informatics mathematics

,

GDR Sécurité
Paris, 1 Juin 2017

1.

2.

3.

4.

5. -

4

...

≠

...

- !

Is my software secure?

attacker model,

.

(, , ,...)

(, ,...)

(, ,...)

,

.

-

,

.

, ' , .

-

.

,

1. $A \hookrightarrow B : \{N_A, A\}_{K_B}$
2. $B \hookrightarrow A : \{N_A, N_B, B\}_{K_A}$
3. $A \hookrightarrow B : \{N_B\}_{K_B}$

-

,

( ).

+ , ,

(,…, ,..) → (, ,…, ,…)

(" ")

, - , …

("

", " ")

, , , , ...

- , , π- , ...

,

,

-

.

,

.

.

.

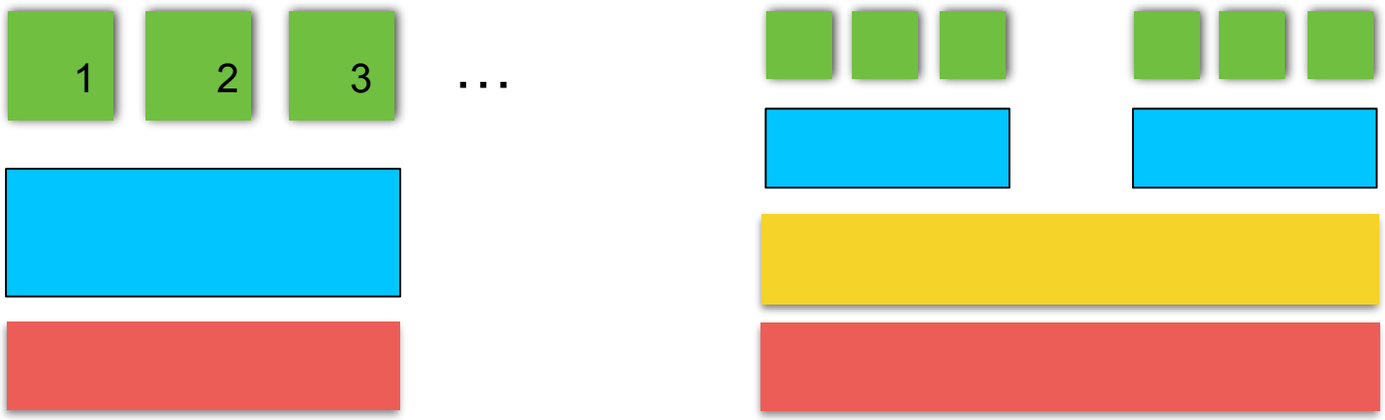
. cryptoverif

.

,

.

isolation properties.



,

-

.

4

2004-2014.

' 4 - .

( ),

, , , -

,

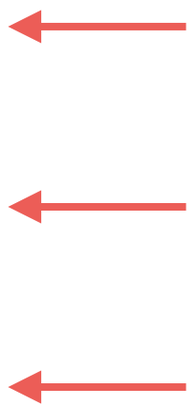
,

/ .

( )

-

4



4

"

",

,

200 000 / 25 -

& '

4 /

-

- .

&

,

.

, ,

'

,

.

,

, , , ...

" – "

.

-

.

(, *

).

" – "

.

*

/

, ,

,

'

xxx.

, , ,

.

