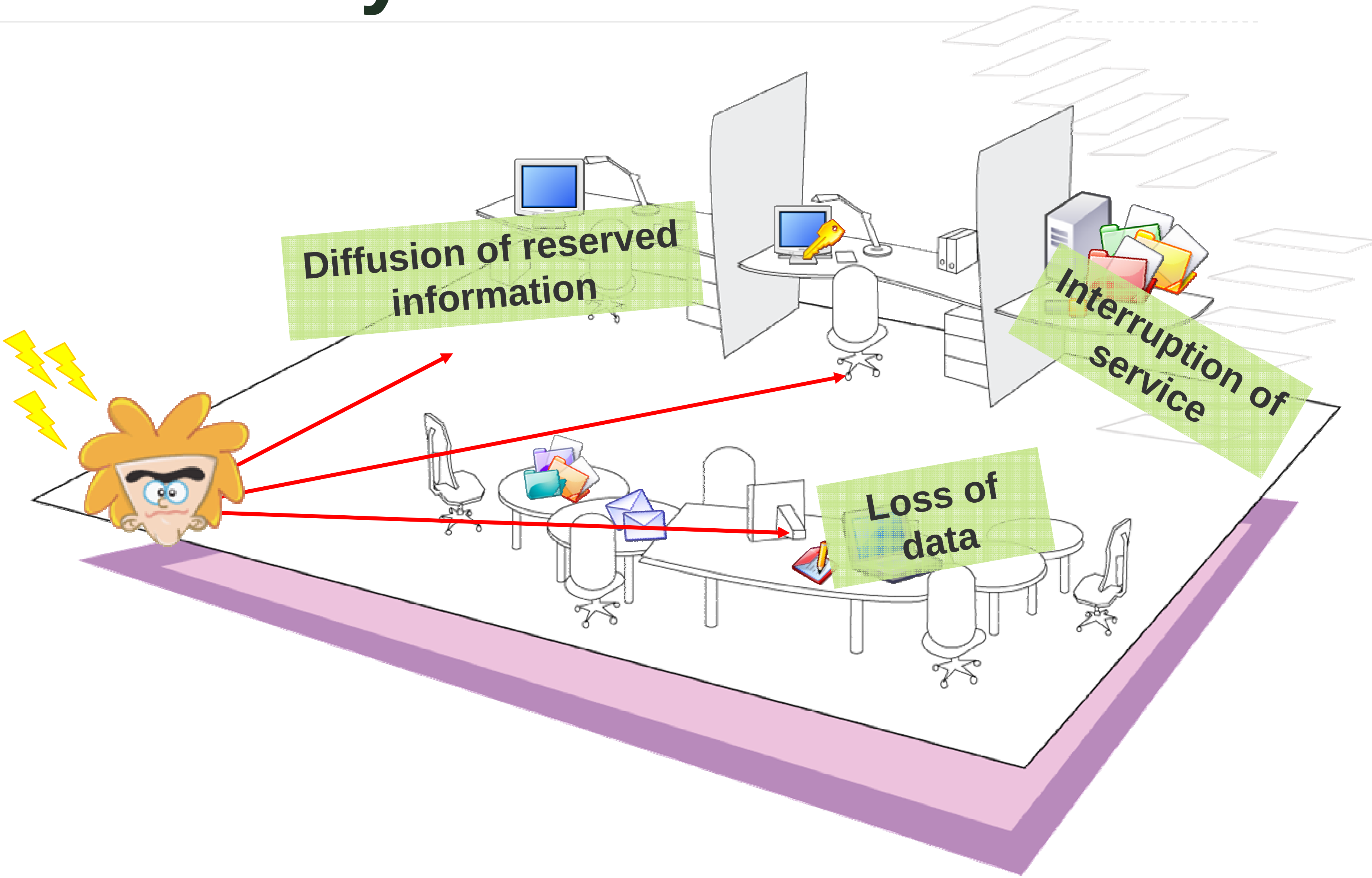
Pescara, 2 aprile 2008

Modeling and selecting preferred countermeasures using CP-nets and Answer Set Programming

