AFADL 2016

GenISIS: un outil de recherche d'attaques d'initié en Systèmes d'Information

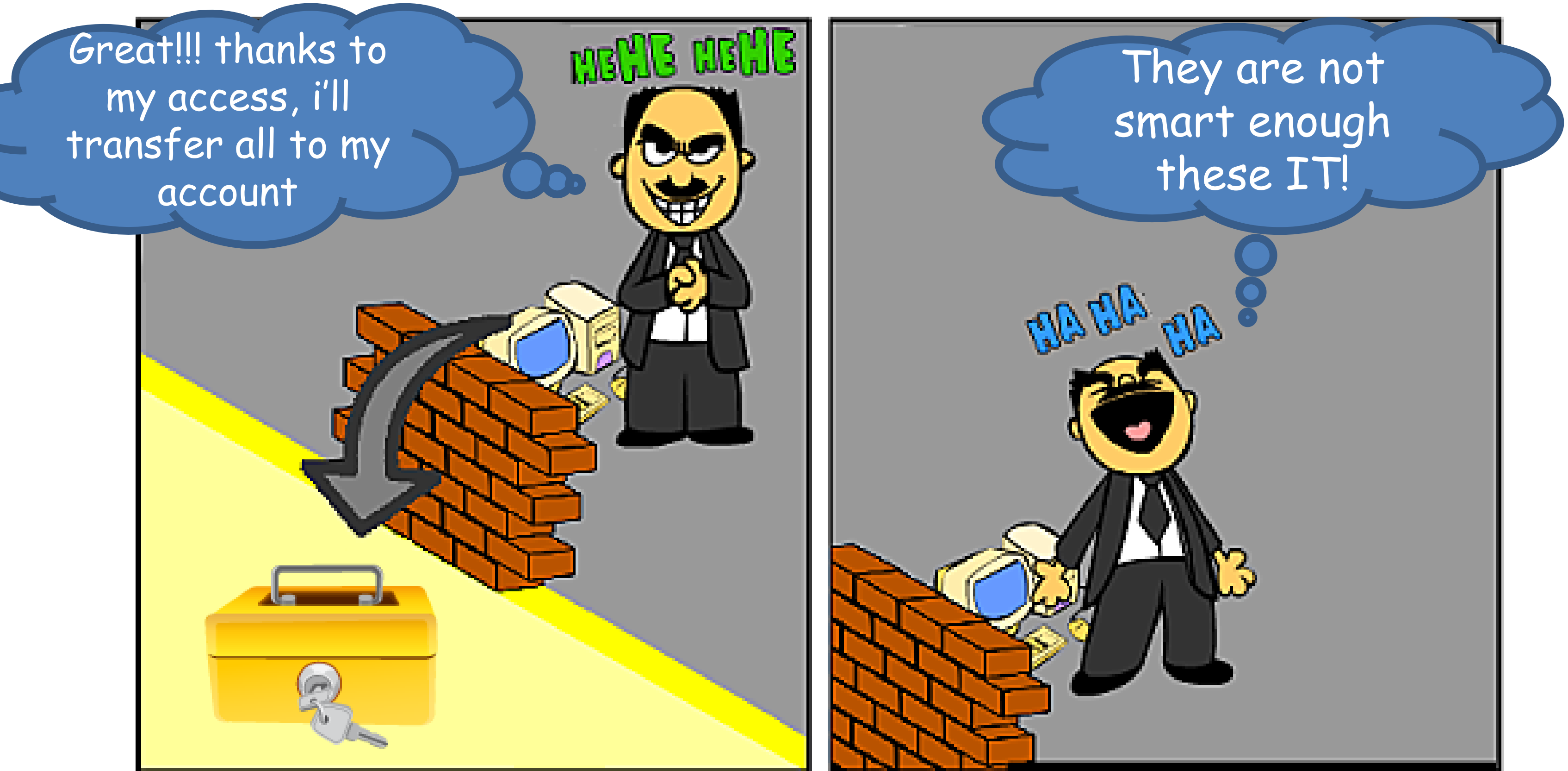
Authors: Amira RADHOUANI
Akram IDANI
Yves LEDRU
Narjes BEN RAJEB

L I G

Laboratoire d'Informatique de Grenoble

CONTEXT AND MOTIVATION

- Information System security includes =
  Protection against external intruders
  +
  Insider attacks.


Great!!! thanks to my access, i'll transfer all to my account
HEHE HEHE
They are not smart enough these IT!
HA HA HA

