Sicurezza di programmi multi-threaded distribuiti

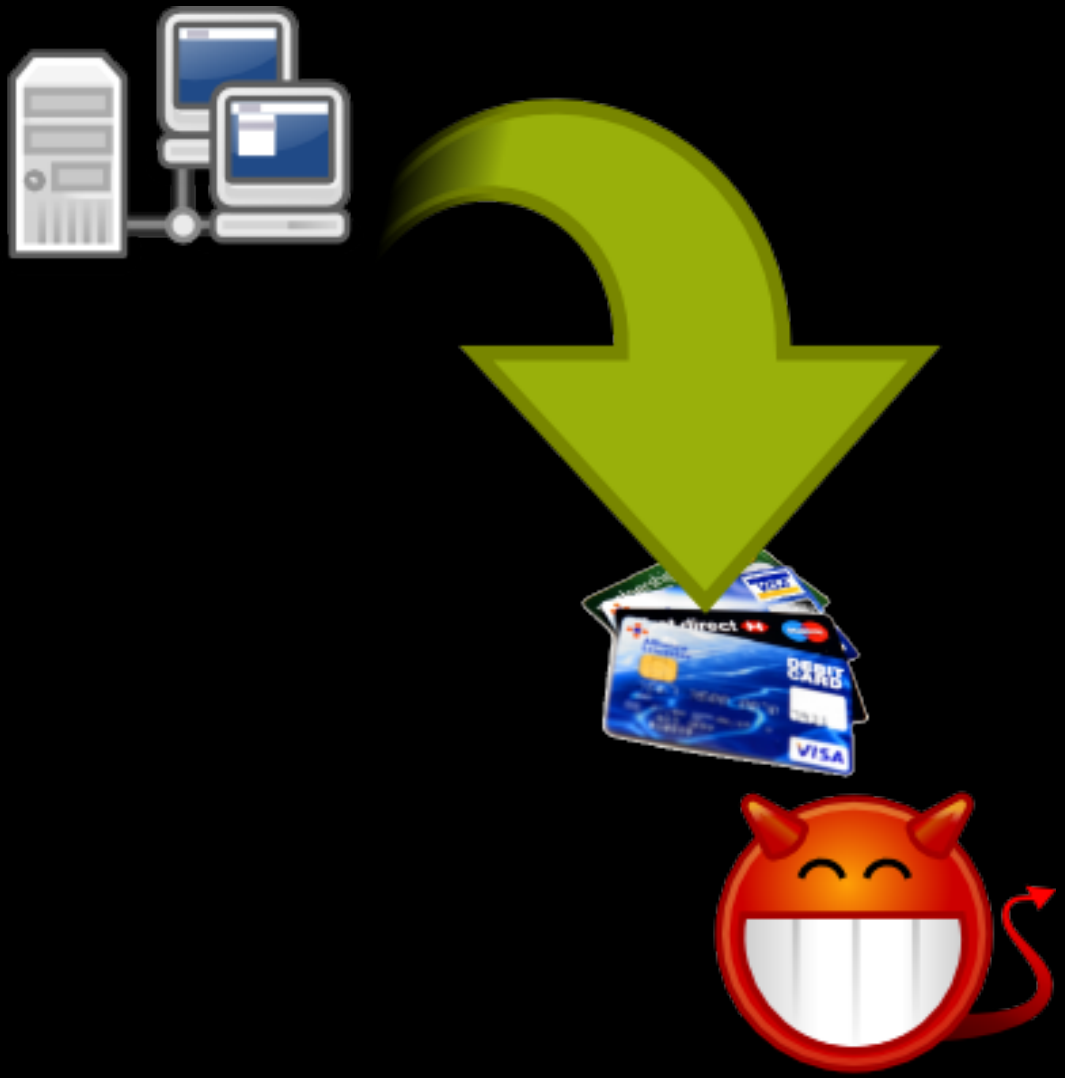
Matteo Centenaro e Riccardo Focardi

Terzo Workshop di Dipartimento
17 Aprile 2008

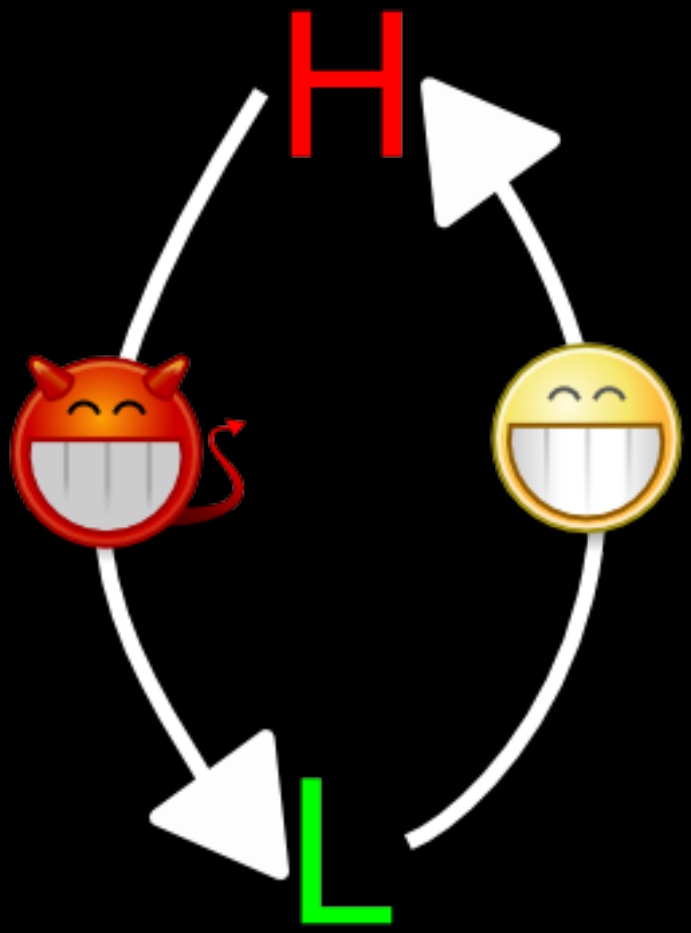
Dipartimento di Informatica

SICUREZZA?