-

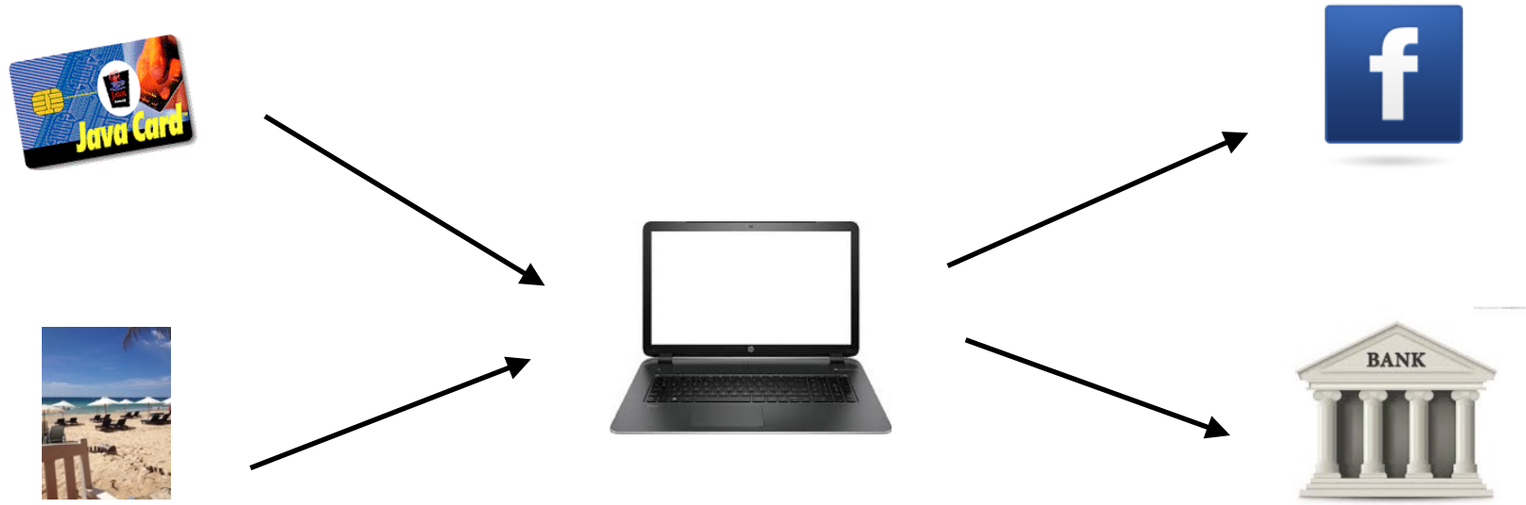
,

,

(- , - ,).

Alarms	A1	A2	A3	A4	A5	A6	A7	A8
ClassCastException	✓	✓	✓	✓	✓	✓	✓	✓
NegativeArraySize	✓	✓	✓	✓	✓	✓	✓	✓
ArrayStoreException	✓	✓	✓	✓	✓	✓	✓	✓
SecurityException	✓	✓	✓	✓	✓	✓	✓	✓
AppletInStaticFields	✓	✓	✓	✓	✓	✓	✓	✓
ArrayConstantSize	✓	✓	✓	✓	✓	✓	✓	✓
InitMenuEntries	✓	✓	✓	✓	✓	✓	✓	✓

Alarms	A1	A2	A3	A4	A5	A6	A7	A8
NullPointerException	94	98	**99**	99	**97**	**98**	97	**99**
ArrayOutOfBounds	71	88	92	87	92	98	90	98
CatchIndividually	**46**	**23**	**82**	**31**	**32**	**67**	**57**	**53**
CatchNonISOException	x	x	x	x	x	x	x	x
HandlerAccess	x	✓	x	x	x	✓	✓	✓
AllocSingleton	✓	✓	✓	✓	✓	x	✓	✓
SDOrGlobalRegPriv	x	✓	✓	✓	✓	✓	✓	✓
SWValid	?	✓	✓	✓	✓	✓	✓	✓
ReplyBusy	?	✓	✓	✓	✓	✓	✓	✓


