

Secure contexts for Information Flow Security

A. Bossi, D. Macedonio, C. Piazza, and S. Rossi

Department of Computer Science
University Ca' Foscari of Venezia

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

Venezia, December 5, 2002

Plan of the Talk

- ▷ A Security Problem
- ▷ The SPA language: syntax and semantics
- ▷ The notion of Secure Contexts
- ▷ Some examples
- ▷ Secure Contexts using Bisimulation
- ▷ Secure Contexts using Trace Equivalence

A Security Problem

- ▷ Information Flow Security
 - ▷ **Aim**: capture information flow from a **high** level to a **low** one
 - ▷ **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
- ▷ We have a process E and a context C , we want no information flow when E is executed inside C .

The SPA syntax

T	$::=$	$\mathbf{0}$	<i>empty process</i>
		Z	<i>variable</i>
		$a.T$	<i>actions</i>
		$T + T$	<i>non-det. choice</i>
		$T \mid T$	<i>parallel composition</i>
		$T \setminus v$	<i>restriction</i>
		$T[f]$	<i>relabelling</i>
		$recZ.T$	<i>recursion</i>

- ▷ H high actions and L low actions
- ▷ \mathcal{E} Processes: terms without free variables
- ▷ Contexts: terms in which free variables can occur.

The SPA semantics - Transitions

Semantics given through transition relations \rightarrow among processes defined by axioms and inference rules

<p>Action</p> $\frac{}{a.E \xrightarrow{a} E}$	<p>Restriction</p> $\frac{E \xrightarrow{a} E' \quad a \notin v}{E \setminus v \xrightarrow{a} E' \setminus v}$
<p>Parallel</p> $\frac{E_1 \xrightarrow{a} E'_1}{E_1 E_2 \xrightarrow{a} E'_1 E_2}$	$\frac{E_1 \xrightarrow{a} E'_1 \quad E_2 \xrightarrow{\bar{a}} E'_2}{E_1 E_2 \xrightarrow{\tau} E'_1 E'_2}$

$E \setminus H$ is E restricted to low actions.

Example: Security for Process

E a **Java applet** downloadable from the site of MONEY&MONEY LTD, which allows MONEY&MONEY's customers to get the **price-list**, while the rest of the world can only see the **product-list**.

$$E = \text{PWD_SELLER} \cdot (\overline{\text{PRICE_LIST}} \cdot 0 + \overline{\text{PRICE_LIST}} \cdot 0) + (\overline{\text{PROD_LIST}} \cdot 0 + \overline{\text{PROD_LIST}} \cdot 0)$$

Machines running E :

▷ $X \mid \overline{\text{PWD_SELLER}} \cdot 0$

▷ X

▷ $\text{PWD_HIGH} \cdot (X \mid \overline{\text{PWD_SELLER}} \cdot 0) + \text{PWD_LOW} \cdot X$

Example: Security for Context

MR EARNER has on his own machine C some files containing the information about his investments. He bought a program E which checks on the stock market, reads the files and determines whether the investments are profitable, and, if necessary, checks again on the stock market, for better opportunities.

$$C = X | \overline{\text{ACCESS_GOOD}}.0 \quad \text{or}$$

$$X | \overline{\text{ACCESS_BAD}}.\text{SUGGESTIONS}.0.$$

$$E = \text{CHECK_MARKET}.\left(\text{ACCESS_GOOD}.0 + \text{ACCESS_BAD}.\text{CHECK_MARKET}.\overline{\text{SUGGESTIONS}}.0\right)$$

Example: Security for Context

MR EARNER has on his own machine C some files containing the information about his investments. He bought a program E which checks on the stock market, reads the files and determines whether the investments are profitable, and, if necessary, checks again on the stock market, for better opportunities.

$$C = X | \overline{\text{ACCESS_GOOD}}.0 \quad \text{or}$$

$$X | \overline{\text{ACCESS_BAD}}.\text{SUGGESTIONS}.0.$$

$$E = \text{CHECK_MARKET}.\left(\text{ACCESS_GOOD}.\text{CHECK_MARKET}.0 + \text{ACCESS_BAD}.\text{CHECK_MARKET}.\overline{\text{SUGGESTIONS}}.0\right)$$

The notion of Secure Contexts - 1

- ▷ \sim_l a low level observational equivalence
- ▷ E_l process E without high level capabilities

\mathcal{C} class of contexts, \mathcal{P} class of processes, and X a variable.

\mathcal{C} is secure for \mathcal{P} with respect to X if

$$\forall C[X] \in \mathcal{C}, \forall E \in \mathcal{P}, \quad C[E] \sim_l C[E_l]$$

A low level user cannot discern whether C is interacting with E or E_l

The notion of Secure Contexts - 2

We require that

$$\forall C[X] \in \mathcal{C}, \forall E \in \mathcal{P}, \quad C[E] \sim_l C[E_l]$$

Two points of view

- ▷ **Security for the process:** C is not able to reveal any high level information of E , since it reveals only the information that is revealed by the interaction with E_l
- ▷ **Security for the context:** E is not able to reveal any high information of C , since it reveals the same information which can be revealed by E_l

The SPA semantics - Weak Bisimulation

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

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

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 $(E', F') \in \mathcal{S}$

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

An instance: Weak Bisimulation and Restriction

- ▷ $E \sim_l F$ iff $E \setminus H \approx_b F \setminus H$
- ▷ E_l is $E \setminus H$

\mathcal{C} is secure for \mathcal{P} with respect to X iff

$$\forall C[X] \in \mathcal{C}, \forall E \in \mathcal{P}, C[E] \setminus H \approx_b C[E \setminus H] \setminus H$$