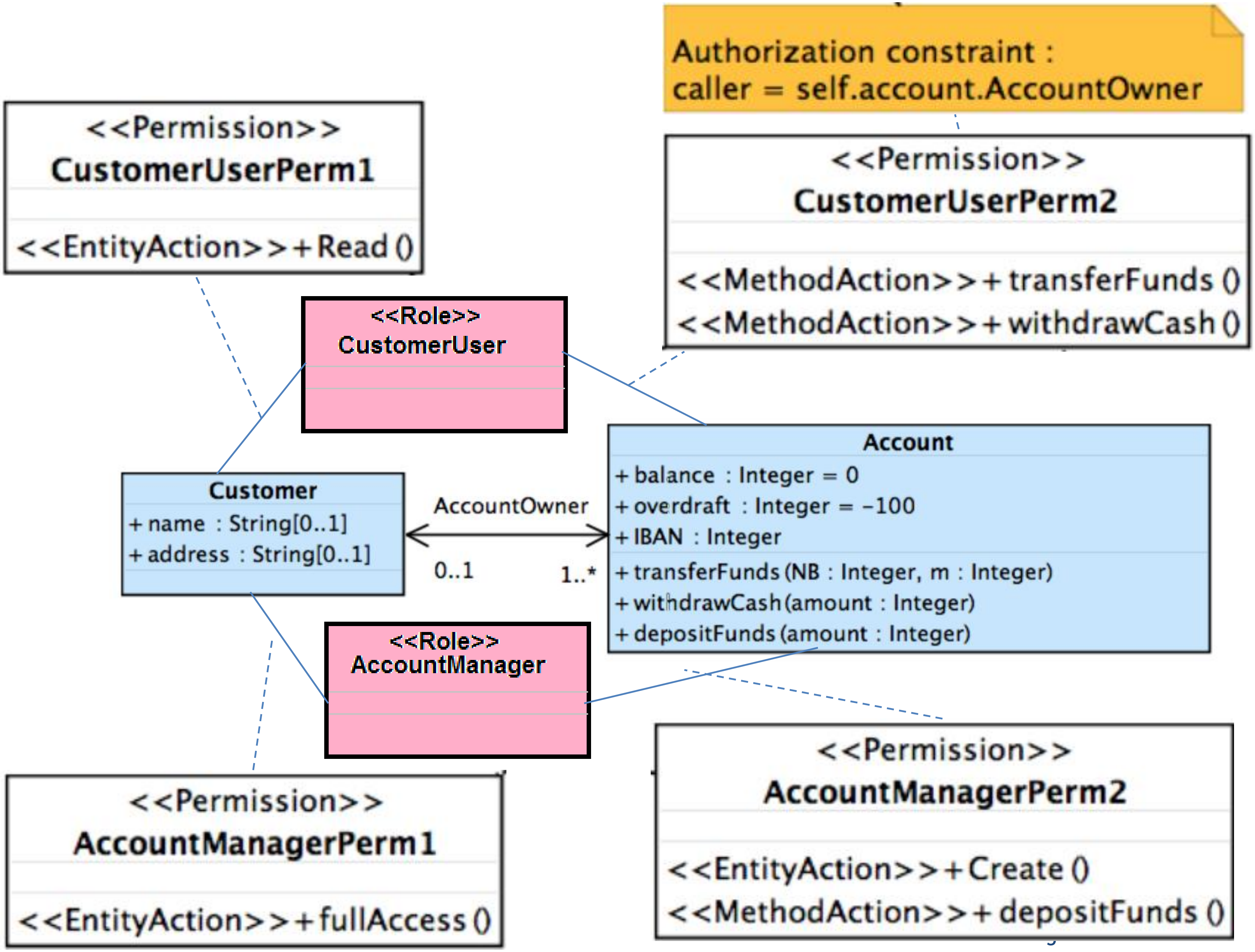
OUTLINE

1. Introduction
   - Illustration example
2. Malicious behavior
3. Extraction of malicious behaviors
   - Extraction of malicious behaviors from B Specification
   - Constraint solving based approach
   - GenISIS tool
4. Conclusion

Introduction

1. Illustration example
2. Dynamic analysis

ILLUSTRATION EXAMPLE



Authorization constraint :
caller = self.account.AccountOwner

<<Permission>>
CustomerUserPerm1
<<EntityAction>>+Read ()

<<Permission>>
CustomerUserPerm2
<<MethodAction>>+transferFunds ()
<<MethodAction>>+withdrawCash ()

<<Role>>
CustomerUser

Customer
+name : String[0..1]
+address : String[0..1]

AccountOwner
0..1
1..*

Account
+balance : Integer = 0
+overdraft : Integer = −100
+IBAN : Integer
+transferFunds (NB : Integer, m : Integer)
+withdrawCash (amount : Integer)
+depositFunds (amount : Integer)

