P-Congruences as Noninterference for the π-Calculus

Silvia Crafa

Universita' di Padova

Italy

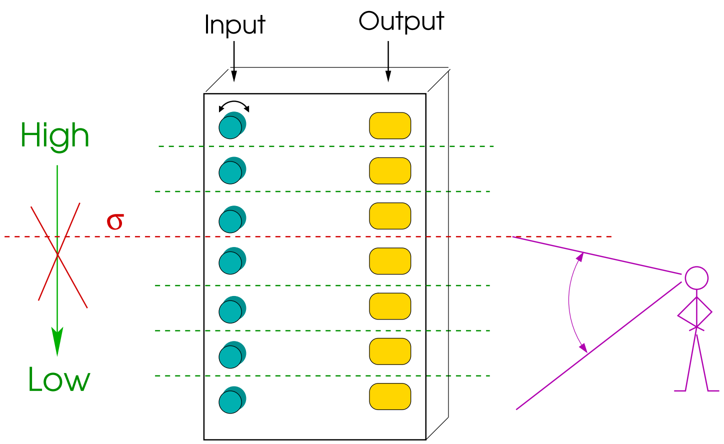
Sabina Rossi

Universita' Ca' Foscari Venezia

Italy

FMSE 06, Fairfax Virginia USA, 3 Nov. 2006

Noninterference



Noninterference

information does not flow from high to low

if the high behavior has no effect on

what can be observed at low level.

INGREDIENTS:

- something to modify the high behaviour: attackers affecting *high components*
- something that observes: contexts affecting *low components*
- something to compare behaviours: *behavioral equivalence*

Noninterference in π-calculus

- $h().\ell() \mid \overline{h}\langle\rangle$ is insecure

Noninterference in π-calculus

- $h().\ell() \mid \overline{h}\langle\rangle$ is insecure

- $\overline{h}\langle n\rangle \mid \overline{h}\langle m\rangle \mid h(x).\mathsf{if}\ x = n\ \mathsf{then}\ \overline{\ell_1}\langle\rangle\ \mathsf{else}\ \overline{\ell_2}\langle\rangle$

  An attack can destroy the nondeterminism causing an interference.

Noninterference in π-calculus

- $h().\ell() \mid \overline{h}\langle\rangle$ is insecure
- $\overline{h}\langle n\rangle \mid \overline{h}\langle m\rangle \mid h(x).\text{if } x = n \text{ then } \overline{\ell_1}\langle\rangle \text{ else } \overline{\ell_2}\langle\rangle$

  An attack can destroy the nondeterminism causing an interference.
- $P = (\boldsymbol{\nu}\ell)\ (\overline{\ell_1}\langle\ell\rangle.\overline{\ell}\langle\rangle.P^?)$ and $Q = (\boldsymbol{\nu}\ell)\ (\overline{h}\langle\ell\rangle.\overline{\ell}\langle\rangle.Q^?)$

  The security of P/Q depends on that of $P^?/Q^?$??

$$P = (\boldsymbol{\nu}\ell)\ \overline{\ell_1}\langle\ell\rangle.\overline{\ell}\langle\rangle.P^? \quad \xrightarrow{(\boldsymbol{\nu}\ell)\overline{\ell_1}\langle\ell\rangle} \quad \overline{\ell}\langle\rangle.P^? \quad \xrightarrow{\overline{\ell}\langle\rangle} \quad P^?$$

$$Q = (\boldsymbol{\nu}\ell)\ \overline{h}\langle\ell\rangle.\overline{\ell}\langle\rangle.Q^? \quad \xrightarrow{(\boldsymbol{\nu}\ell)\overline{h}\langle\ell\rangle} \quad \overline{\ell}\langle\rangle.Q^? \quad \xrightarrow{\overline{\ell}\langle\rangle} \quad Q^?$$

The **low** observer will be able to observe $P^?$, which must be secure.

However, it will not learn ℓ, hence it will never observe $Q^?$

Noninterference in π-calculus

- $h().\ell() \mid \overline{h}\langle\rangle$ is insecure
- $\overline{h}\langle n\rangle \mid \overline{h}\langle m\rangle \mid h(x).\text{if } x = n \text{ then } \overline{\ell_1}\langle\rangle \text{ else } \overline{\ell_2}\langle\rangle$

  An attack can destroy the nondeterminism causing an interference.
- $P = (\boldsymbol{\nu}\ell)\,(\overline{\ell_1}\langle\ell\rangle.\overline{\ell}\langle\rangle.P^?)$ and $Q = (\boldsymbol{\nu}\ell)\,(\overline{h}\langle\ell\rangle.\overline{\ell}\langle\rangle.Q^?)$

  The security of P/Q depends on that of $P^?/Q^?$??

$$P = (\boldsymbol{\nu}\ell)\,\overline{\ell_1}\langle\ell\rangle.\overline{\ell}\langle\rangle.P^? \xrightarrow{(\boldsymbol{\nu}\ell)\overline{\ell_1}\langle\ell\rangle} \overline{\ell}\langle\rangle.P^? \xrightarrow{\overline{\ell}\langle\rangle} P^?$$

$$Q = (\boldsymbol{\nu}\ell)\,\overline{h}\langle\ell\rangle.\overline{\ell}\langle\rangle.Q^? \xrightarrow{(\boldsymbol{\nu}\ell)\overline{h}\langle\ell\rangle} \overline{\ell}\langle\rangle.Q^? \xrightarrow{\overline{\ell}\langle\rangle} Q^?$$

  The low observer will be able to observe $P^?$, which must be secure.

