Simple noninterference by normalization

Carlos Tomé Cortiñas

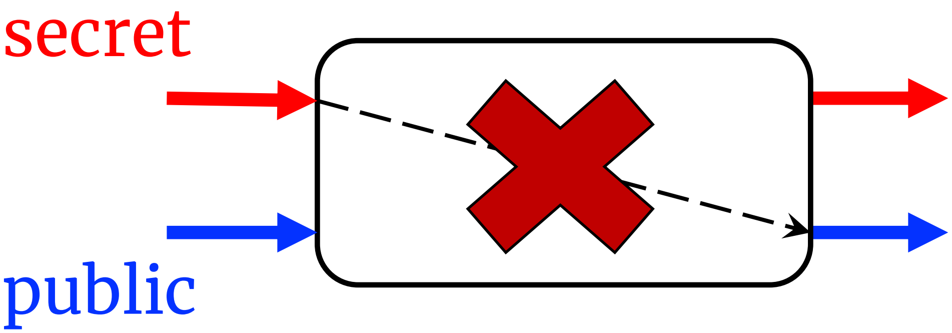
Nachiappan Valliappan

{web:sec}

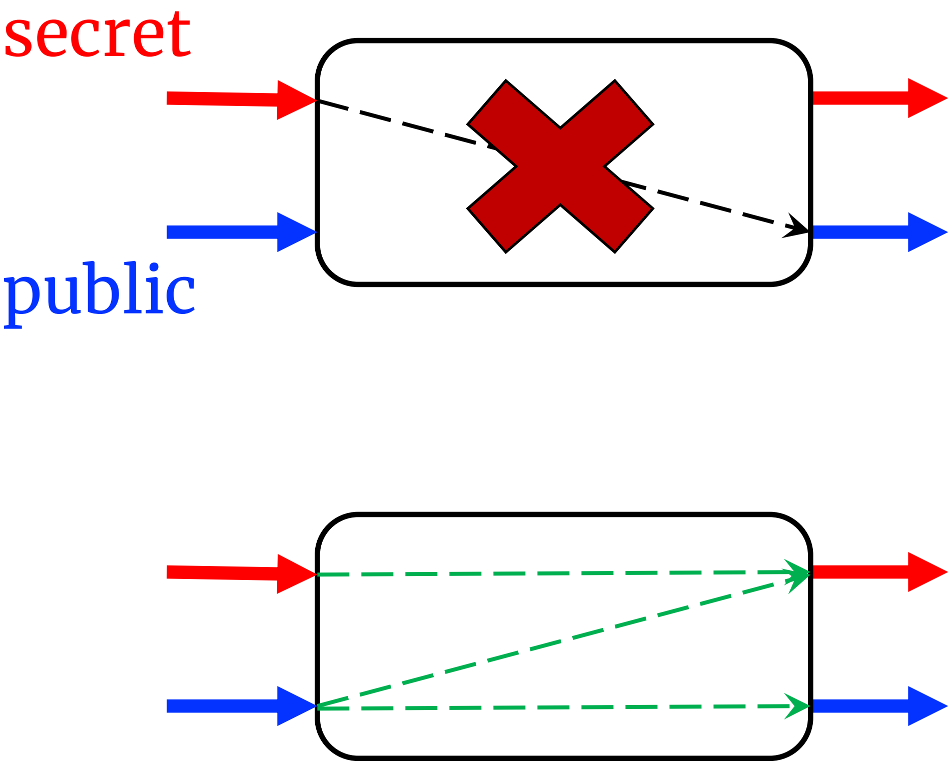
CHALMERS
UNIVERSITY OF TECHNOLOGY

OCTOPI

What is noninterference?



What is noninterference?



Static language-based security

$$\boxed{\Gamma \vdash t : \tau}$$

Return

$$\frac{\Gamma \vdash t : \tau}{\Gamma \vdash \mathsf{return}\ t : \mathsf{S}\ \ell\ \tau}$$

Let

$$\frac{\Gamma \vdash t : \mathsf{S}\ \ell\ \tau_1 \qquad \Gamma, x : \tau_1 \vdash s : \mathsf{S}\ \ell\ \tau_2}{\Gamma \vdash \mathsf{let}\ x = t\ \mathsf{in}\ s : \mathsf{S}\ \ell\ \tau_2}$$

Up

$$\frac{\Gamma \vdash t : \mathsf{S}\ \ell_{\mathrm{L}}\ \tau \qquad \ell_{\mathrm{L}} \sqsubseteq \ell_{\mathrm{H}}}{\Gamma \vdash \mathsf{up}\ t : \mathsf{S}\ \ell_{\mathrm{H}}\ \tau}$$