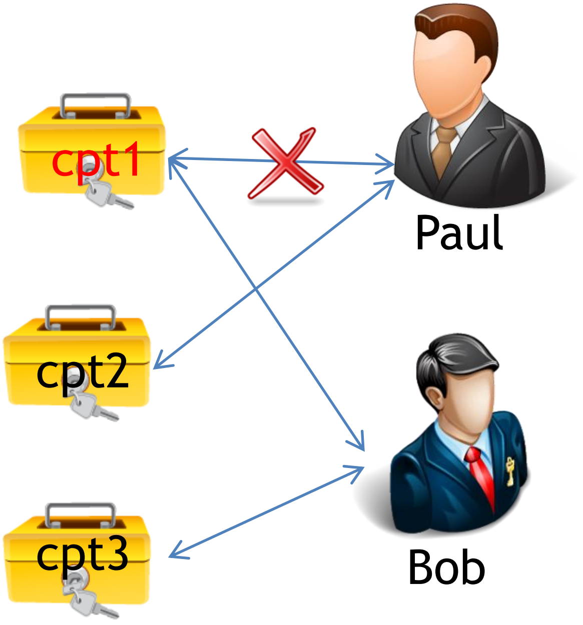
<<Role>>
AccountManager

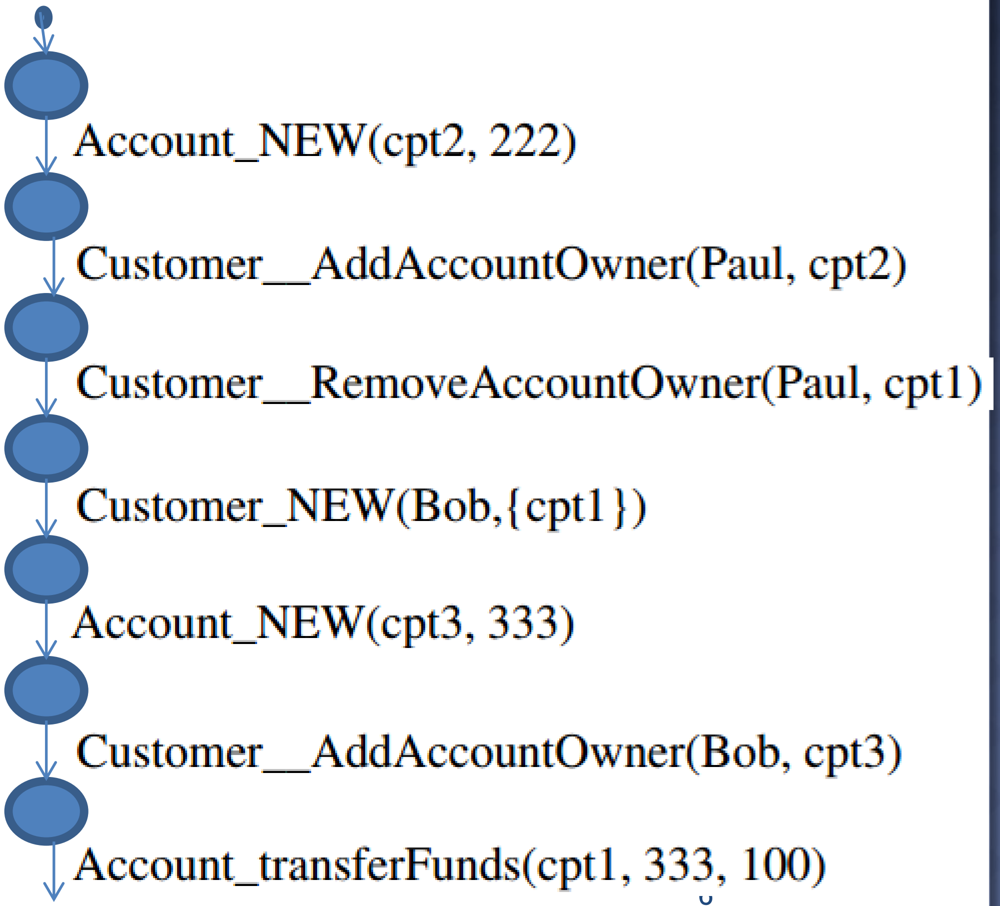
<<Permission>>
AccountManagerPerm1
<<EntityAction>>+fullAccess ()

<<Permission>>
AccountManagerPerm2
<<EntityAction>>+Create ()
<<MethodAction>>+depositFunds ()

DYNAMIC ANALYSIS

- Dynamic analysis searches for sequences of actions modifying the state and breaking the authorization constraint.





Account_NEW(cpt2, 222)

Customer__AddAccountOwner(Paul, cpt2)

Customer__RemoveAccountOwner(Paul, cpt1)

Customer_NEW(Bob,{cpt1})

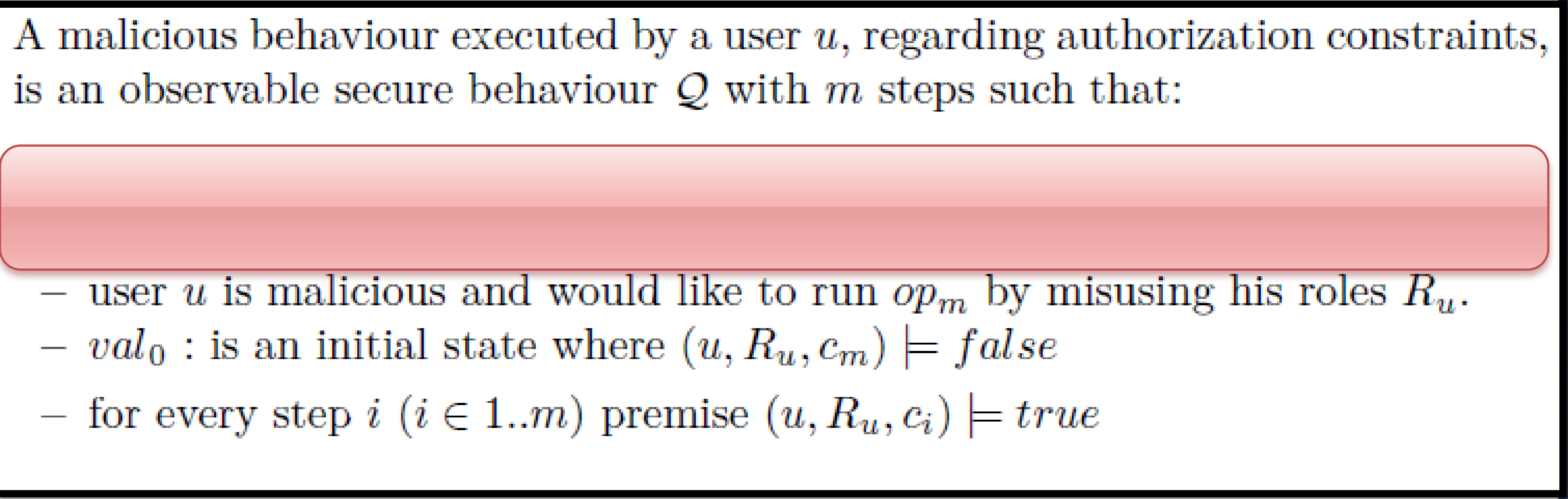
Account_NEW(cpt3, 333)

Customer__AddAccountOwner(Bob, cpt3)

Account_transferFunds(cpt1, 333, 100)