  However, it will not learn ℓ, hence it will never observe $Q^?$
- $(\boldsymbol{\nu}h)(\overline{h} \mid !h.(\overline{k} \mid \overline{h}) \mid k.\overline{\ell})$ is it secure??

Noninterference in π-calculus

We provide a semantic characterization of noninterference
in terms of the process behavior.

- Our characterizations of secure processes admit effective proof techniques (for finite state processes)
- Use a lightweight type system to avoid explicit flows: no safety theorem.
- Our framework also consider a declassification mechanism.

Prefixes

$$\pi \ ::= \ \overline{a}\langle\tilde{b}\rangle \quad \text{output}$$
$$\mid \ a(\tilde{x}{:}\tilde{T}) \quad \text{input}$$

Types

$$T \ ::= \ \delta[\,]$$
$$\mid \ \delta[\tilde{T}]$$

Processes

$$P \ ::= \ \pi.P \quad \text{prefix}$$
$$\mid \ \text{if } a = b \text{ then } P \text{ else } P \quad \text{matching}$$
$$\mid \ P \mid P \quad \text{parallel}$$
$$\mid \ (\boldsymbol{\nu} n : T)P \quad \text{restriction}$$
$$\mid \ !P \quad \text{replication}$$
$$\mid \ \mathbf{0} \quad \text{inactive}$$

(EMPTY TYPE)

$$\frac{}{\vdash \delta[\,]}$$

(CHANNEL TYPE)

$$\frac{\vdash T_i \quad \Lambda(T_i) \preceq \delta}{\vdash \delta[\tilde{T}]}$$

absence of explicit flows

High and Low Contexts

- P is a *σ-low level source* in Γ, denoted $\Gamma \vdash_\sigma P$, if $\Gamma \vdash P$ and $\forall m \in \mathrm{fn}(P)$ it holds $\Lambda(\Gamma(m)) \preceq \sigma$.

- P is a *σ-high level source* in Γ, denoted $\Gamma \vdash^\sigma P$, if for all names a used in P as a subject in an input or an output prefix, $\Lambda(\Gamma(a)) \not\preceq \sigma$.

$$C[\cdot_\Gamma] \;\; ::= \;\; [\cdot_\Gamma] \;\;|\;\; (\boldsymbol{\nu} n{:}T)C[\cdot_\Gamma] \;\;|\;\; C[\cdot_\Gamma] \,|\, P \;\;|\;\; P \,|\, C[\cdot_\Gamma]$$

$C[\cdot_\Gamma]$ is a **σ-low** (resp. **σ-high**) **context** if it is a (Γ'/Γ)-context generated by the grammar above where $\Lambda(T) \preceq \sigma$ (resp. $\Lambda(T) \not\preceq \sigma$) and $\Gamma' \vdash_\sigma P$ (resp. $\Gamma' \vdash^\sigma P$).

$(\boldsymbol{\nu} h)(\,\overline{h}\langle\ell\rangle \mid [\cdot_\Gamma]\,)$ is a σ-high context whereas
$(\boldsymbol{\nu} h)(\,\overline{h}\langle\ell\rangle \mid h(x).\overline{x}\langle\rangle\,) \mid [\cdot_\Gamma]$ is a σ-low context.

Reduction barbed congruence $\Gamma \models P \cong Q$

The largest type-indexed relation over processes which is symmetric,

reduction closed:

if $\Gamma \models P \,\mathcal{R}\, Q$ and $P \xrightarrow{\tau} P'$ then

$\exists Q'$ such that $Q \Longrightarrow Q'$ and $\Gamma \models P' \,\mathcal{R}\, Q'$,

barb preserving:

if $\Gamma \models P \,\mathcal{R}\, Q$ and $\Gamma \models P\!\downarrow_n$ then $\Gamma \models Q\!\Downarrow_n$.

Where $\Gamma \models P\!\downarrow_n$ means $P \xrightarrow{\overline{n}\langle m \rangle}$.

It captures the behaviour of processes

contextual:

if $\Gamma \models P \,\mathcal{R}\, Q$ and $\Gamma' \vdash C[\cdot_\Gamma]$ then

$\Gamma' \models C[P] \,\mathcal{R}\, C[Q]$ for all typed contexts $C[\cdot_\Gamma]$.