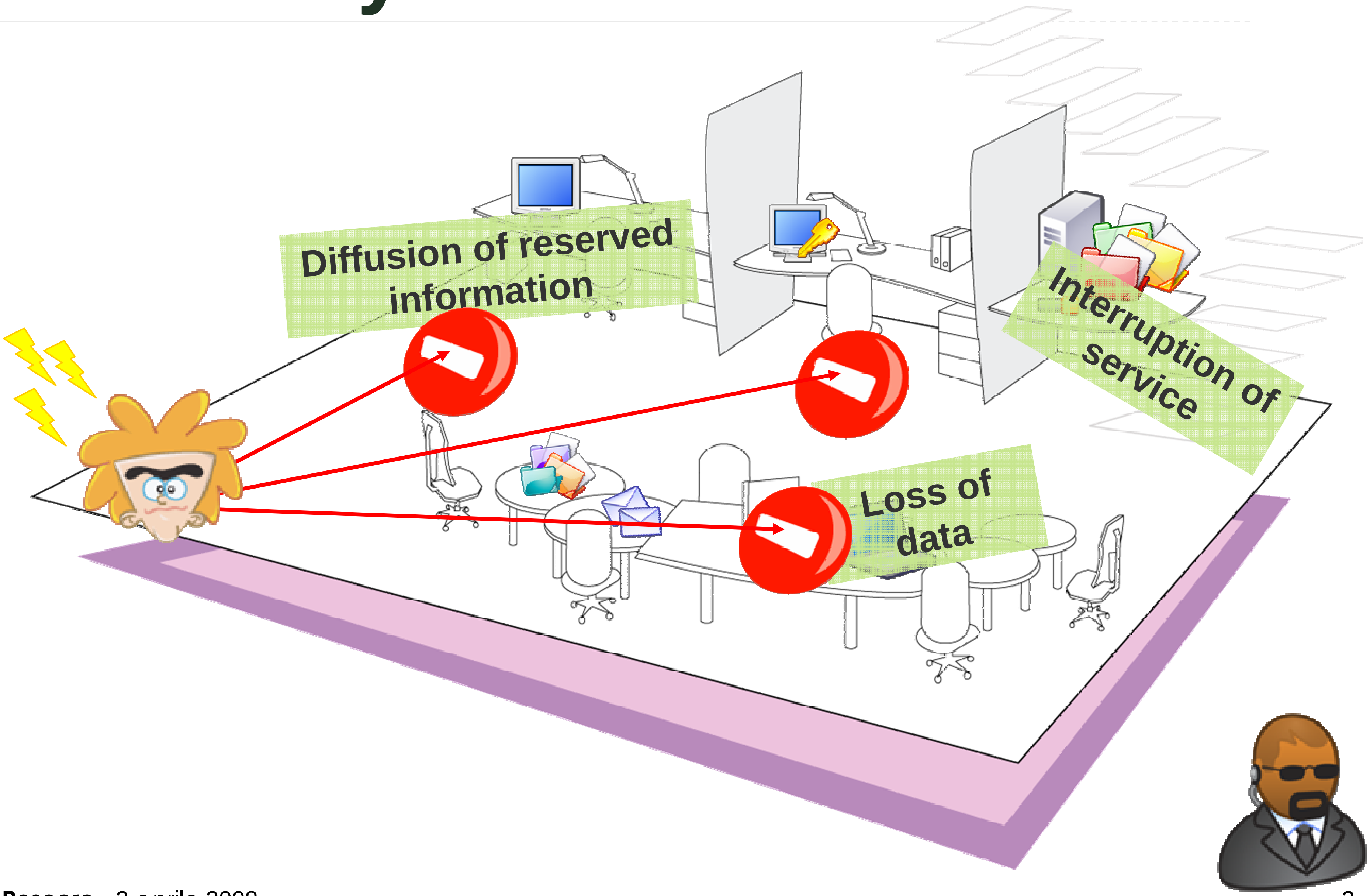
Pamela Peretti

Dipartimento di Scienze Università degli Studi “G. d’Annunzio”
Pescara

A security scenario



A security scenario



Agenda

- Instruments
  - Defence trees
  - Cp-networks
- CP-defence trees
  - and-composition of attacks
  - or-composition of attacks
- From CP-defence trees to ASO programs:
  - Modelling defence tree
  - Modelling preferences among attacks and countermeasures
- Implementation

Agenda

- Instruments
  - Defence trees
  - Cp-networks
- CP-defence trees
  - and-composition of attacks
  - or-composition of attacks
- From CP-defence trees to ASO programs:
  - Modelling defence tree
  - Modelling preferences among attacks and countermeasures
- Implementation

Defence trees

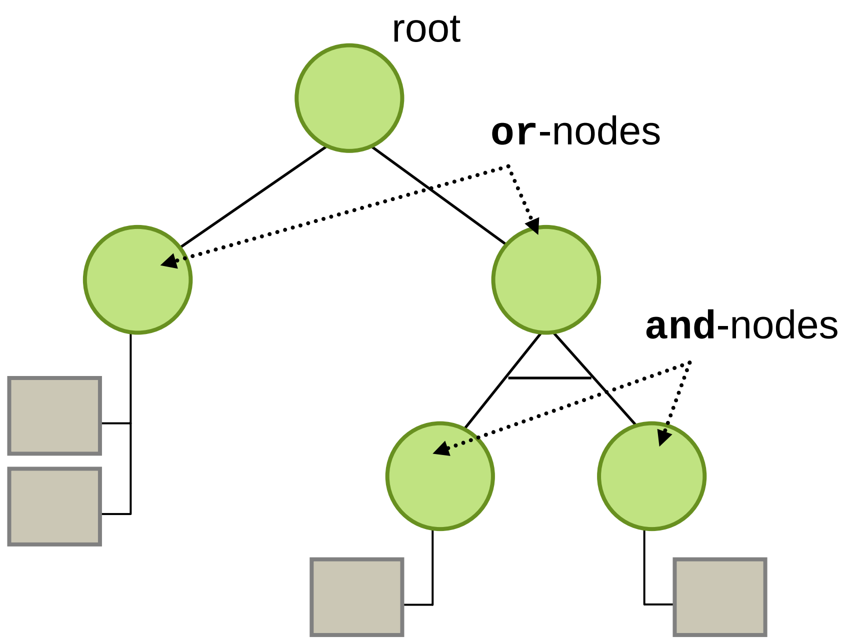
Defence trees are an extension of attack trees [Schneier00].