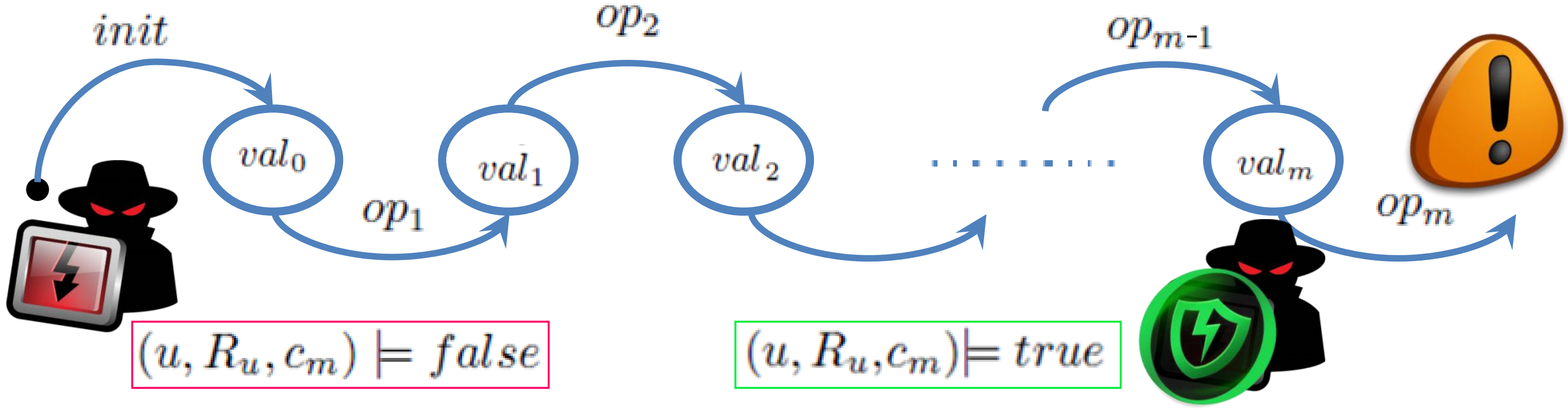
Malicious behavior

MALICIOUS BEHAVIOR



A malicious behaviour executed by a user u, regarding authorization constraints, is an observable secure behaviour Q with m steps such that:

- user u is malicious and would like to run op_m by misusing his roles R_u.
- val_0 : is an initial state where $(u, R_u, c_m) \models false$
- for every step i $(i \in 1..m)$ premise $(u, R_u, c_i) \models true$



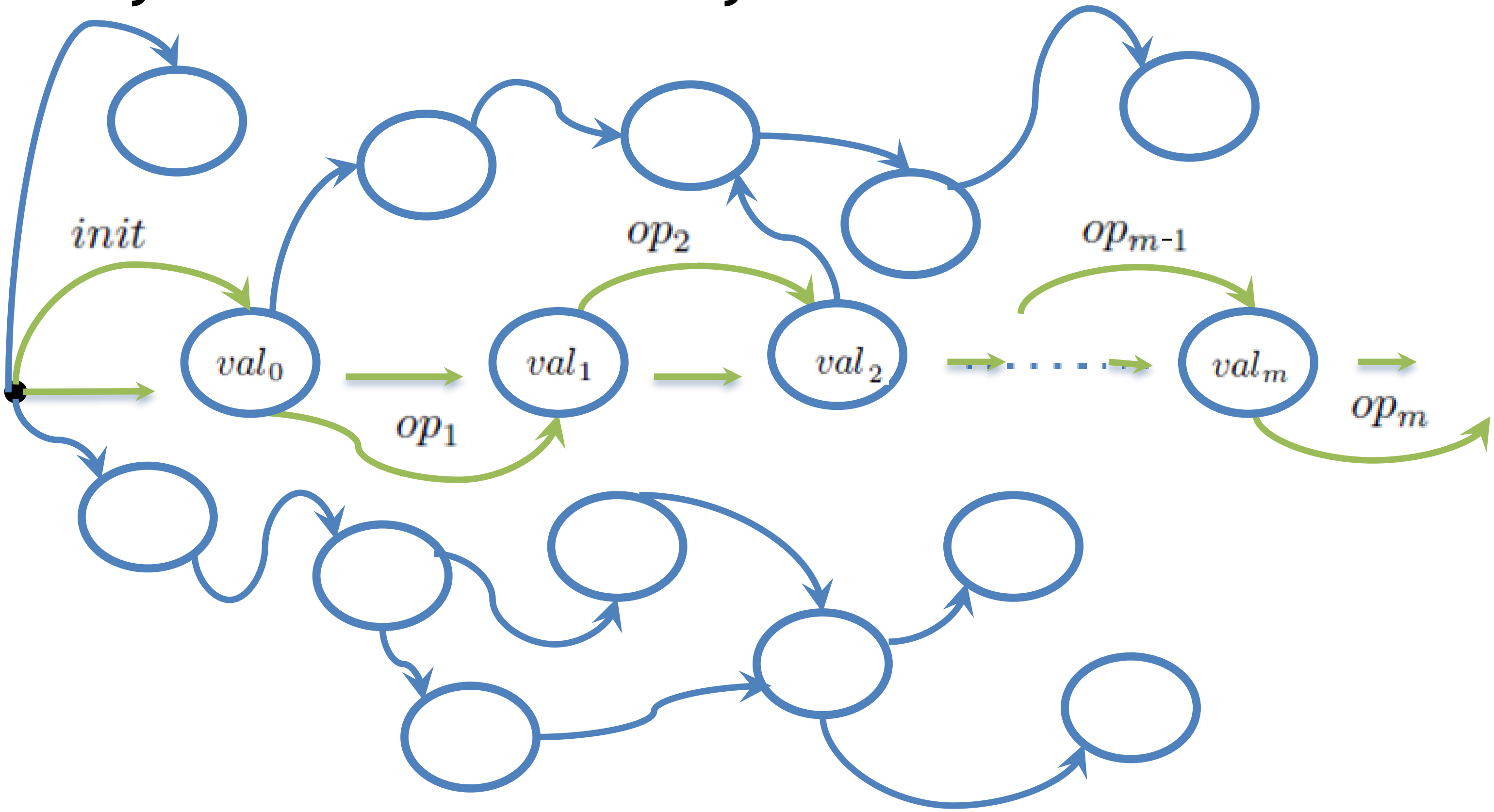
[A. Radhouani et al., Trans. Petri Nets and Other Models of Concurrency 10: 131-152 (2015)]