σ-Reduction barbed congruence $\quad \Gamma \vDash P \overset{\bullet}{\cong}_\sigma Q$

The largest type-indexed relation over processes which is symmetric,

reduction closed:

if $\Gamma \vDash P \mathcal{R} Q$ and $P \xrightarrow{\tau} P'$ then

$\exists Q'$ such that $Q \Longrightarrow Q'$ and $\Gamma \vDash P' \mathcal{R} Q'$,

σ-barb preserving:

if $\Gamma \vDash P \mathcal{R} Q$ and $\Gamma \vDash P \downarrow_n^\sigma$ then $\Gamma \vDash Q \Downarrow_n^\sigma$.

$\Gamma \vDash P \downarrow_n^\sigma$ when $P \xrightarrow{\overline{n}\langle m \rangle}$ with $\Lambda(\Gamma(n)) \preceq \sigma$.

It captures the σ-low behaviour of processes

σ-contextual:

if $\Gamma \vDash P \mathcal{R} Q$ and $\Gamma' \vdash C[\cdot_\Gamma]$ then

$\Gamma' \vDash C[P] \mathcal{R} C[Q]$ for all σ-low contexts $C[\cdot_\Gamma]$

(interacting with the hole just thorugh σ-channels).

σ-reduction barbed P-congruence $\Gamma \models P \cong_\sigma Q$

$\cong$	equates processes exhibiting the same behaviour
$\dot{\cong}_\sigma$	equates processes exhibiting the same σ-low behaviour
$\cong_\sigma$	equates processes exhibiting the same σ-low behaviour whatever is the surrounding σ-high context

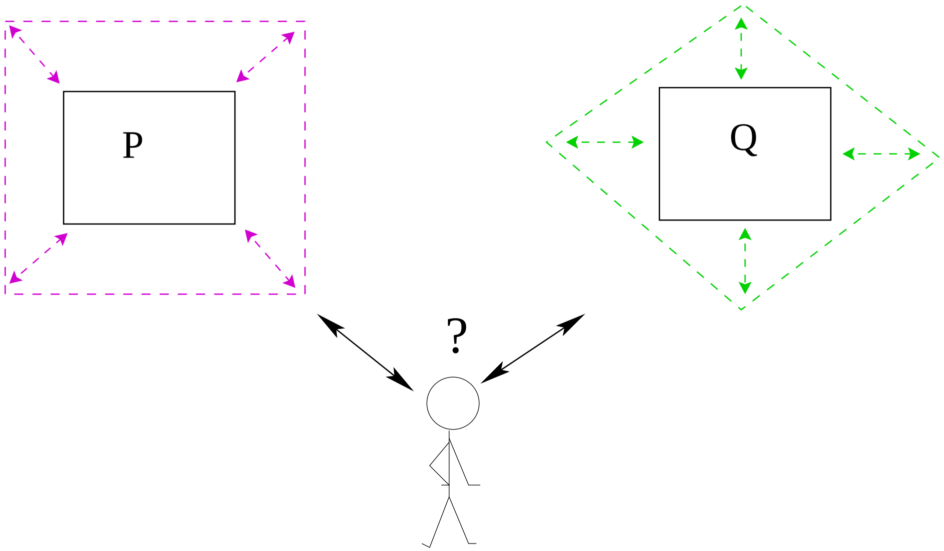
σ-reduction barbed P-congruence $\Gamma \vDash P \cong_\sigma Q$

The largest type-indexed relation over processes which is symmetric,

- *reduction closed, σ-barb preserving*
- *σ-P-contextual:*

  if $P \cong_\sigma Q$, then $C_L[\,C_H^1[\,P\,]\,] \cong_\sigma C_L[\,C_H^2[\,Q\,]\,]$

  for all σ-low contexts C_L and for all σ-high contexts C_H^1, C_H^2



It captures the σ-low behaviour whatever is the surrounding σ-high context

σ-reduction barbed P-congruence $\Gamma \models P \cong_\sigma Q$

The largest type-indexed relation over processes which is symmetric,

- *reduction closed, σ-barb preserving*
- *σ-P-contextual:*

  if $P \ \cong_\sigma \ Q$, then $C_L[\,C_H^1[\,P\,]\,] \ \cong_\sigma \ C_L[\,C_H^2[\,Q\,]\,]$

  for all σ-low contexts C_L and for all σ-high contexts C_H^1, C_H^2

It captures the σ-low behaviour whatever is the surrounding σ-high context

$\Longrightarrow$?? $P \cong_\sigma P$??