Attack tree:

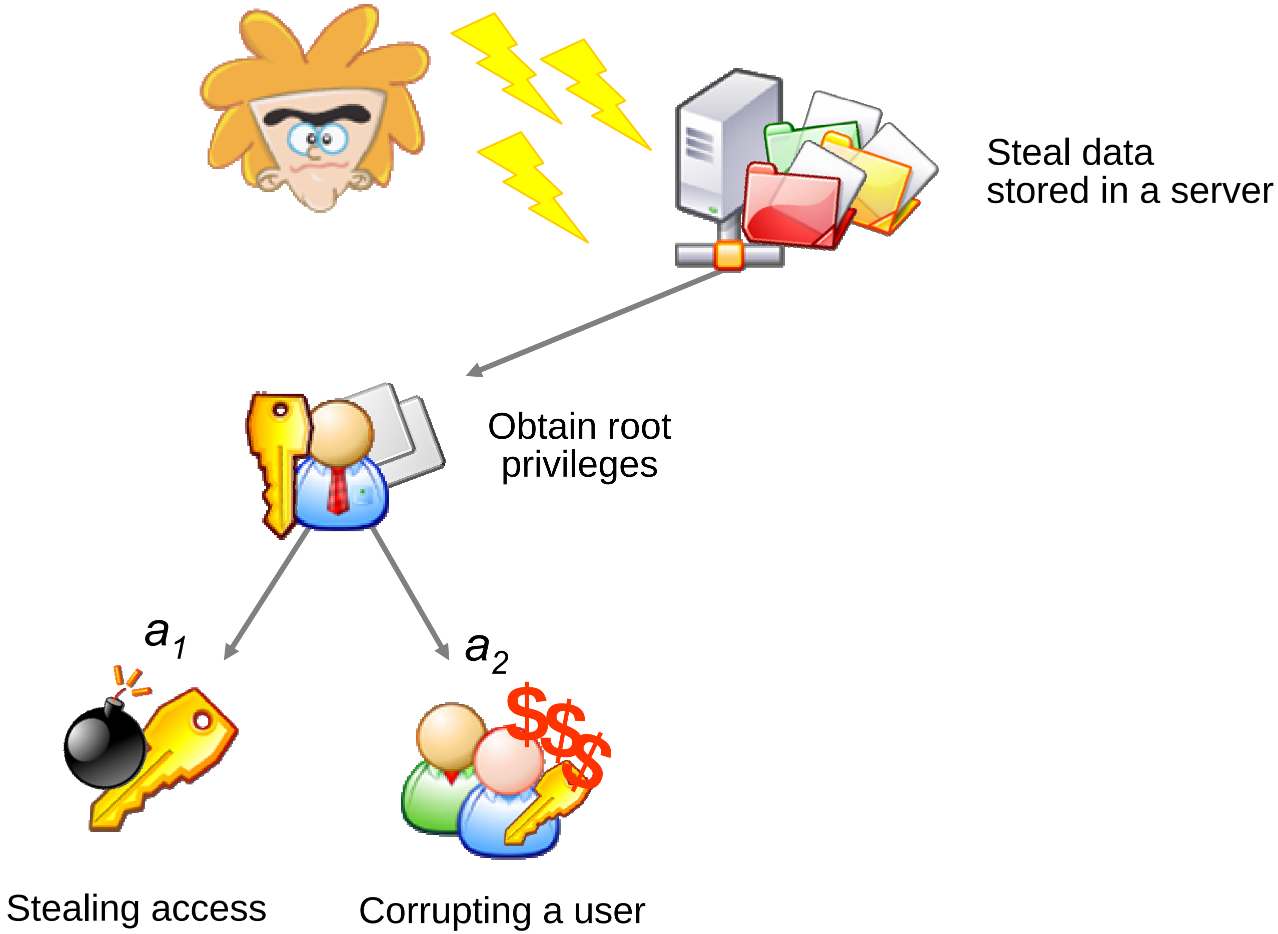
- the root is an asset of an IT system
- paths from a leaf to the root represent attacks to the asset
- the non-leaf nodes can be:
  - and-nodes
  - or-nodes

Defence tree:

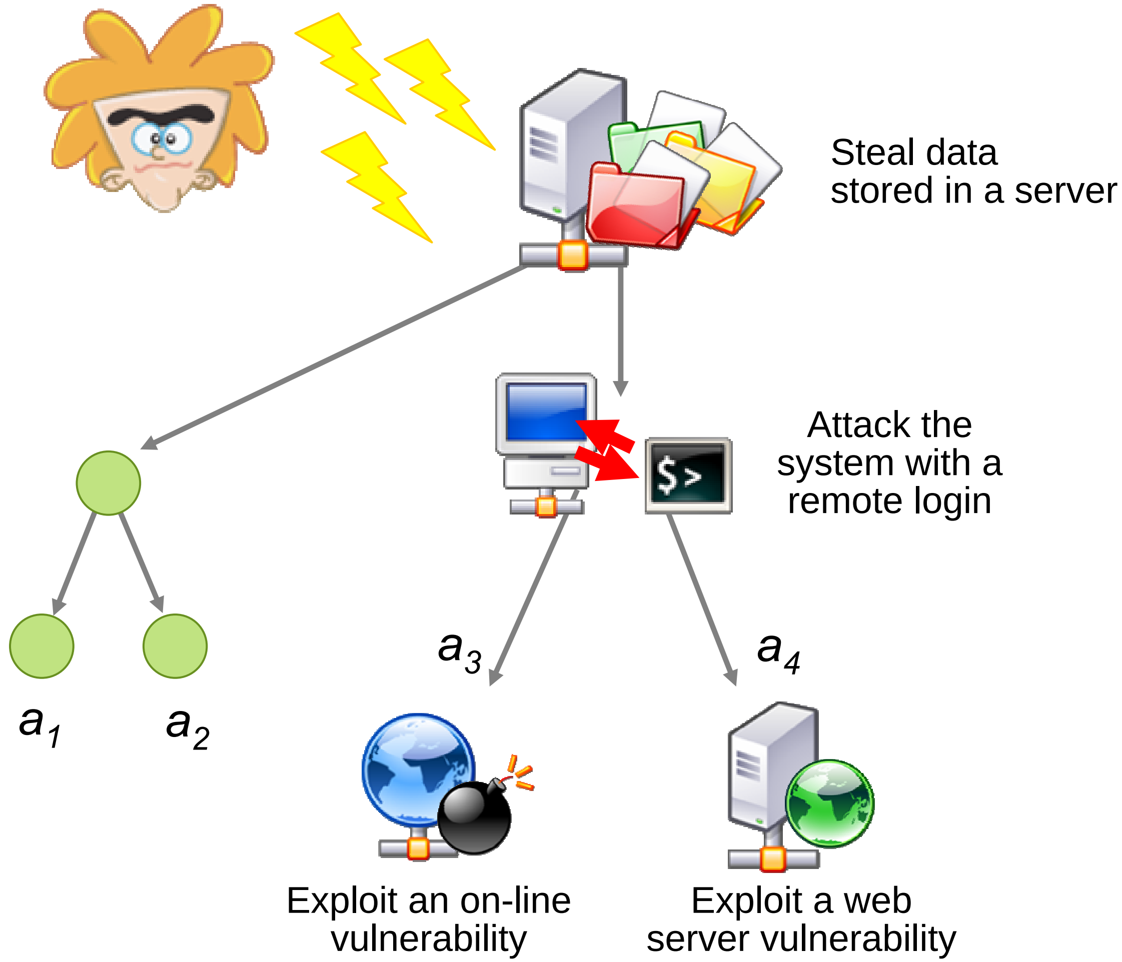
- attack tree
- a set of countermeasures