WWW
VISA


VISA

Information Flow



Un attaccante distingue/vede solo la parte pubblica

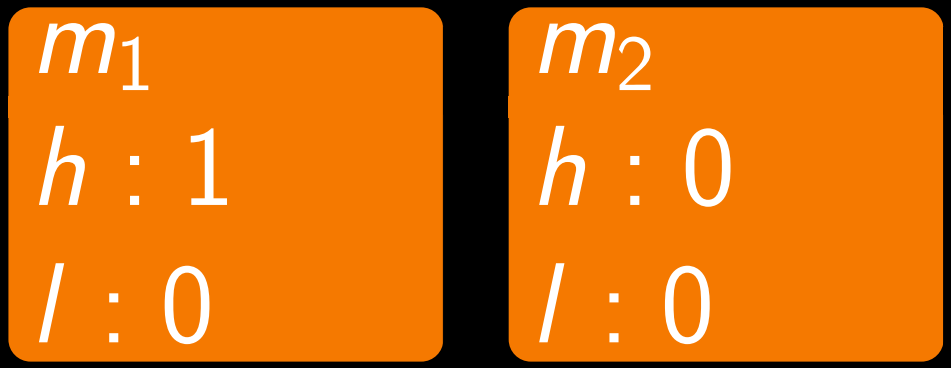
$m_1 =_L m_2$

m_1	m_2
$h : 0$	$h : 1$
$l_1 : 2$	$l_1 : 2$
$l_2 : 0$	$l_2 : 0$

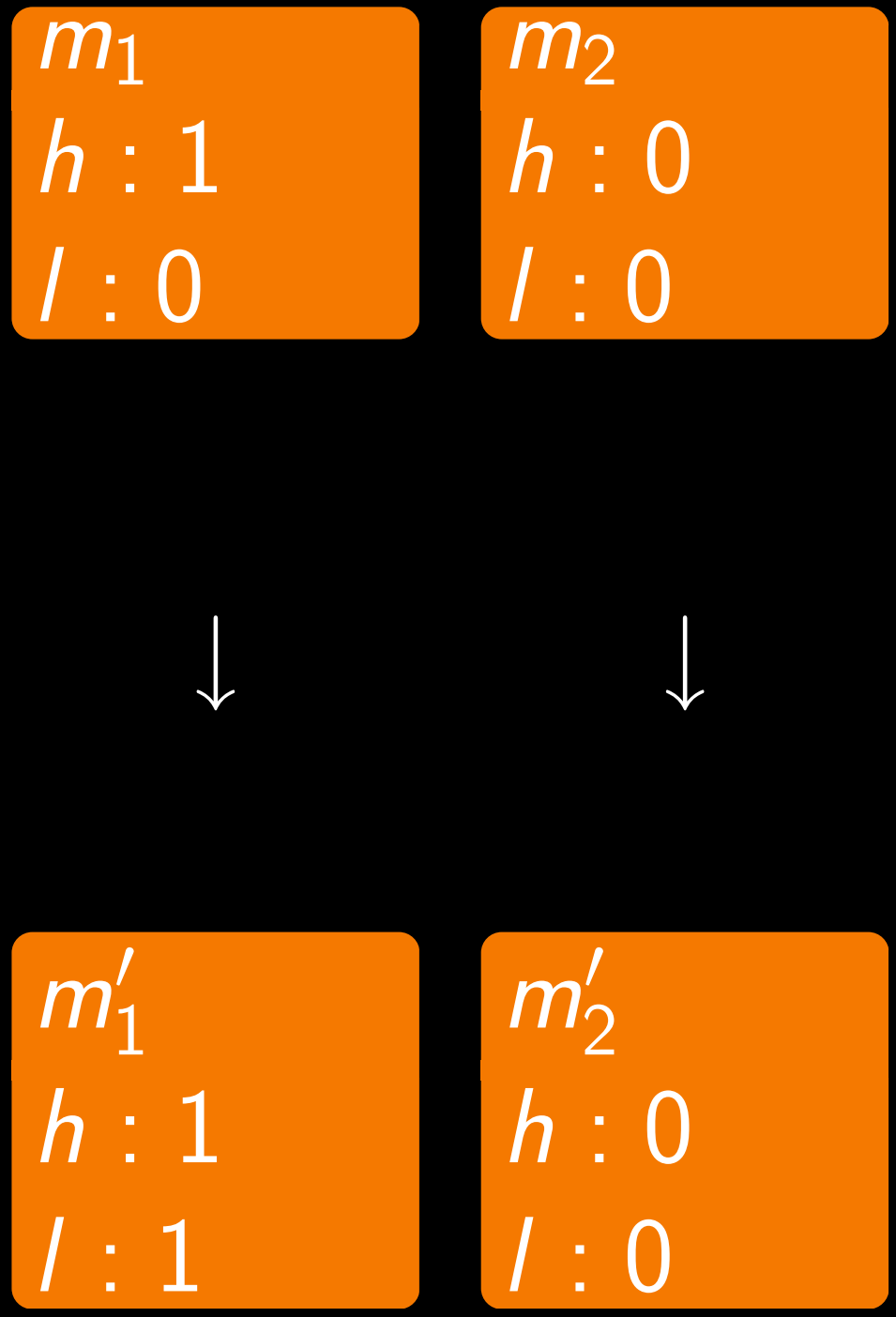
Un programma $\mathcal{C}$ è sicuro solo se non produce memorie distinguibili