σ-reduction barbed P-congruence $\Gamma \models P \cong_\sigma Q$

The largest type-indexed relation over processes which is symmetric,

- *reduction closed, σ-barb preserving*
- *σ-P-contextual:*

  if $P \cong_\sigma Q$, then $C_L[\, C_H^1[\, P\,]\,] \cong_\sigma C_L[\, C_H^2[\, Q\,]\,]$

  for all σ-low contexts C_L and for all σ-high contexts C_H^1, C_H^2

It captures the σ-low behaviour whatever is the surrounding σ-high context

$\Longrightarrow$

P exhibits the same σ-low behaviour whatever is the surrounding σ-high context

when

P is interference-free

P-congruences as Noninterference

$$P \in \mathcal{NI}(\cong_\sigma)$$

iff

$$P \cong_\sigma P$$

iff

$$C_L[\,C_H^1[\,P\,]\,] \;\cong_\sigma\; C_L[\,C_H^2[\,P\,]\,]$$

for all σ-low contexts C_L and for all σ-high contexts C_H^1, C_H^2

$\cong \not\subseteq \cong_\sigma$ $(P_1 = h().\ell())$

$\cong_\sigma \not\subseteq \cong$ $(P_2 = \ell().h(), P_3 = \ell().k())$

If $P \cong_\sigma P$ then $\forall Q$ s.t. $P \cong Q$ it holds $Q \cong_\sigma Q \cong_\sigma P$

Examples

For **INSECURE** processes, simply find distinguishing contexts.

Let be L $\preceq$ H and $\sigma =$ L,

- $P_2 = h(x : T).\,\textsf{if}\ x = n\ \textsf{then}\ \overline{\ell_1}\langle\rangle\ \textsf{else}\ \overline{\ell_2}\langle\rangle$

  (the level of n is irrelevant). Then $P_2 \notin \mathcal{NI}(\cong_\sigma)$ since one can choose $C_H^1 = \overline{h}\langle n\rangle \mid [\,], C_H^2 = C_L = [\,]$ and observe that $P_2 \not\cong_\sigma P_2 \mid \overline{h}\langle n\rangle$.

For **INSECURE** processes, simply find distinguishing contexts.

Let be $\mathsf{L} \preceq \mathsf{H}$ and $\sigma = \mathsf{L}$,

- $P_2 = h(x:T).\ \mathsf{if}\ x = n\ \mathsf{then}\ \overline{\ell_1}\langle\rangle\ \mathsf{else}\ \overline{\ell_2}\langle\rangle$

  (the level of n is irrelevant). Then $P_2 \notin \mathcal{NI}(\cong_\sigma)$ since one can choose $C_H^1 = \overline{h}\langle n\rangle \mid [\,], C_H^2 = C_L = [\,]$ and observe that $P_2 \ncong_\sigma P_2 \mid \overline{h}\langle n\rangle$.

- $P_3 = \overline{h}\langle n\rangle \mid \overline{h}\langle m\rangle \mid h(x).\ \mathsf{if}\ x = n\ \mathsf{then}\ \overline{\ell_1}\langle\rangle\ \mathsf{else}\ \overline{\ell_2}\langle\rangle$,

  where x can be nondeterministically substituted either with n or m. An external attack can destroy the nondeterminism causing an interference: let $C_H^1 = h(y).h(z).\overline{h}\langle n\rangle \mid [\,], C_H^2 = C_L = [\,]$, then $P_3 \ncong_\sigma P_3 \mid h(y).h(z).\overline{h}\langle n\rangle$. Hence $P_3 \notin \mathcal{NI}(\cong_\sigma)$.

P-congruences as Noninterference

$$P \in \mathcal{NI}(\cong_\sigma)$$

iff

$$P \cong_\sigma P$$

iff

$$C_L[\,C_H^1[\,P\,]\,] \;\cong_\sigma\; C_L[\,C_H^2[\,P\,]\,]$$

for all σ-low contexts C_L and for all σ-high contexts C_H^1, C_H^2 !? !?

Looking for a proof technique

Define a LTS of *typed actions* over configurations $\Gamma \triangleright P$ (that means $\Gamma \vdash P$)

$$\Gamma \triangleright P \xrightarrow{\alpha}_{\delta} \Gamma' \triangleright P'$$

action of
level (at most) δ

(OUT)

$$\frac{\Gamma \vdash n : \delta_1[T] \quad \delta_1 \preceq \delta}{\Gamma \triangleright \overline{n}\langle m\rangle.P \xrightarrow{\overline{\mathbf{n}}\langle \mathbf{m}\rangle}_{\delta} \Gamma \triangleright P}$$

(IN)

$$\frac{\Gamma \vdash n : \delta_1[T] \quad \Gamma \vdash m : T \quad \delta_1 \preceq \delta}{\Gamma \triangleright n(x{:}T).P \xrightarrow{\mathbf{n}(\mathbf{m})}_{\delta} \Gamma \triangleright P\{x := m\}}$$