Extraction of malicious behaviors

1. Extraction of malicious behaviors from B Specification
2. Proof based approach
3. Constraint solving based approach
4. GenISIS Tool

EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION

- Symbolic transition system

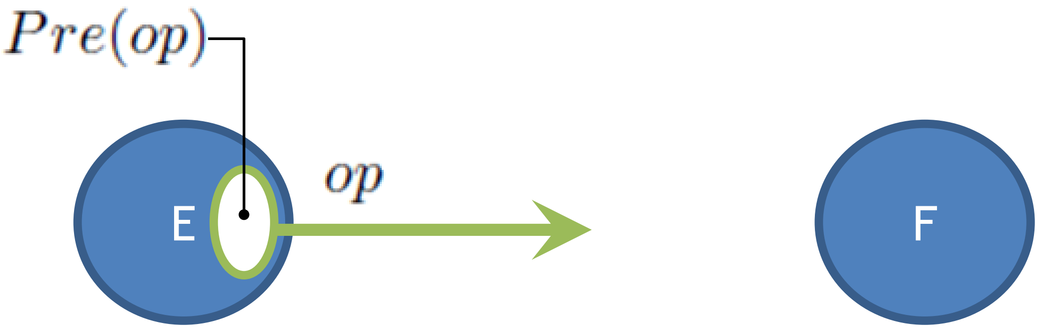


EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION

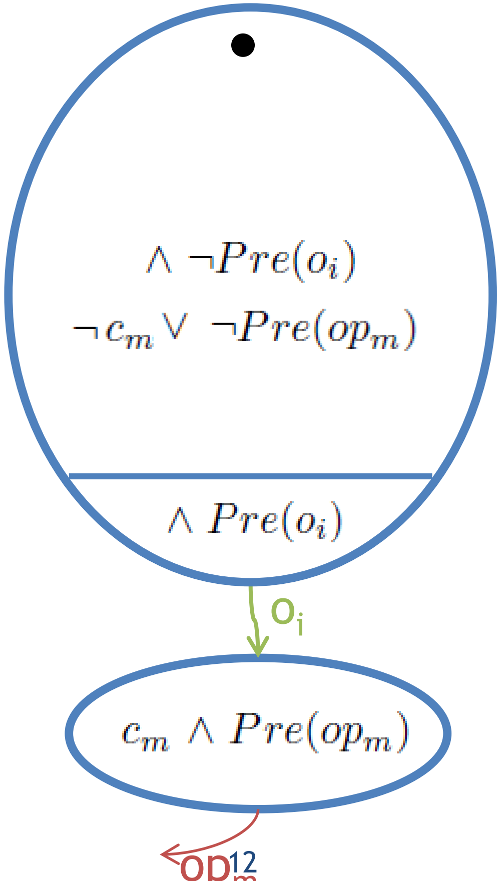
- Symbolic proof
  - Proof obligations on reachability properties:
    - Having *E* and *F*, 2 disjoint state predicates
    - And *op(*$x_1, x_2, \ldots, x_n$*)* is an operation of the IS.

- Enabledness: $\exists x_1, \ldots, x_n, var.\mathrm{P_I} \wedge Pre(op)$
- Reachability: $\exists x_1, \ldots, x_n, var.\mathrm{P_I} \wedge Pre(op) \Rightarrow \neg[Action(op)]\neg\mathrm{P_F}$

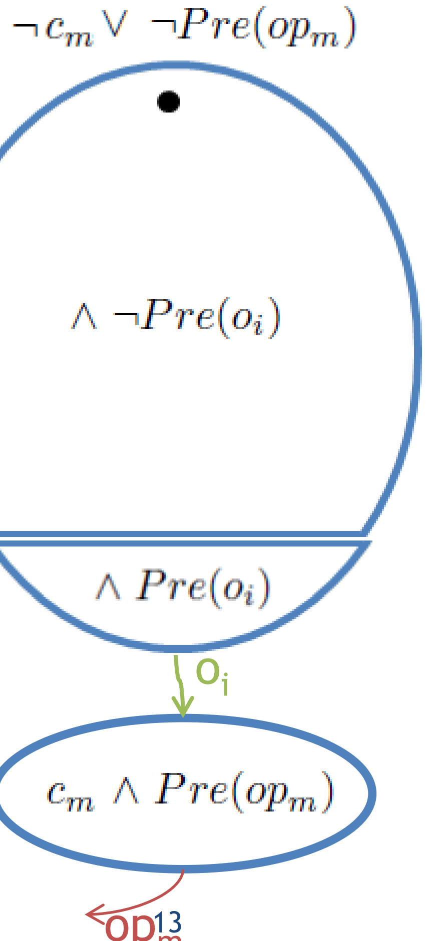
$$\exists x_1, \ldots, x_n, var.\mathrm{P_I} \wedge Pre(op) \wedge \neg[Action(op)]\neg\mathrm{P_F}$$