Noninterference

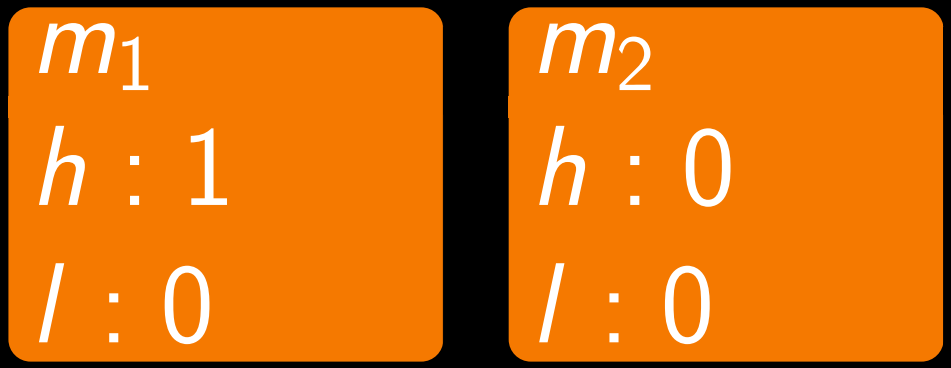
$\forall m_1, m_2.\ m_1 =_L m_2,$
$\langle C, m_1 \rangle \longrightarrow^* m_1', \langle C, m_2 \rangle \longrightarrow^* m_2'$ e
$m_1' =_L m_2'$