A proof technique for $\cong_\sigma$

$$\frac{\Gamma, m : T \triangleright P \xrightarrow{n(m)}_\delta \Gamma' \triangleright P'}{\Gamma \triangleright P \xrightarrow{(\boldsymbol{\nu}\mathbf{m}:\mathbf{T})\,\mathbf{n}(\mathbf{m})}_\delta \Gamma' \triangleright P'}$$

$$\frac{\Gamma, m{:}T \triangleright P \xrightarrow{\overline{n}\langle m\rangle}_\delta \Gamma' \triangleright P' \quad m \neq n}{\Gamma \triangleright (\boldsymbol{\nu} m{:}T)P \xrightarrow{(\boldsymbol{\nu}\mathbf{m}:\mathbf{T})\,\overline{\mathbf{n}}\langle\mathbf{m}\rangle}_\delta \Gamma' \triangleright P'}$$

$$\frac{\Gamma \triangleright P \xrightarrow{\alpha}_\delta \Gamma' \triangleright P' \; \mathrm{bn}(\alpha) \cap \mathrm{fn}(Q) = \emptyset}{\Gamma \triangleright P \mid Q \xrightarrow{\alpha}_\delta \Gamma' \triangleright P' \mid Q}$$

$$\frac{P \xrightarrow{\tau} P'}{\Gamma \triangleright P \xrightarrow{\tau}_\delta \Gamma \triangleright P'}$$

$$\frac{\Gamma, n{:}T \triangleright P \xrightarrow{\alpha}_\delta \Gamma', n{:}T \triangleright P' \quad n \notin \mathrm{fn}(\alpha) \cup \mathrm{bn}(\alpha)}{\Gamma \triangleright (\boldsymbol{\nu} n{:}T)P \xrightarrow{\alpha}_\delta \Gamma' \triangleright (\boldsymbol{\nu} n{:}T)P'}$$

$$\frac{\Gamma \triangleright P \xrightarrow{\alpha}_\delta \Gamma' \triangleright P'}{\Gamma \triangleright !P \xrightarrow{\alpha}_\delta \Gamma' \triangleright P' \mid !P}$$

Noninterference through a PER model

Partial bisimilarity on σ-low actions:

it is the largest symmetric relation $\dot{\approx}_\sigma$ s.t. whenever $P \dot{\approx}_\sigma Q$

- on observable (σ-low) actions it behaves as bisimilarity:
  if $P \xrightarrow{\alpha}_\sigma P'$, then $\exists Q'$ s.t. $Q \xRightarrow{\hat{\alpha}}_\sigma Q'$ with $Q' \dot{\approx}_\sigma P'$.
- σ-high actions are simulated by internal transitions:

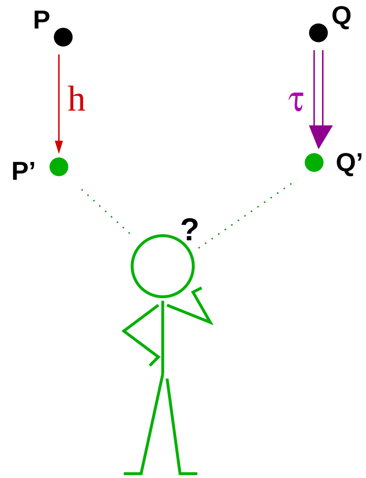
Noninterference through a PER model

Partial bisimilarity on σ-low actions:

it is the largest symmetric relation $\dot{\approx}_\sigma$ s.t. whenever $P \;\dot{\approx}_\sigma\; Q$

- on observable (σ-low) actions it behaves as bisimilarity:
  if $P \xrightarrow{\alpha}_\sigma P'$, then $\exists Q'$ s.t. $Q \xRightarrow{\hat{\alpha}}_\sigma Q'$ with $Q' \;\dot{\approx}_\sigma\; P'$.

- σ-high actions are simulated by internal transitions:



Noninterference through a PER model

Partial bisimilarity on σ-low actions:

it is the largest symmetric relation $\dot{\approx}_\sigma$ s.t. whenever $P \dot{\approx}_\sigma Q$

- on observable (σ-low) actions it behaves as bisimilarity:
  if $P \xrightarrow{\alpha}_\sigma P'$, then $\exists Q'$ s.t. $Q \xRightarrow{\hat{\alpha}}_\sigma Q'$ with $Q' \dot{\approx}_\sigma P'$.

- σ-high actions are simulated by internal transitions:
  if $\Gamma \triangleright P \xrightarrow{\alpha}{}^{\sigma} \Gamma' \triangleright P'$ with $\alpha \in \{(\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\,\overline{n}\langle\tilde{m}\rangle, (\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\,n(\tilde{m})\}$
  where $\tilde{p} : \tilde{T} = \tilde{p}_1{:}\tilde{T}_1,\ \tilde{p}_2{:}\tilde{T}_2$ such that $\Lambda(\tilde{T}_1) \not\preceq \sigma$, and $\Lambda(\tilde{T}_2) \preceq \sigma$,
  then $\exists\, Q'$ s. t. $\Gamma \triangleright Q \Longrightarrow \Gamma \triangleright Q'$ with
  $\Gamma, \tilde{p}_1{:}\tilde{T}_1 \vDash Q' \dot{\approx}_\sigma (\boldsymbol{\nu}\tilde{p}_2{:}\tilde{T}_2)P'$.