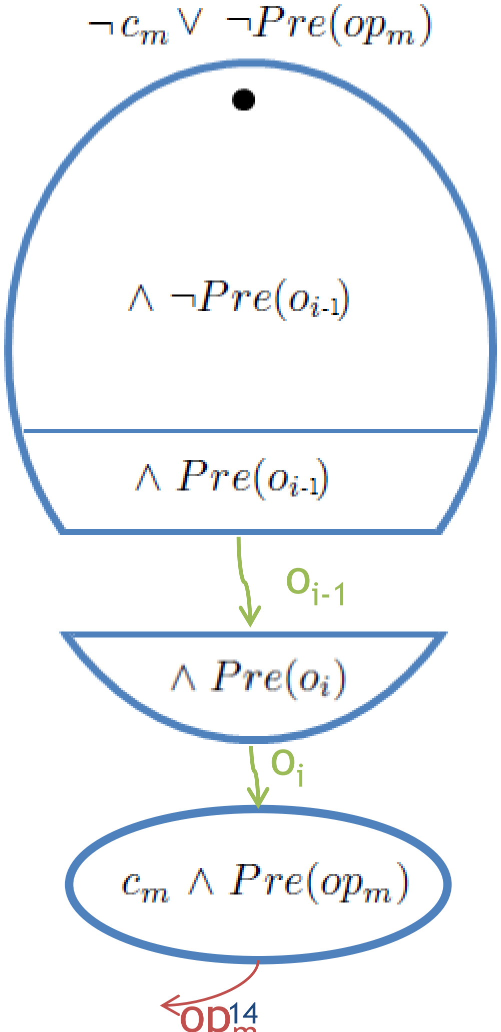
EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION



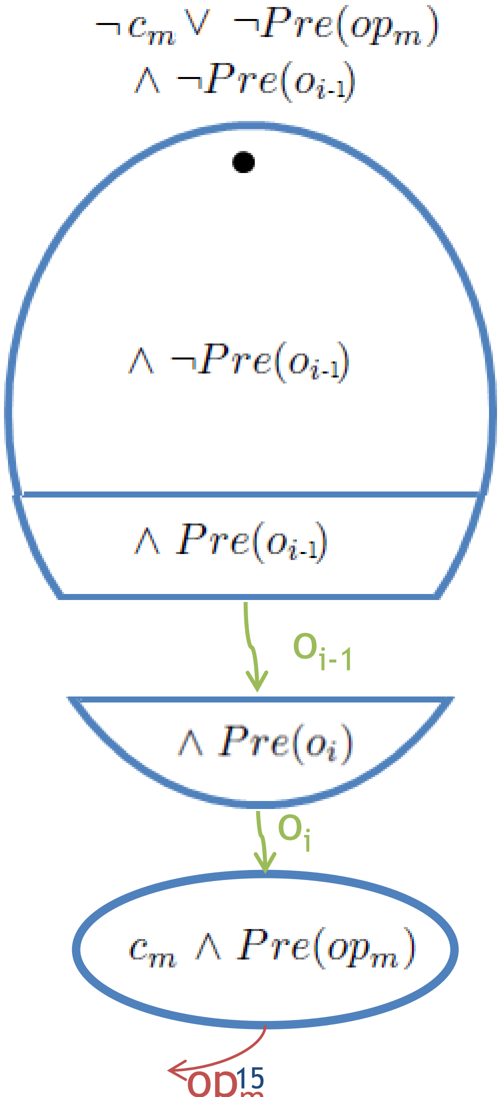
EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION



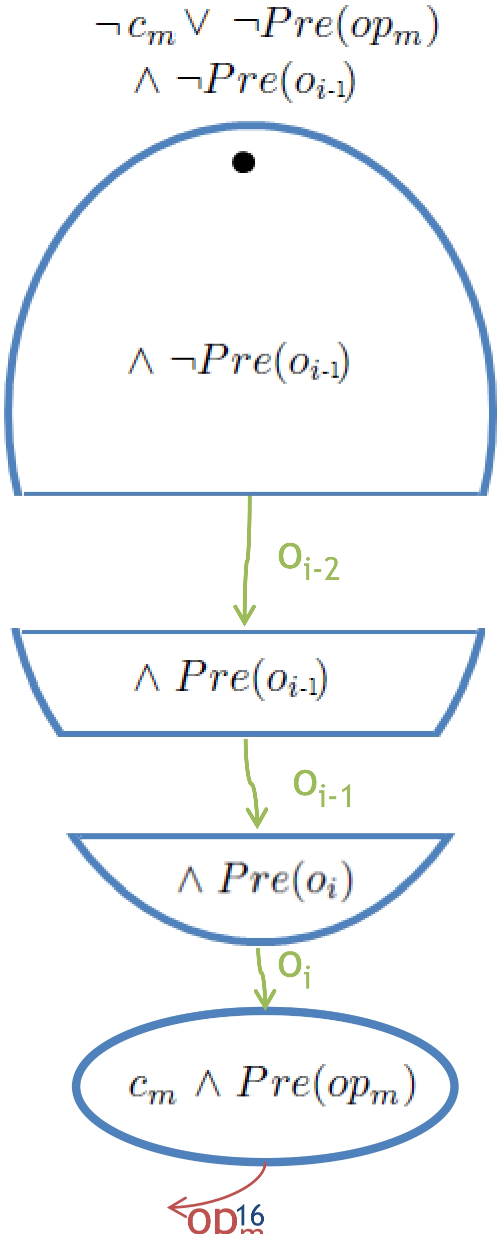
EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION


$\neg c_m \vee \neg Pre(op_m)$
$\wedge \neg Pre(o_{i\text{-}1})$
$\wedge Pre(o_{i\text{-}1})$
o_{i-1}
$\wedge Pre(o_i)$
o_i
$c_m \wedge Pre(op_m)$
op_m

EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION

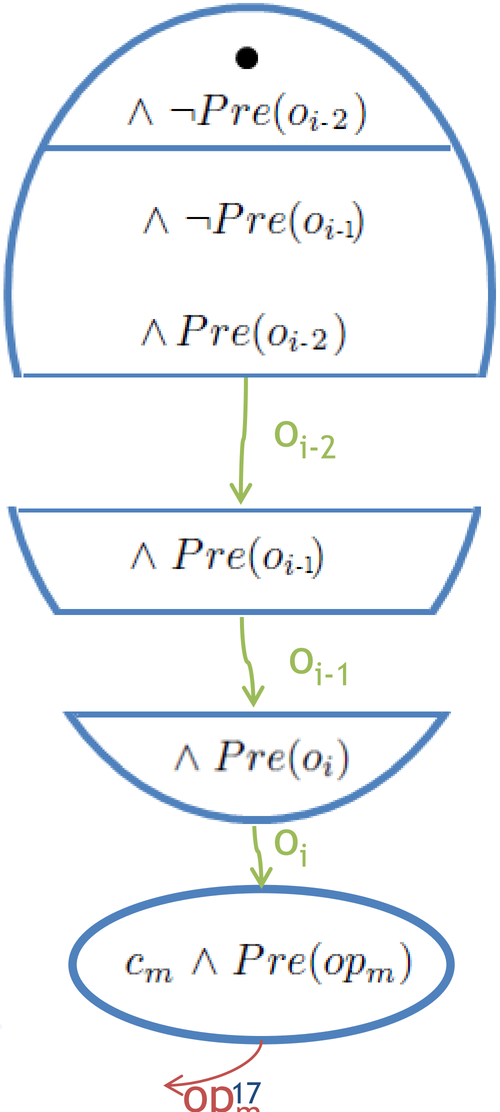

$\neg c_m \vee \neg Pre(op_m)$
$\wedge \neg Pre(o_{i\text{-}1})$
$\wedge \neg Pre(o_{i\text{-}1})$
$\wedge Pre(o_{i\text{-}1})$
o_{i-1}
$\wedge Pre(o_i)$
o_i
$c_m \wedge Pre(op_m)$
op_m

EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION


$\neg c_m \vee \neg Pre(op_m)$
$\wedge \neg Pre(o_{i\text{-}1})$
$\wedge \neg Pre(o_{i\text{-}1})$
o_{i-2}
$\wedge Pre(o_{i\text{-}1})$
o_{i-1}
$\wedge Pre(o_i)$
o_i
$c_m \wedge Pre(op_m)$
op_m

EXTRACTION OF MALICIOUS BEHAVIORS FROM B SPECIFICATION

$\neg c_m \vee \neg Pre(op_m)$
$\wedge \neg Pre(o_i)$


●
$\wedge \neg Pre(o_{i\text{-}2})$
$\wedge \neg Pre(o_{i\text{-}1})$
$\wedge Pre(o_{i\text{-}2})$
o_{i-2}
$\wedge Pre(o_{i\text{-}1})$
o_{i-1}
$\wedge Pre(o_i)$
o_i
$c_m \wedge Pre(op_m)$
op_m

$Q \triangleq init \; ; \qquad ; \qquad ; \qquad ; \; op_m$

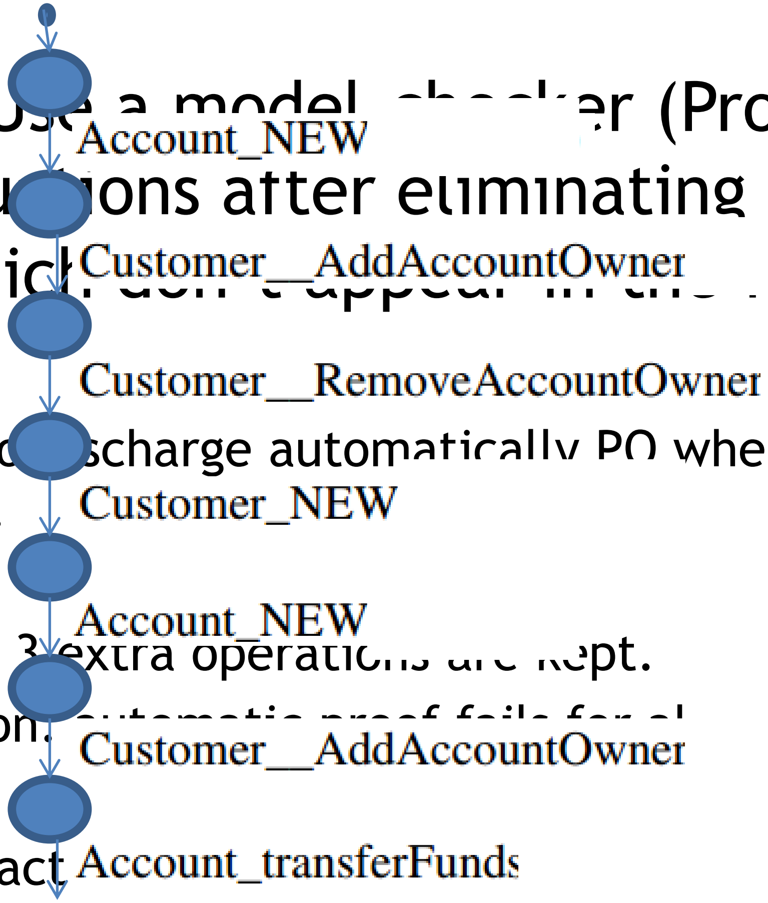
PROOF BASED APPROACH

[A. Radhouani, A. Idani, Y. Ledru and N. Ben Rajeb. TopNoc10: 131-152 (2015)]

- First step: Use of a prover (AtelierB) to extract **symbolic operations**.
- Second step: Use a model checker (ProB) to find operation valuations after eliminating operations which don't appear in the first step.
  - AtelierB fails to discharge automatically PO when the proof becomes huge.

