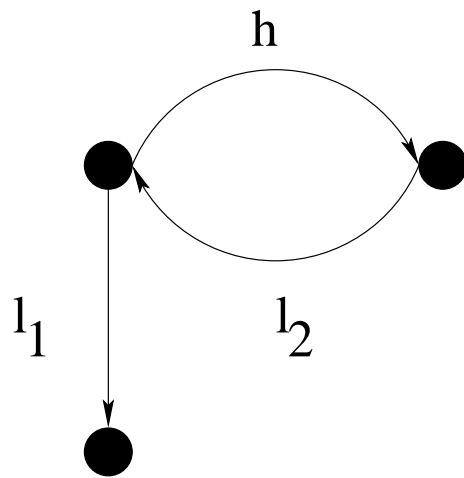
Its τ completion E^τ is of the form

$$E^\tau = \sum_{i \in I} l_i.F_i^\tau + \sum_{j \in J} h_j.F_j^\tau + \sum_{j \in J} \tau.F_j^\tau$$

Example

$$\begin{cases} E &= h.F + l_1.\mathbf{0} \\ F &= l_2.E \end{cases}$$

$$\begin{cases} E^\tau &= h.F^\tau + \tau.F^\tau + l_1.\mathbf{0} \\ F^\tau &= l_2.E^\tau \end{cases}$$



Properties of the τ completion

Theorem For any process E , E^τ is P_BNDC

- ▷ $E/H \approx E^\tau/H$: E and E^τ behave in the same way if we hide high actions
- ▷ $E \setminus H \approx E^\tau \setminus H$ iff $E \setminus H \approx E/H$: if E is BSNNI, then from the low level point of view E and E^τ behave in the same way

Theorem E is P_BNDC iff $E \approx_{\setminus H} E^\tau$

Compositionality of P_BNDC

- ▷ if E is a closed process in \mathcal{E}_L , then $E \in P_BNDC$
- ▷ if E is a closed process in \mathcal{E}_H , then $E \in P_BNDC$
- ▷ if $E \in P_BNDC$, then $E \setminus v \in P_BNDC$
- ▷ if $E \in P_BNDC$, then $E[f] \in P_BNDC$
- ▷ if $E, F \in P_BNDC$, then $E|F \in P_BNDC$
- ▷ if $E_i, F_j \in P_BNDC$, $i \in I$ and $j \in J$, then
$$\sum_{i \in I} a_i \cdot E_i + \sum_{j \in J} (h_j \cdot F_j + \tau \cdot F_j) \in P_BNDC$$
where $a_i \in L$ and $h_j \in H$
- ▷ if $E \in P_BNDC$ and $X \stackrel{\text{def}}{=} E$, then $X \in P_BNDC$

The proof system Core - 1

$$\frac{}{P \in \mathcal{HP}[\emptyset]} \quad P \in \mathcal{E}_L, P \text{ is closed} \quad (\textit{Low})$$

$$\frac{}{P \in \mathcal{HP}[\emptyset]} \quad P \in \mathcal{E}_H, P \text{ is closed} \quad (\textit{High})$$

$$\frac{}{X \in \mathcal{HP}[\{X\}]} \quad X \text{ is a constant} \quad (\textit{Const})$$

$$\frac{E \in \mathcal{HP}[A] \quad F \in \mathcal{HP}[B]}{E|F \in \mathcal{HP}[A \cup B]} \quad (\textit{Par})$$

The proof system Core - 2

$$\frac{E \in \mathcal{HP}[A]}{E \setminus v \in \mathcal{HP}[A]} \quad (\textit{Rest})$$

$$\frac{E \in \mathcal{HP}[A]}{E[f] \in \mathcal{HP}[A]} \quad (\textit{Label})$$

$$\frac{E \in \mathcal{HP}[A]}{X \in \mathcal{HP}[A]} \quad X \stackrel{\textit{def}}{=} E \quad (\textit{Def})$$

$$\frac{E_i \in \mathcal{HP}[A_i] \quad F_j \in \mathcal{HP}[B_j]}{\sum_i a_i \cdot E_i + \sum_j (h_j \cdot F_j + \tau \cdot F_j) \in \mathcal{HP}[\cup_i A_i \cup \cup_j B_j]} \quad (\textit{Choice})$$

$$a_i \in L \cup \{\tau\}, h_j \in H$$

Example

$$\begin{array}{c}
 \frac{}{b.\mathbf{0} \in \mathcal{HP}[\emptyset]} \quad (Low) \\
 \frac{}{h.b.\mathbf{0} + \tau.b.\mathbf{0} \in \mathcal{HP}[\emptyset]} \quad (Choice) \\
 \frac{}{a.(h.b.\mathbf{0} + \tau.b.\mathbf{0}) \in \mathcal{HP}[\emptyset]} \quad (Choice) \qquad \frac{}{X \in \mathcal{HP}[\{X\}]} \quad (Const) \\
 \hline
 a.(h.b.\mathbf{0} + \tau.b.\mathbf{0}) | X \in \mathcal{HP}[\{X\}] \quad (Par)
 \end{array}$$