How to prove noninterference?

```
f : S H a -> S L b
```

How to prove noninterference?

```
f : S H a -> S L b
```

1. Dynamically

$$f\,(sa_1) \rightsquigarrow pb$$

$$f\,(sa_2) \rightsquigarrow pb$$

…

How to prove noninterference?

```
f : S H a -> S L b
```

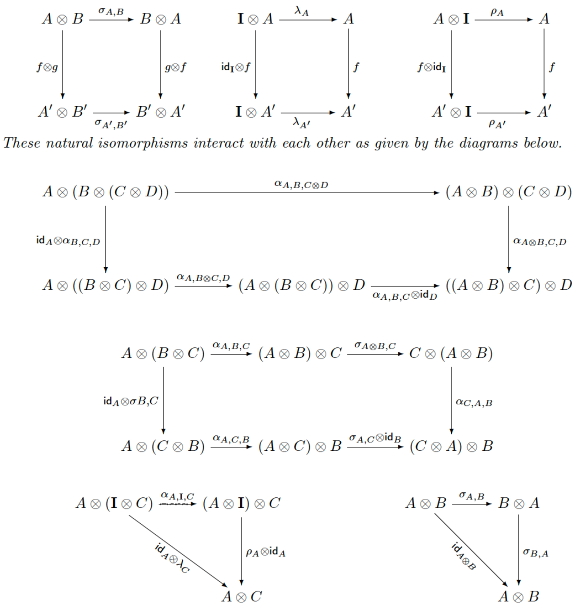
1. Dynamically

$f\,(sa_1) \rightsquigarrow pb$

$f\,(sa_2) \rightsquigarrow pb$

…

2. Denotationally



$$\begin{tikzcd}
A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[d, "f \otimes g"'] & B \otimes A \arrow[d, "g \otimes f"] & \mathbf{I} \otimes A \arrow[r, "\lambda_A"] \arrow[d, "\mathsf{id}_{\mathbf{I}} \otimes f"'] & A \arrow[d, "f"] & A \otimes \mathbf{I} \arrow[r, "\rho_A"] \arrow[d, "f \otimes \mathsf{id}_{\mathbf{I}}"'] & A \arrow[d, "f"] \\
A' \otimes B' \arrow[r, "\sigma_{A',B'}"'] & B' \otimes A' & \mathbf{I} \otimes A' \arrow[r, "\lambda_{A'}"'] & A' & A' \otimes \mathbf{I} \arrow[r, "\rho_{A'}"'] & A'
\end{tikzcd}$$

These natural isomorphisms interact with each other as given by the diagrams below.

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[rr, "\alpha_{A,B,C \otimes D}"] \arrow[d, "\mathsf{id}_A \otimes \alpha_{B,C,D}"'] & & (A \otimes B) \otimes (C \otimes D) \arrow[d, "\alpha_{A \otimes B,C,D}"] \\
A \otimes ((B \otimes C) \otimes D) \arrow[r, "\alpha_{A,B \otimes C,D}"] & (A \otimes (B \otimes C)) \otimes D \arrow[r, "\alpha_{A,B,C} \otimes \mathsf{id}_D"'] & ((A \otimes B) \otimes C) \otimes D
\end{tikzcd}$$

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "\mathsf{id}_A \otimes \sigma B{,}C"'] & (A \otimes B) \otimes C \arrow[r, "\sigma_{A \otimes B,C}"] & C \otimes (A \otimes B) \arrow[d, "\alpha_{C,A,B}"] \\
A \otimes (C \otimes B) \arrow[r, "\alpha_{A,C,B}"] & (A \otimes C) \otimes B \arrow[r, "\sigma_{A,C} \otimes \mathsf{id}_B"] & (C \otimes A) \otimes B
\end{tikzcd}$$

$$\begin{tikzcd}
A \otimes (\mathbf{I} \otimes C) \arrow[r, dashed, "\alpha_{A,\mathbf{I},C}"] \arrow[dr, "\mathsf{id}_A \oplus \lambda_C"'] & (A \otimes \mathbf{I}) \otimes C \arrow[d, "\rho_A \otimes \mathsf{id}_A"] & A \otimes B \arrow[r, "\sigma_{A,B}"] \arrow[dr, "\mathsf{id}_{A \oplus B}"'] & B \otimes A \arrow[d, "\sigma_{B,A}"] \\
& A \otimes C & & A \otimes B
\end{tikzcd}$$

Can we prove it statically?

```
f : S H Bool -> S L Bool

f sb = return (not false)
```

or

```
f sb = snd (let b = sb in b
           , return false)
```

definitions of `f` maybe arbitrarily complex...

Can we prove it statically?

```
f : S H Bool -> S L Bool

f sb = return true
```

or

```
f sb = return false
```

...but normal forms of `f` are very simple!

Static semantics

$$\boxed{\Gamma \vdash t_1 \approx t_2 : \tau}$$

β-S

$$\frac{\Gamma \vdash t_1 : \tau \qquad \Gamma, x : \tau \vdash t_2 : \mathsf{S}\ \ell\ \tau}{\Gamma \vdash \mathsf{let}\ x = (\mathsf{return}\ t_1)\ \mathsf{in}\ t_2 \approx t_2\,[x/t_1] : \mathsf{S}\ \ell\ \tau}$$

η-S

$$\frac{\Gamma \vdash t : \mathsf{S}\ \ell\ \tau}{\Gamma \vdash t \approx \mathsf{let}\ x = t\ \mathsf{in}\ (\mathsf{return}\ x) : \mathsf{S}\ \ell\ \tau}$$

+ more S-monad rules + standard beta-eta

Key Idea

Normalize programs & prove noninterference by showing that ***all*** *normal forms from secret → public are* ***constant***

The story

- *Normalization by Evaluation* for λsec (STLC + monads graded by security levels)

- Proof of noninterference for λsec using syntactic properties of normal forms (e.g., subformula prop., eta-long form, etc.)

Link: nachivpn.me/nibnbe.pdf