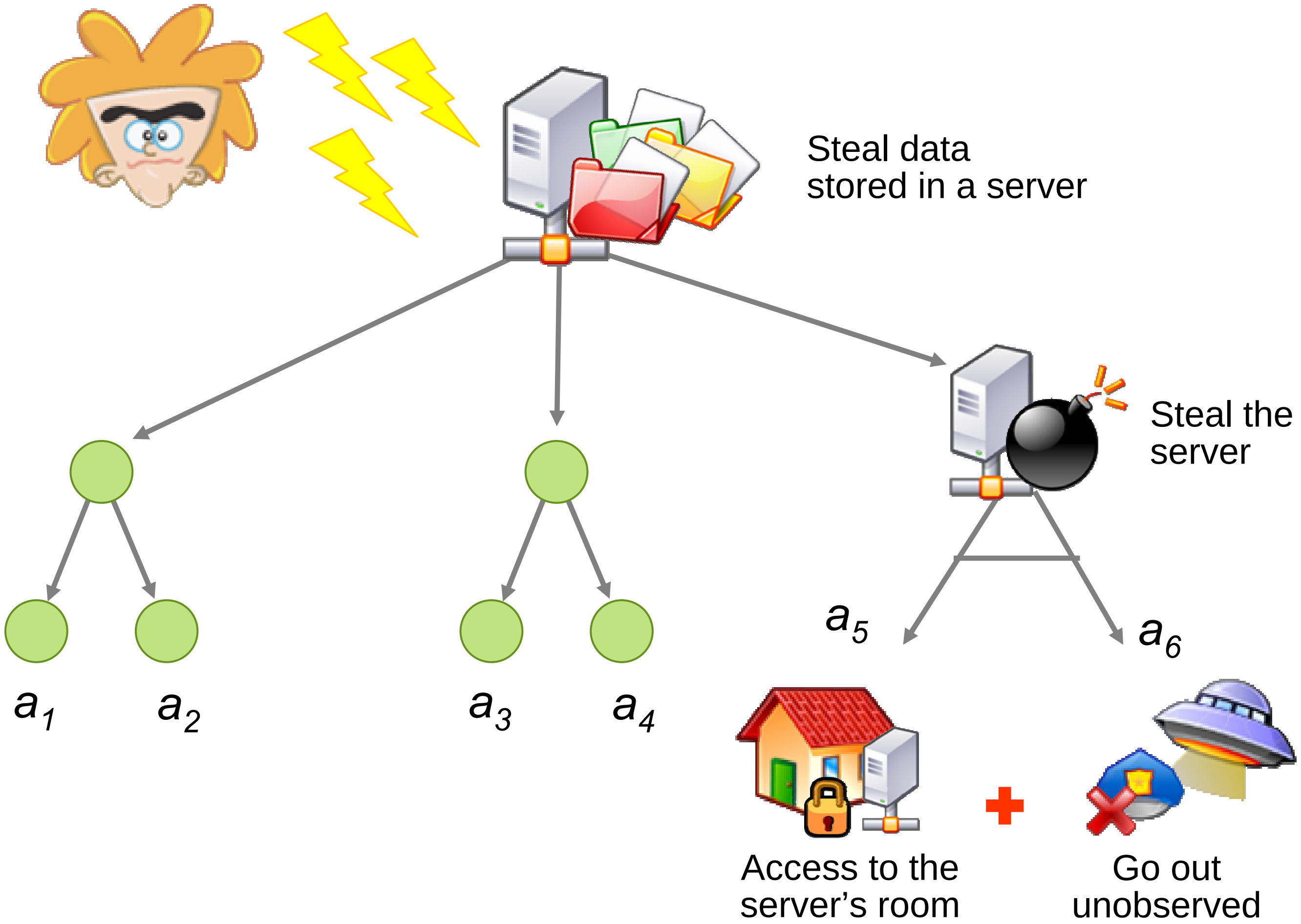
Defence trees (example)



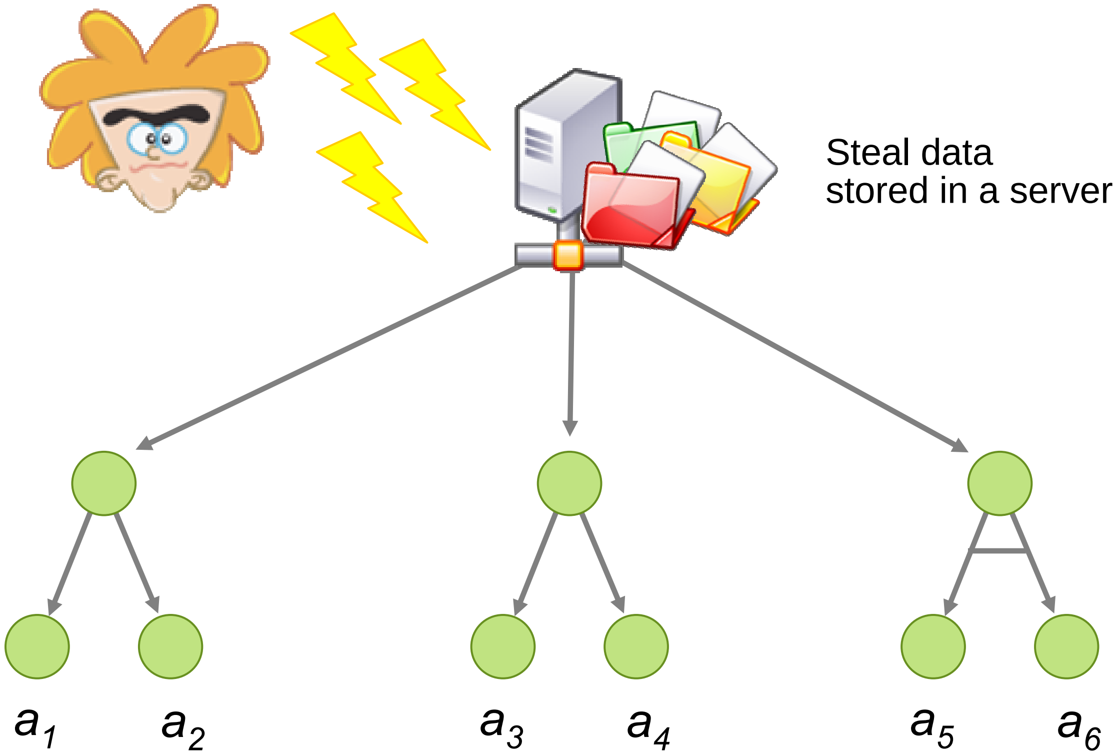
Defence trees (example)