$$P_1 = (\boldsymbol{\nu}\ell)(\overline{h}\langle\ell\rangle.\overline{\ell}\langle\rangle.R) \qquad P_2 = (\boldsymbol{\nu}k)(\overline{h}\langle k\rangle.\overline{k}\langle\rangle.R)$$

Time for an assessment

P is secure

iff $P \in \mathcal{NI}(\cong_\sigma)$ iff $P \mathrel{\dot{\approx}_\sigma} P$

- almost independent of typing constraints
- compositionality results:

  if $P, Q \in \mathcal{NI}(\cong_\sigma)$ then

  $P \mid Q \in \mathcal{NI}(\cong_\sigma),\ \ !P \in \mathcal{NI}(\cong_\sigma),\ \ (\boldsymbol{\nu} n)P \in \mathcal{NI}(\cong_\sigma)$

Time for an assessment

P is secure

iff $P \in \mathcal{NI}(\cong_\sigma)$ iff $P \mathrel{\dot{\approx}_\sigma} P$

- almost independent of typing constraints
- compositionality results:

  if $P, Q \in \mathcal{NI}(\cong_\sigma)$ then

  $P \mid Q \in \mathcal{NI}(\cong_\sigma),\ \ !P \in \mathcal{NI}(\cong_\sigma),\ \ (\boldsymbol{\nu} n)P \in \mathcal{NI}(\cong_\sigma)$

$\mathcal{NI}(\cong_\sigma)$ is a strong security property!!

... well suited in open networks

... but what about the expressivity and flexibility of secure systems?

Declassification

To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards.

By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

Which expressions are downgraded?

Declassification

To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards.

By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

Which expressions are downgraded?

- downgrade names, or values, as in imperative languages: $\overline{\ell}\langle\, \mathsf{dec}(h)\,\rangle.P$ or $\overline{\ell}\langle\, \mathsf{dec}(F(h_1, ..., h_k))\,\rangle.P$

Declassification

To increase the flexibility of the system, we add a declassification mechanism that coerces the security level of (specific) expressions downwards.

By declassifying certain expressions, the programmer may intentionally violate noninterference, but only in a controlled way.

Which expressions are downgraded?

- downgrade names, or values, as in imperative languages:
  $\overline{\ell}\langle\, \mathsf{dec}(h)\,\rangle.P$ or $\overline{\ell}\langle\, \mathsf{dec}(F(h_1, ..., h_k))\,\rangle.P$
- downgrade process actions:
  $\mathsf{dec}\, h(x).P$ and $\overline{\mathsf{dec}\, h}\langle n\rangle.P$ stand for a declassified read/write action over the channel h, which can still be used as a secret channel!

Declassifying actions: Dec π-calculus

- $\mathsf{dec}_\delta\; n(x).P$ and $\overline{\mathsf{dec}_\delta\; n}\langle m\rangle.P$ represent "escape hatches" for information release: they allow info arising from these actions to flow down up to level δ.
- Both users of the channel must agree to downgrade the communication:

$$\mathsf{dec}_\delta\; n(x).P \mid \overline{\mathsf{dec}_\delta\; n}\langle m\rangle.Q \quad\longrightarrow\quad P\{m/x\} \mid Q$$

- Only programmers may enable the downgrading of secret information to an observable level; no external entities can synch on such declassified actions.

Controlled Information Release

The theory of P-congruences scales to the $\mathsf{Dec}\ \pi$-calculus:

- $\cong_\sigma^{\mathsf{dec}}$ is the largest relation which is symmetric, reduction closed, σ-barb preserving and σ-contextual, where σ-low and σ-high context cannot fire declassified communications.

Controlled Information Release

The theory of P-congruences scales to the Dec π-calculus:

- $\cong_\sigma^{\mathsf{dec}}$ is the largest relation which is symmetric, reduction closed, σ-barb preserving and σ-contextual, where σ-low and σ-high context cannot fire declassified communications.

- The downgrading does not affect the level of typed actions, it only has an impact on the admissible info flows: $\Gamma \triangleright \overline{\mathsf{dec}_{\mathsf{L}}\, h}\langle m \rangle.P \xrightarrow{\overline{\mathsf{dec}_{\mathsf{L}}\, \mathsf{h}}\langle \mathsf{m} \rangle}{}_{\mathsf{H}} \Gamma \triangleright P$

Controlled Information Release

The theory of P-congruences scales to the Dec π-calculus:

- $\cong_\sigma^{\mathsf{dec}}$ is the largest relation which is symmetric, reduction closed, σ-barb preserving and σ-contextual, where σ-low and σ-high context cannot fire declassified communications.