A special instance: *BNDC* processes

- ▷ Definition: $E \in \text{BNDC}$ iff $\forall \Pi \in \mathcal{E}_H, E \setminus H \approx_b (E|\Pi) \setminus H$
- ▷ Characterization: $E \in \text{BNDC}$ iff it is **secure**
for all contexts $C[X] \equiv X|\Pi, \Pi \in \mathcal{E}_H$

Example: Security for Process \approx_b

$$E = \text{PWD_SELLER}.\left(\overline{\text{PRICE_LIST}}.\mathbf{0} + \overline{\text{PRICE_LIST}}.\mathbf{0}\right) + \left(\overline{\text{PROD_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}\right)$$

$$\triangleright C_1[X] = X \mid \overline{\text{PWD_SELLER}}.\mathbf{0}$$

$$\triangleright C_2[X] = \text{PWD_HIGH}.\left(X \mid \overline{\text{PWD_SELLER}}.\mathbf{0}\right) + \text{PWD_LOW}.X$$

$$C_1[E] \setminus H = \tau.\overline{\text{PRICE_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$C_1[E \setminus H] \setminus H = \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$C_2[E] \setminus H = \text{PWD_LOW}.\overline{\text{PROD_LIST}}.\mathbf{0}$$

$$C_2[E \setminus H] \setminus H = \text{PWD_LOW}.\overline{\text{PROD_LIST}}.\mathbf{0}$$

Secure Processes for a generic class \mathcal{P}

A class of contexts which are **secure for all the processes**:

the minimum class \mathcal{C}_s such that:

- ▷ if $F \in \mathcal{E}$, then $F \in \mathcal{C}_s$
- ▷ if Y is a variable, then $Y \in \mathcal{C}_s$
- ▷ if $C_i \in \mathcal{C}_s$ for all $i \in I$, then $\sum_{i \in I} a_i.C_i \in \mathcal{C}_s$
- ▷ if $C \in \mathcal{C}_s$, then $C \setminus v \in \mathcal{C}_s$
- ▷ if $C \in \mathcal{C}_s$, then $C[f] \in \mathcal{C}_s$
- ▷ if $C \in \mathcal{C}_s$, then $recY.C \in \mathcal{C}_s$

No parallel composition:

X is secure for \mathcal{E} , but $X|X$ is not secure for $h.l.\mathbf{0} + \bar{h}.\mathbf{0}$

Secure processes for P_BNDC class

$E \in P_BNDC$ iff $\forall E'$ reachable from E , $E' \in BNDC$

$C[X]$ is a P_BNDC -context with respect to X if for all $E \in P_BNDC$ it holds that $C[E] \in P_BNDC$.

Let C and D be two P_BNDC -contexts with respect to X which are secure for P_BNDC with respect to X . The context $C|D$ is a P_BNDC -context with respect to X and it is secure for P_BNDC with respect to X .

Example: Security for Process $\not\approx_b$

MONEY&MONEY could imagine that people usually set cookies in which they store passwords. Hence it decides to change the applet: if the password is inserted, then an encrypted price-list is given.

$$\triangleright E = \text{PWD_SELLER}.\overline{\text{PRICE_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$\triangleright C[X] = X|\overline{\text{PWD_SELLER}}.\mathbf{0}$$

$$C[E] \setminus H = \tau.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$C[E \setminus H] \setminus H = \overline{\text{PROD_LIST}}.\mathbf{0}$$

The two processes are **not weak bisimilar**.

The SPA semantics - Trace Equivalence

$$E \xrightarrow{a_1 \dots a_n} E' = E(\tau)^* \xrightarrow{a_1} (\tau)^* \dots (\tau)^* \xrightarrow{a_n} (\tau)^* E'$$

Trace

For any process $E \in \mathcal{E}$ the set of traces associates with E is

$$Tr(E) = \{a_1 \dots a_n \in \mathcal{L}^* : \exists E', E \xrightarrow{a_1 \dots a_n} E'\}$$

Trace Equivalence

Two processes are trace equivalent if they have the same traces, i.e.

$$E \approx_t F \text{ if } Tr(E) = Tr(F)$$

An instance: Trace Equivalence and Restriction

- ▷ $E \sim_l F$ iff $E \setminus H \approx_t F \setminus H$
- ▷ E_l is $E \setminus H$

\mathcal{C} is secure for \mathcal{P} with respect to X iff

$$\forall C[X] \in \mathcal{C}, \forall E \in \mathcal{P} \quad C[E] \setminus H \approx_t C[E \setminus H] \setminus H$$

A special instance: *NDC* processes

- ▷ Definition: $E \in \text{NDC}$ iff $\forall \Pi \in \mathcal{E}_H, E \setminus H \approx_t (E|\Pi) \setminus H$
- ▷ Characterization: $E \in \text{NDC}$ iff it is **secure**
for all contexts $C[X] \equiv X|\Pi, \Pi \in \mathcal{E}_H$

Example: Security for Process \approx_t

$$\triangleright E = \text{PWD_SELLER.} \overline{\text{PRICE_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$\triangleright C[X] = X | \overline{\text{PWD_SELLER}}.\mathbf{0}$$

$$C[E] \setminus H = \tau.\mathbf{0} + \overline{\text{PROD_LIST}}.\mathbf{0}$$

$$C[E \setminus H] \setminus H = \overline{\text{PROD_LIST}}.\mathbf{0}$$

The two processes are **not weak bisimilar**, but they are **trace equivalent**.

Conclusions

- ▶ We consider **information flow security** in a multilevel system in the case we have some knowledge about the contexts where the process is going to run
- ▶ We introduce a parametric notion of **secure context** for a process
- ▶ We study two instances: **bisimulation** and **trace equivalence**
- ▶ We show that **BNDC** and **NDC** properties are special instances of our general notion.