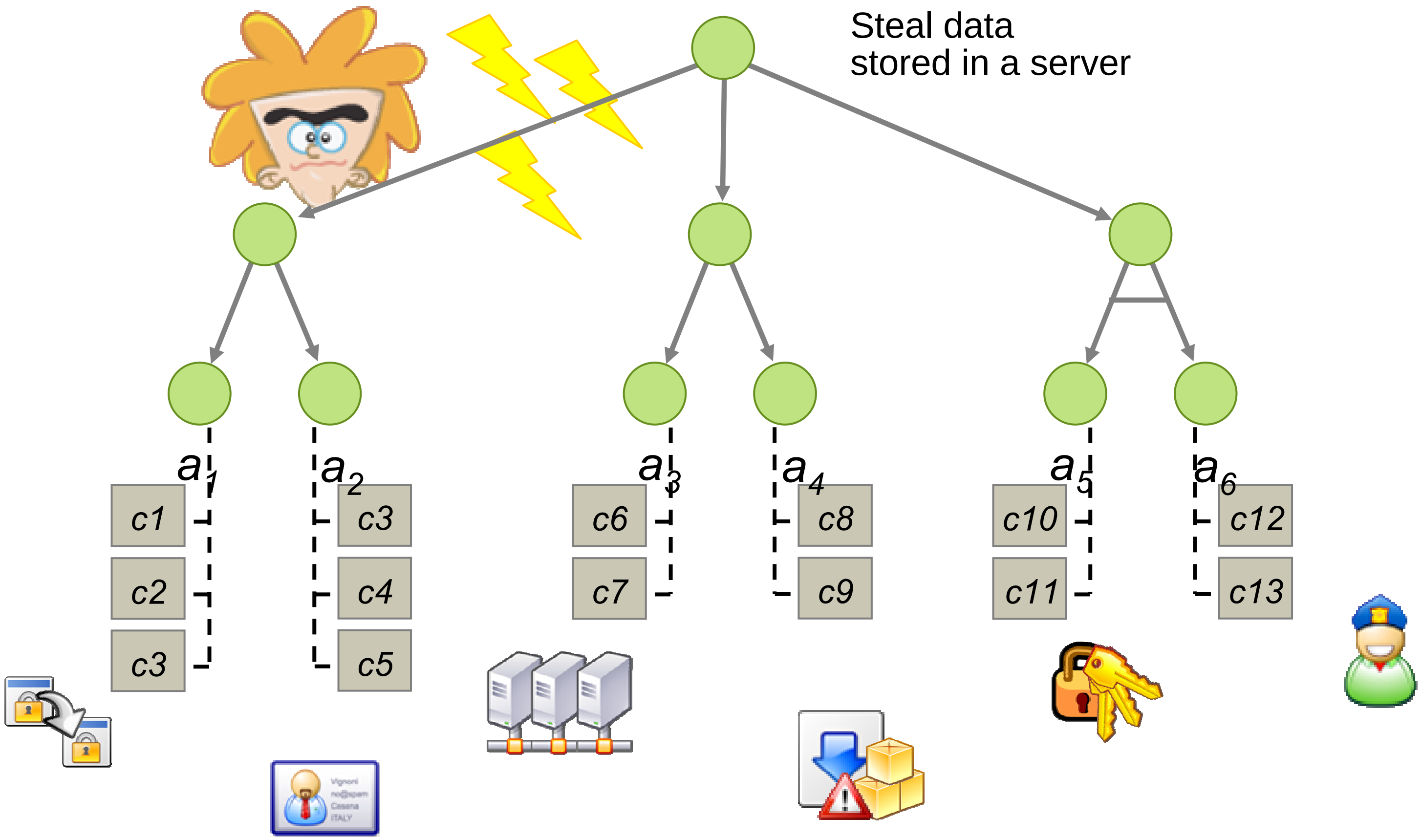
Defence trees (example)



Defence trees (example)



Defence trees (example)



Cp-nets

Conditional preference networks [Boutiliet99] are a graphical formalism to specify and representing conditional preference relations.

* Preferences over attack
* Conditional preferences over countermeasures

… more dangerous then …

a_2

Obtain root privileges corrupting a user

$\succ$

a_1

Obtain root privileges stealing access

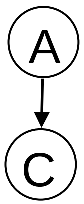
$a_2 \succ a_1$

Cp-nets

Conditional preference networks [Boutiliet99] are a graphical formalism to specify and representing conditional preference relations.