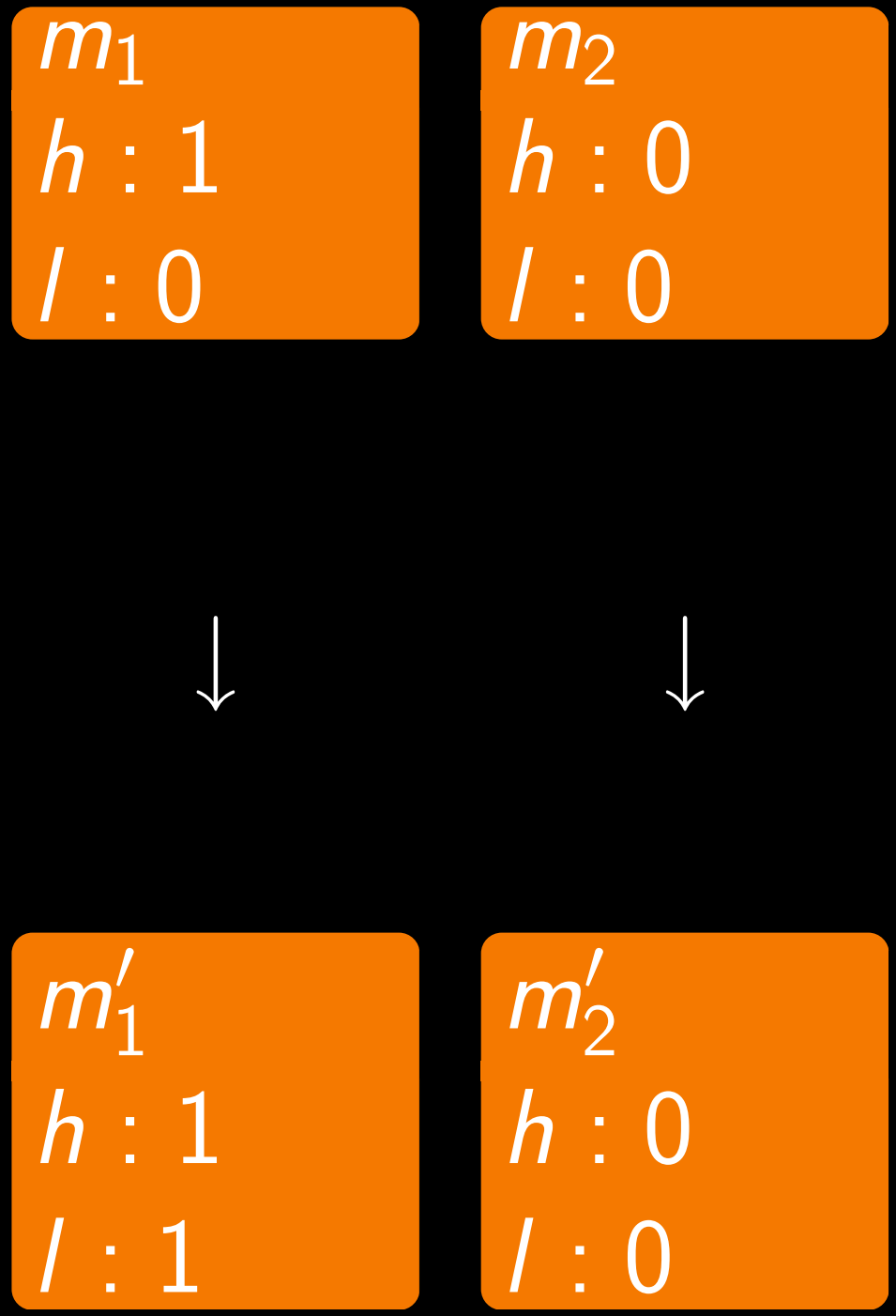

```
l := h
```


m_1
$h : 1$
$l : 0$
m_2
$h : 0$
$l : 0$
l := h
NON SICURO
m'_1
$h : 1$
$l : 1$
m'_2
$h : 0$
$l : 0$

```
if (h) then
     l := 1
else
     l := 0
```



```
if (h) then
     l := 1
else
     l := 0
```