- The downgrading does not affect the level of typed actions, it only has an impact on the admissible info flows: $\Gamma \triangleright \overline{\mathsf{dec}_{\mathsf{L}}\, h}\langle m \rangle.P \xrightarrow{\overline{\mathsf{dec}_{\mathsf{L}}\, \mathsf{h}}\langle \mathsf{m} \rangle}{}_{\mathsf{H}} \Gamma \triangleright P$

- $\dot{\approx}_\sigma^{\mathsf{dec}}$ scales to Dec π:
  - σ-low actions must be precisely matched
  - σ-high actions must be matched by τ-steps
  - σ-high *declassified* actions need not to be matched by τ-steps since they represent an explicitly allowed info flow.

- $P \in \mathcal{NI}(\cong_\sigma^{\mathsf{dec}})$ iff $P \dot{\approx}_\sigma^{\mathsf{dec}} P$

- $P = \overline{h} \mid h.\ell$ is obviously insecure, whereas $P' = \overline{\text{dec } h} \mid \text{dec } h.\ell$ can be shown to be a secure process such that $\Gamma \vDash P' \cong_\sigma \ell$. On the other hand, $P_1 = \overline{k}.(\overline{\text{dec } h} \mid \text{dec } h.\ell)$ is not secure since the observable action ℓ depends on the firing of the high action $\overline{k}$.

Downgrading

- $P = \overline{h} \mid h.\ell$ is obviously insecure, whereas $P' = \overline{\mathsf{dec}\ h} \mid \mathsf{dec}\ h.\ell$ can be shown to be a secure process such that $\Gamma \models P' \cong_\sigma \ell$. On the other hand, $P_1 = \overline{k}.(\overline{\mathsf{dec}\ h} \mid \mathsf{dec}\ h.\ell)$ is not secure since the observable action ℓ depends on the firing of the high action $\overline{k}$.

- $P = \overline{\mathsf{dec}\ h}.\ h.\ \overline{\mathsf{dec}\ h} \mid \mathsf{dec}\ h.\ \overline{\ell}.\ \overline{h}.\ \mathsf{dec}\ h$ is **secure**: a high channel can be used as a secure channel even after a downgrading,

- $P = \overline{h} \mid h.\ell$ is obviously insecure, whereas $P' = \overline{\text{dec } h} \mid \text{dec } h.\ell$ can be shown to be a secure process such that $\Gamma \models P' \cong_\sigma \ell$. On the other hand, $P_1 = \overline{k}.(\overline{\text{dec } h} \mid \text{dec } h.\ell)$ is not secure since the observable action ℓ depends on the fire of the high action $\overline{k}$.

- $P = \overline{\text{dec } h}.\, h.\, \overline{\text{dec } h} \mid \text{dec } h.\, \overline{\ell}.\, \overline{h}.\, \text{dec } h$ is **secure**: a high channel can be used as a secure channel even after a downgrading,

- $P = h(x).\text{if } x = n \text{ then } \overline{\ell_1}\langle\rangle \text{ else } \overline{\ell_2}\langle\rangle \mid \overline{h}\langle n\rangle \mid \overline{h}\langle m\rangle$ is **insecure**, but by declassifying the communication on the channel h, we obtain $P' = \text{dec } h(x).\text{if } x{=}n \text{ then } \overline{\ell_1}\langle\rangle \text{ else } \overline{\ell_2}\langle\rangle \mid \overline{\text{dec } h}\langle n\rangle \mid \overline{\text{dec } h}\langle m\rangle$ which is **secure**.

Conclusions

- a rich and elegant theory of noninterference intrinsic of the π-calculus, where types play a limited role
- a sound and complete characterization leading to efficient verification techniques.
- we integrated the π-calculus with a downgrading mechanism that allows a controlled information release which scales to noninterference.

$$\frac{\Gamma \vdash \overline{a}\langle \tilde{b} \rangle.P \quad \Gamma \vdash a : \delta_1[\tilde{T}]}{\Gamma \vdash \overline{\mathsf{dec}a}\langle \tilde{b} \rangle.P}\ \delta \prec \delta_1 \qquad \frac{\Gamma \vdash a(\tilde{x} : \tilde{T}).P \quad \Gamma \vdash a : \delta_1[\tilde{T}]}{\Gamma \vdash \mathsf{dec}a(\tilde{x} : \tilde{T}).P}\ \delta \prec \delta_1$$

$$\overline{\mathsf{dec}n}\langle \tilde{m} \rangle.P \xrightarrow{\overline{\mathsf{dec}n}\langle \tilde{m} \rangle} P \qquad \mathsf{dec}n(\tilde{x}{:}\tilde{T}).P \xrightarrow{\mathsf{dec}n(\tilde{m})} P\{\tilde{x} := \tilde{m}\}$$