Java Card
BANK

/ /

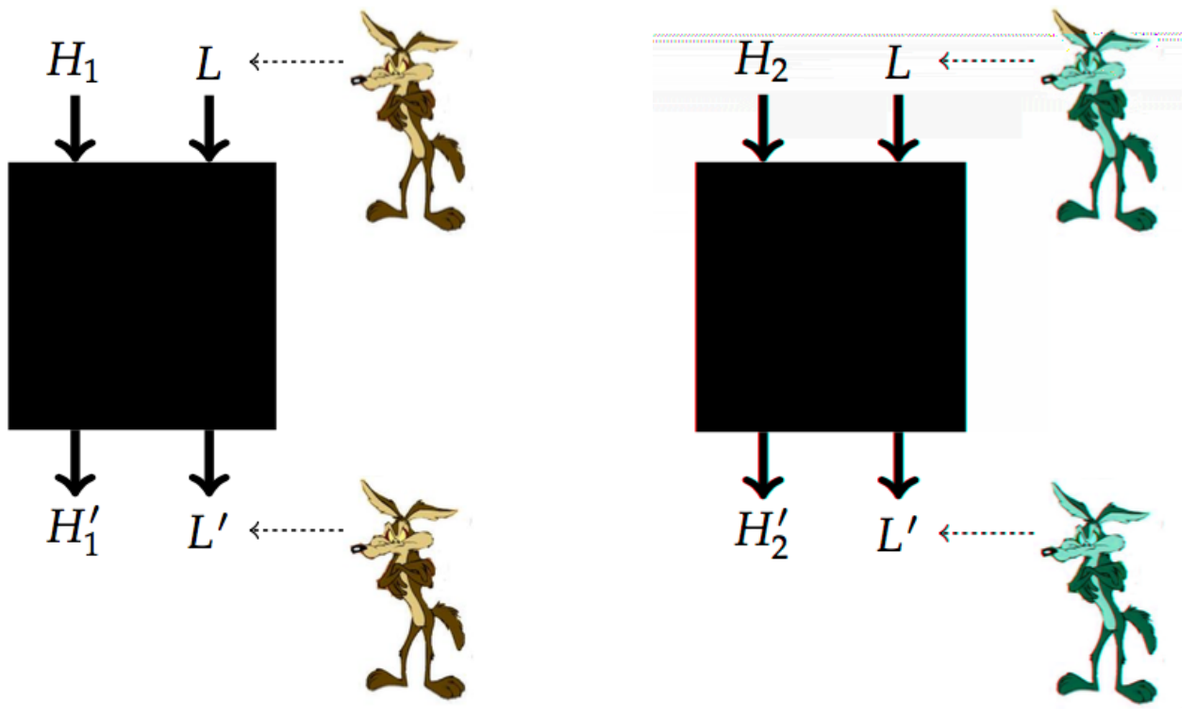
" "

```
int secret s;    // s ∈ {0,1}
int public p;

 p := s;


if s == 1 then
 p := 1
else
 p := 0
```

-

non-interference:

Changes in secret values should not be publicly observable



$$\forall s_1, s_2, s_1', s_2', \quad s_1 \sim s_2 \wedge (P, s_1) \Downarrow s_1' \wedge (P, s_2) \Downarrow s_2' \implies s_1' \sim s_2'$$

(" ")

```
p := s;                    // direct flow
```

```
if s == 1 then
 p := 1
```

!

```
int secret s;    // s ∈ {0,1}
int public p,q;
```

	s=0	s=1
`p := 0; q := 1;`	p=0,q=1	p=0,q=1
`if s == 0 then`		
`  q := 0;`	p=0,q=0	skip
`if q == 1 then`		
`  p := 1;`	skip	p=1,q=1
	p=0	p=1

"no-sensitive-upgrade"

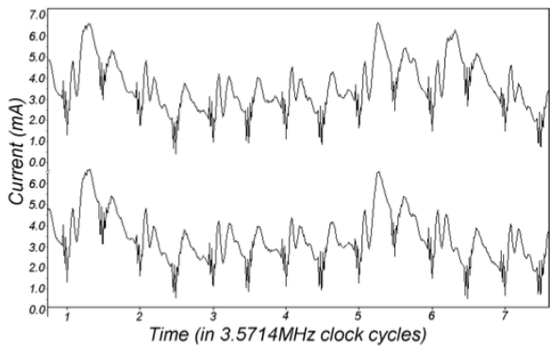
$$\mathsf{T}, \mathsf{T}_{\mathbf{x}}, \mathsf{T}_{\mathsf{pc}} \in \{\mathbf{public} \sqsubseteq \mathbf{secret}\}$$

$$\frac{\vdash \mathbf{e} : \mathsf{T} \quad \mathsf{T} \sqsubseteq \mathsf{T}_{\mathbf{x}} \quad \mathsf{T}_{\mathsf{pc}} \sqsubseteq \mathsf{T}_{\mathbf{x}}}{\mathsf{T}_{\mathsf{pc}} \vdash \mathbf{x} := \mathbf{e}} \; \textit{assign}$$

$$\frac{\vdash \mathbf{e} : \mathsf{T} \quad \mathsf{T}_{\mathsf{pc}} \sqcup \mathsf{T} \vdash \mathbf{S_i} \quad \mathbf{i} = \mathbf{1,2}}{\mathsf{T}_{\mathsf{pc}} \vdash \mathbf{if\ e\ then\ S_1\ else\ S_2}} \; \textit{if}$$

Well-typed programs are non-interferent

(passwd,)



-

(-)

.

( )

.

.

et al.

(.),

( ).

Thank you

Thank you