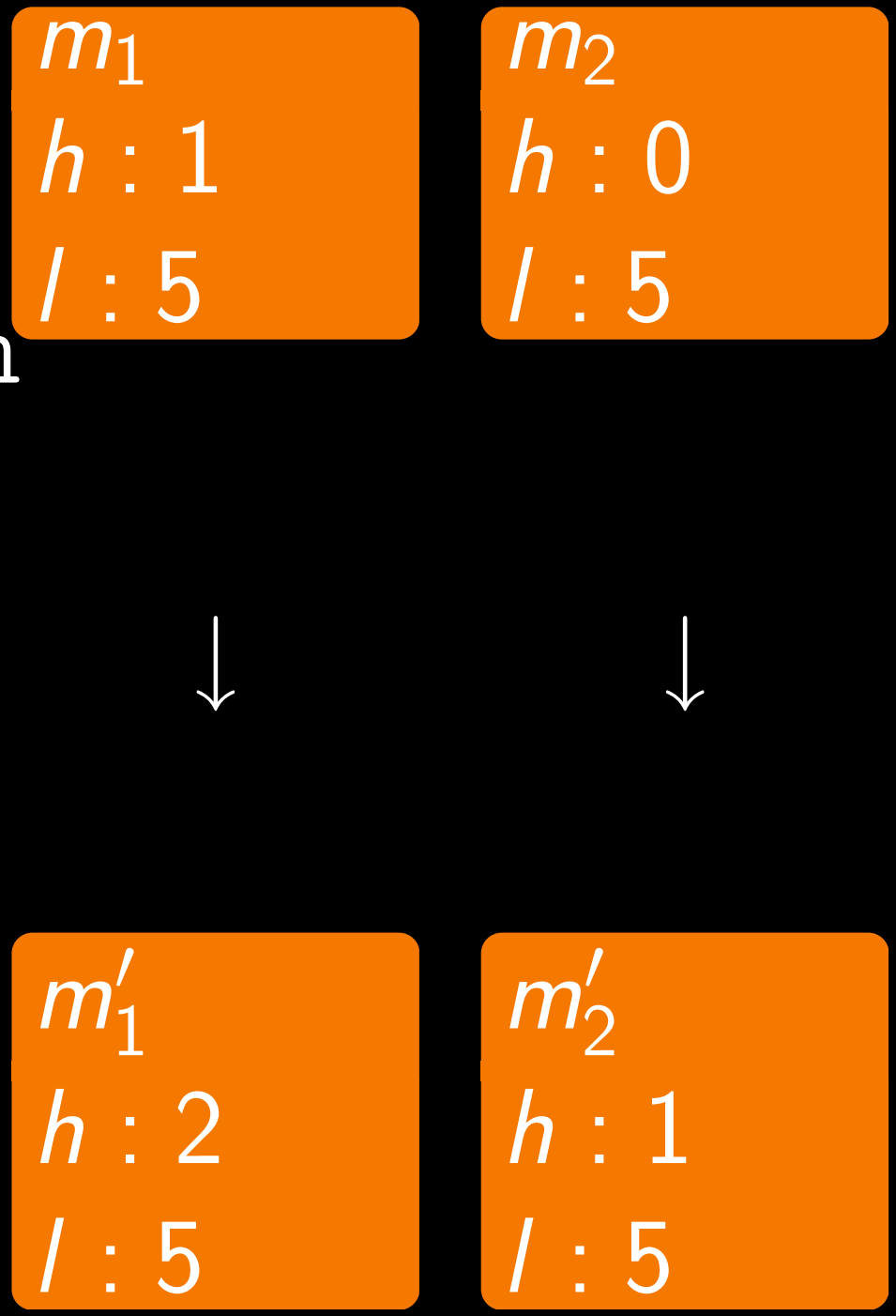
NON SICURO

m_1
$h : 1$
$l : 5$

m_2
$h : 0$
$l : 5$

```
if (l = 5) then
     h := h + 1
else
     l := l +1
```

```
if (l = 5) then
     h := h + 1
else
     l := l +1
```



SICURO!

...CON LA CIFRATURA?

$$encrypt(x, k) \downarrow^{m} \{v, c\}_k$$

```
l := encrypt(a,k)
```

m_1

a : 1234

l : 0

m_2

h : 5678

l : 0

```
l := encrypt(a,k)
```

NON SICURO! :(

m_1
a : 1234
l : 0

m_2
h : 5678
l : 0

m'_1
h : 1234
l : $\{1234, c_1\}_k$

m'_2
h : 5678
l : $\{5678, c_2\}_k$

Assumiamo che il cifrario sia *perfetto*...

$$\{v, c\}_k$$

Cosa vede un attaccante?

Assumiamo che il cifrario sia *perfetto*...

$$\{v, c\}_k$$

Cosa vede un attaccante? $\Box_c$

$\{v, c\}_k \approx_C \{v', c'\}'_k$ se $\Box_c = (\Box_{c'})\rho$

Assumiamo che il cifrario sia *perfetto*...

$$\{v, c\}_k$$

Cosa vede un attaccante? $\Box_c$

$\{v, c\}_k \approx_C \{v', c'\}'_k$ se $\Box_c = (\Box_{c'})\rho$

$$\{1234, c_1\}_k \approx_C \{5678, c_2\}_k,$$