- Preferences over attack
- Conditional preferences over countermeasures

… less expensive then …



a_1	$c_1 \succ c_3$

a_1

Obtain root privileges stealing access **:**

c_1

Change the password periodically $\succ$

c_3

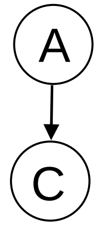
Add an identification token

Agenda

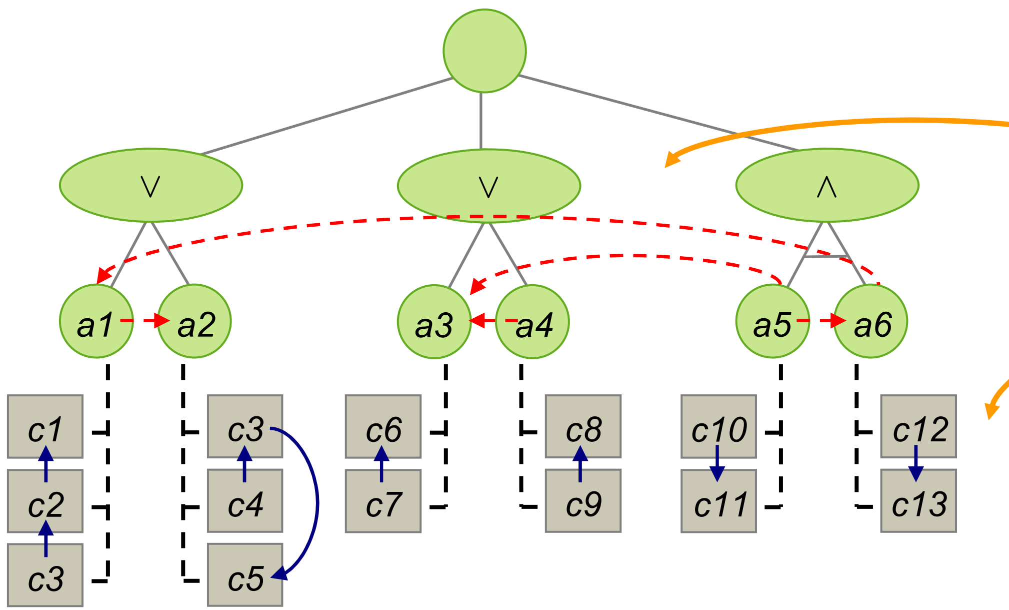
- Instruments
  - Defence trees
  - Cp-networks
- CP-defence trees
  - and-composition of attacks
  - or-composition of attacks
- From CP-defence trees to ASO programs:
  - Modelling defence tree
  - Modelling preferences among attacks and countermeasures
- Implementation

Cp-defence tree

Cp-defence tree is a defence tree enriched with conditional preference over attack and countermeasures.



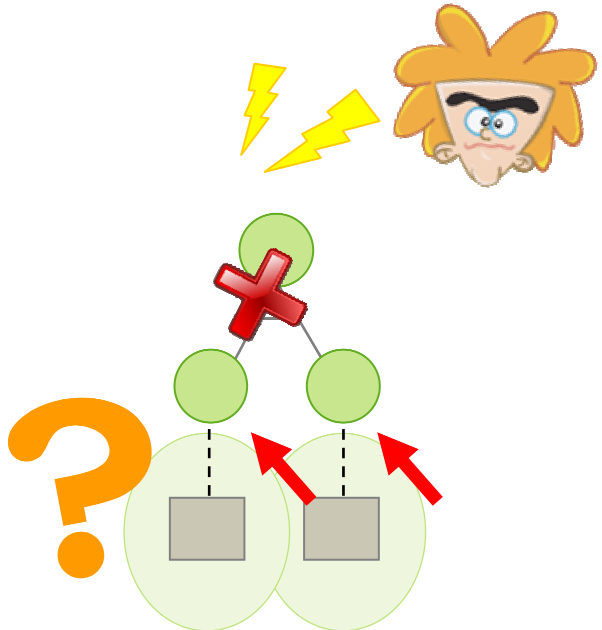
$a_2 \succ a_1 \succ a_6 \succ a_5 \succ a_3 \succ a_4$



a_1	$c_1 \succ c_2 \succ c_3$
a_2	$c_5 \succ c_3 \succ c_4$
a_3	$c_6 \succ c_7$
a_4	$c_8 \succ c_9$
a_5	$c_{11} \succ c_{10}$
a_6	$c_{13} \succ c_{12}$

and-composition

An and-attack is an attack composed by a set of actions that an attacker has to successfully achieve to obtain his goal.

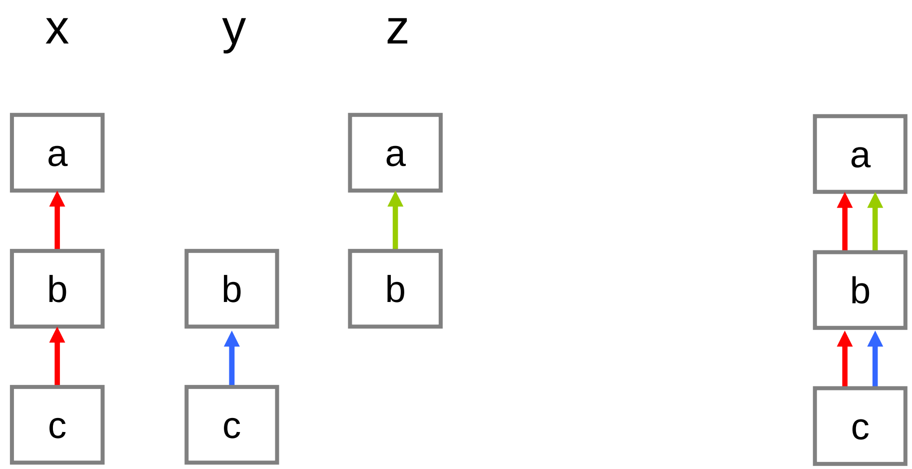


How to combine the preferences for the countermeasure associated to each attack action?