The full system

Consider the systems

$$\left\{ \begin{array}{l} X \stackrel{\text{def}}{=} h.X + l.Y \\ Y \stackrel{\text{def}}{=} l.X \end{array} \right.$$

$$\left\{ \begin{array}{l} X \stackrel{\text{def}}{=} h.Y + \tau.Z \\ Y \stackrel{\text{def}}{=} h.Y + l.Z \\ Z \stackrel{\text{def}}{=} l.Z \end{array} \right. \quad Y \setminus H \equiv Z \setminus H$$

The rule (**Sys**) allows us to prove that they are P_BNDC

Checking the unwinding condition: example 2

If $E \rightsquigarrow E_i \xrightarrow{h} E_j$, then $E_i \xrightarrow{\hat{\tau}} E_k$ and $E_j \setminus H \approx E_k \setminus H$

Let

$$\left\{ \begin{array}{l} X \stackrel{\text{def}}{=} h.Y + \tau.Z \\ Y \stackrel{\text{def}}{=} a.Y \\ Z \stackrel{\text{def}}{=} \tau.Y \\ V \stackrel{\text{def}}{=} h.(h.V + \tau.V) + a.Z \end{array} \right.$$

$X \xrightarrow{h} Y$ but also $X \xrightarrow{\tau} Y$

$V \xrightarrow{h} (h.V + \tau.V)$ but also $V \xrightarrow{\hat{\tau}} V$ and $(h.V + \tau.V) \setminus H \approx V \setminus H$

Safety Set: $Safe(E)$

If $F \in Safe(E)$ then there exists F' such that $E \xRightarrow{\hat{\tau}} F'$ and $F \setminus H \equiv F' \setminus H$

Hence a possible transition $E \xrightarrow{h} F$ is not a problem.

$$safe_1(E) = \{F \mid E \xRightarrow{\hat{\tau}} F\}$$

$$safe_2(E) = \{F \mid F \setminus H \equiv E \setminus H\}$$

$$safe_3(E) = \{F \mid F \setminus H \equiv \tau.E \setminus H\}$$

Example 0.1 Let $a, b \in L$ and $h \in H$. Consider the system S :

$$\left\{ \begin{array}{l} X = h.Y + \tau.Z \\ Y = a.Y \\ Z = \tau.Y \\ V = h.(h.V + \tau.V) + a.Z \end{array} \right.$$

We have that $Y \in \text{safe}_1(X)$, $W \in \text{safe}_2(W)$ and $(h.V + \tau.V) \in \text{safe}_3(V)$.

Correctness and Completeness

- ▷ The system is correct (unwinding and compositionality)
- ▷ The system is not complete:
 - ▷ The rule (**Choice**) is not complete
 - ▷ The rule (**Sys**) is not complete
- ▷ It possible to extend both rules

Conclusions

- ▷ **P_BNDC** ensures Non-Interference in dynamic contexts.
- ▷ We give an **unwinding condition** for P_BNDC which allows us to express P_BNDC in terms of a local property.
- ▷ We show how to **ensure** P_BNDC by **transforming** a given process
- ▷ We define a **proof system** which allow us to **incrementally** build secure processes.
- ▷ We are working on
 - ▷ new **unwinding conditions** for other security properties
 - ▷ a **refinement** operator which preserves these properties
 - ▷ a definition of **secure context**

References

- ▷ R. Focardi, S. Rossi. **Information Flow Security in Dynamic Contexts** CSFW 2002, pag. 307-319, IEEE, 2002.
- ▷ R. Focardi, C. Piazza, S. Rossi. **Proofs Methods for Bisimulation based Information Flow Security** VMCAI 2002, LNCS 2294, pag. 16-31, Springer, 2002.
- ▷ A. Bossi, R. Focardi, C. Piazza, S. Rossi. **Transforming Processes to Check and Ensure Information Flow Security** AMAST 2002, LNCS 2422 , pag. 271-286, Springer, 2002.
- ▷ A. Bossi, R. Focardi, C. Piazza, S. Rossi. **A Proof System for Information Flow Security** LOPSTR '02, LNCS, Springer, 2002, to appear.

Downloadable at <http://www.dsi.unive.it/~srossi>