$$\Box_{c_1} = (\Box_{c_2})[c_2 \mapsto c_1]$$

Non dimentichiamo il confronto bit-a-bit...

```
l := encrytpt(b,k)
send(ch,l)
if (h) then
    l := encrypt(a,k)
else
    skip
```

IDEA: **pattern**

$$\{(l, \Box_{c_1}), (ch, \Box_{c_1})\}$$

$$\{(l, \Box_{c_2'}), (ch, \Box_{c_1'})\}$$

Per iniziare...

Language-Based Information-Flow Security
Andrei Sabelfeld and Andrew C. Myers

Il nostro lavoro...

Information Flow Security of Multi-Threaded Distributed Programs
Matteo Centenaro and Riccardo Focardi (mail us)

Per iniziare...

Language-Based Information-Flow Security
Andrei Sabelfeld and Andrew C. Myers

Il nostro lavoro...

Information Flow Security of Multi-Threaded Distributed Programs
Matteo Centenaro and Riccardo Focardi (mail us)

Domande?

Per iniziare...

Language-Based Information-Flow Security
Andrei Sabelfeld and Andrew C. Myers

Il nostro lavoro...

Information Flow Security of Multi-Threaded Distributed Programs
Matteo Centenaro and Riccardo Focardi (mail us)

Domande?

BUON PRANZO :)