$$\frac{P \xrightarrow{(\boldsymbol{\nu}\tilde{p}:\tilde{T})\,\overline{\mathsf{dec}n}\langle \tilde{m} \rangle} P' \quad q \neq n \quad q \in \tilde{m}}{(\boldsymbol{\nu}q{:}T)P \xrightarrow{(\boldsymbol{\nu}q:T)(\boldsymbol{\nu}\tilde{p}:\tilde{T})\,\overline{\mathsf{dec}n}\langle \tilde{m} \rangle} P'}$$

$$\frac{P \xrightarrow{(\boldsymbol{\nu}\tilde{p}:\tilde{T})\,\overline{\mathsf{dec}n}\langle \tilde{m} \rangle} P' \quad Q \xrightarrow{\mathsf{dec}n(\tilde{m})} Q' \quad \tilde{p} \cap \mathrm{fn}(Q) = \emptyset}{P \mid Q \xrightarrow{\tau} (\boldsymbol{\nu}\tilde{p} : \tilde{T})(P' \mid Q')}$$

$$\frac{\Gamma \vdash n : \delta_1[\tilde{T}]}{\Gamma \triangleright \overline{\mathsf{dec}_{\delta_2} n}\langle \tilde{m} \rangle.P \xrightarrow{\overline{\mathsf{dec}_{\delta_2} n}\langle \tilde{m} \rangle}_{\delta} \Gamma \triangleright P} \quad \delta_1 \preceq \delta$$

$$\frac{\Gamma \vdash n : \delta_1[\tilde{T}] \quad \Gamma \vdash \tilde{m} : \tilde{T}}{\Gamma \triangleright \mathsf{dec}_{\delta_2} n(\tilde{x}{:}\tilde{T}).P \xrightarrow{\mathsf{dec}_{\delta_2} n(\tilde{m})}_{\delta} \Gamma \triangleright P\{\tilde{x} := \tilde{m}\}} \quad \delta_1 \preceq \delta$$

$$\frac{\Gamma, q{:}T \triangleright P \xrightarrow{(\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\ \mathsf{dec}_{\delta_1} n(\tilde{m})}_{\delta} \Gamma' \triangleright P' \quad q \neq n, \tilde{p} \quad q \in \tilde{m}}{\Gamma \triangleright P \xrightarrow{(\boldsymbol{\nu} q{:}T)(\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\ \mathsf{dec}_{\delta_1} n(\tilde{m})}_{\delta} \Gamma' \triangleright P'}$$

$$\frac{\Gamma, q{:}T \triangleright P \xrightarrow{(\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\ \overline{\mathsf{dec}_{\delta_1} n}\langle \tilde{m} \rangle}_{\delta} \Gamma' \triangleright P' \quad q \neq n, \tilde{p} \quad q \in \tilde{m}}{\Gamma \triangleright (\boldsymbol{\nu} q{:}T)P \xrightarrow{(\boldsymbol{\nu} q{:}T)(\boldsymbol{\nu}\tilde{p}{:}\tilde{T})\ \overline{\mathsf{dec}_{\delta_1} n}\langle \tilde{m} \rangle}_{\delta} \Gamma' \triangleright P'}$$

$$\overline{n}\langle m\rangle.P \xrightarrow{\overline{n}\langle m\rangle} P \qquad\qquad n(x:T).P \xrightarrow{n(m)} P\{x := m\}$$

$$\frac{P \xrightarrow{\overline{\mathbf{n}}\langle\mathbf{m}\rangle} P' \quad Q \xrightarrow{\mathbf{n}(\mathbf{m})} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \qquad\qquad \frac{P \xrightarrow{\overline{n}\langle m\rangle} P' \quad m \neq n}{(\boldsymbol{\nu} m{:}T)P \xrightarrow{(\boldsymbol{\nu} m{:}T)\,\overline{n}\langle m\rangle} P'}$$

$$\frac{P \xrightarrow{(\boldsymbol{\nu} m{:}T)\,\overline{n}\langle m\rangle} P' \quad Q \xrightarrow{n(m)} Q' \quad m \notin \mathrm{fn}(Q)}{P \mid Q \xrightarrow{\tau} (\boldsymbol{\nu} m{:}T)(P' \mid Q')}$$

$$\text{if } n = n \text{ then } P \text{ else } Q \xrightarrow{\tau} P \qquad \text{if } n = m \text{ then } P \text{ else } Q \xrightarrow{\tau} Q$$

(PAR)

$$\frac{P \xrightarrow{\alpha} P' \quad \mathrm{bn}(\alpha) \cap \mathrm{fn}(Q) = \emptyset}{P \mid Q \xrightarrow{\alpha} P' \mid Q}$$

(RES)

$$\frac{P \xrightarrow{\alpha} P' \quad n \notin \mathrm{fn}(\alpha) \cup \mathrm{bn}(\alpha)}{(\boldsymbol{\nu} n{:}T)P \xrightarrow{\alpha} (\boldsymbol{\nu} n{:}T)P'}$$

(REP-ACT)

$$\frac{P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P' \mid !P}$$