  In our example:

  - First iteration: 3 extra operations are kept.
  - Second iteration: automatic proof fails for al ns.
  - Unable to extract eration several times.


Account_NEW
Customer__AddAccountOwner
Customer__RemoveAccountOwner
Customer_NEW
Account_NEW
Customer__AddAccountOwner
Account_transferFunds

CONSTRAINT SOLVING BASED APPROACH

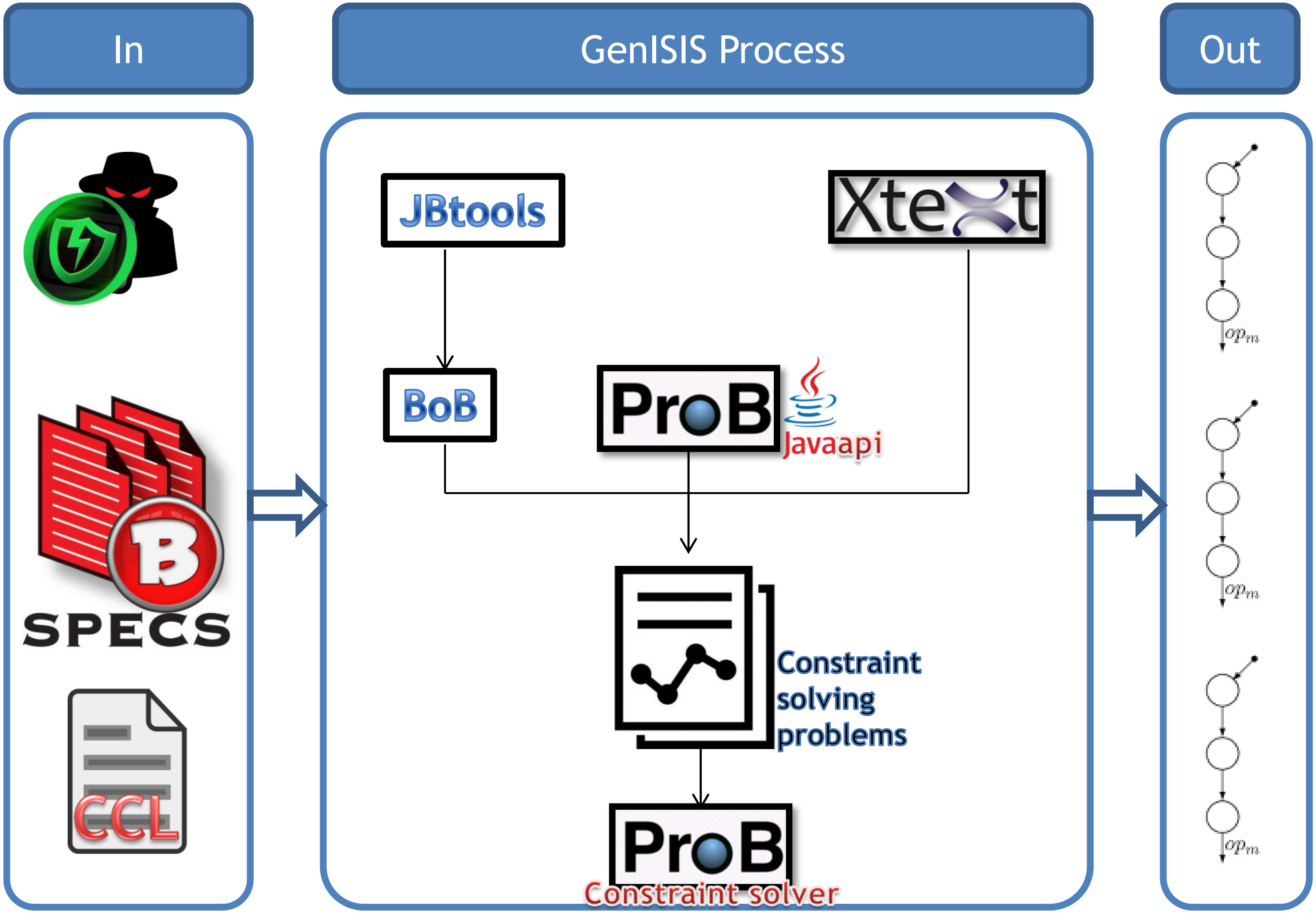
- Constraint solving problem:

$$\{x_1, \ldots, x_n \mid \exists var.\, \mathsf{P}_\mathsf{I} \wedge Pre(op) \wedge \neg[Action(op)]\neg \mathsf{P}_\mathsf{F}\}$$

  - Allows to valuate operation parameters.
  - Simplifies the proof.
  - Allows to extract scenarios which involves the same operation several times (the same operation with different valuations).

GENISIS TOOL

-Generator of Insider Scenarios from an Information System-



Conclusion

CONCLUSIONS

- GenISIS was able to extract 9 scenarios.
  - 2 real attacks: allowed in the security model.
  - 7 fake attacks: not allowed in the security model.

- A model-checker (i.e ProB) extracted the same attacks after exploring more than 1500 states and 36000 transitions.

- GenISIS was Was successfully tested on 5 case studies.

GenISIS

Try it, it is available on open source in: http://genisis.forge.imag.fr/

Thanks for your attention