and-composition (example)

A = {x,y,z}
C = {a,b,c}

x	$a \succ b \succ c$
y	$b \succ c$
z	$a \succ b$



$x \wedge y \wedge z : a \succ b \succ c$

and-composition

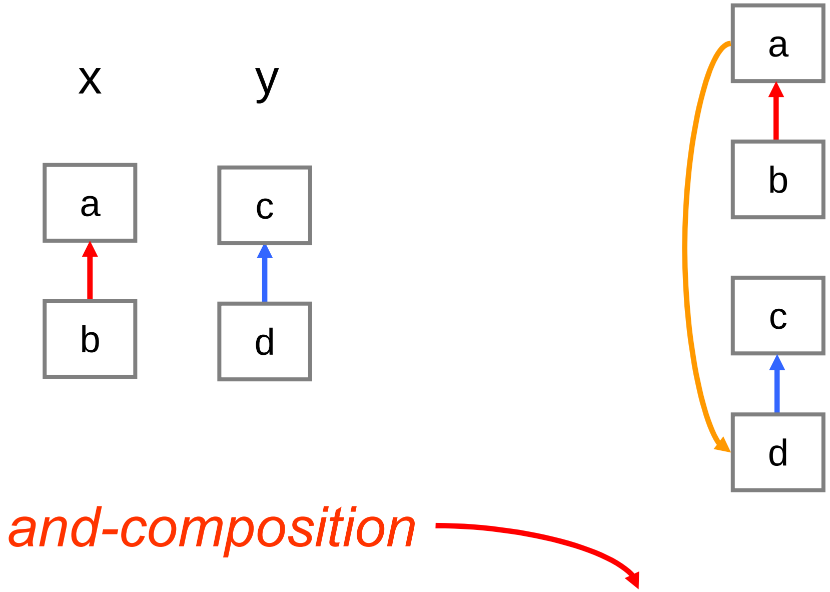
A countermeasure is preferred to another one if it is preferred in, at least, one of the partial orders.

and-composition (example 2)

$A = \{x,y\}$
$C = \{a,b,c,d\}$

x	$a \succ b$
y	$c \succ d$

$x \succ y$



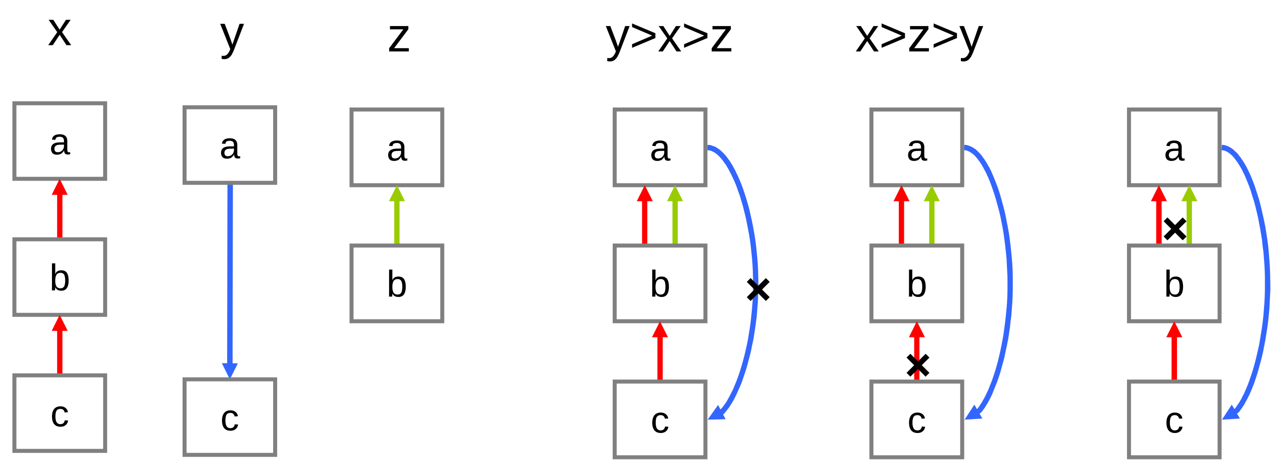
$x \wedge y : c \succ d \succ a \succ b$

We have also to consider the preferences over the value of the parent variable

and-composition: cycle

A = {x,y,z}
C = {a,b,c}

x	$a \succ b \succ c$
y	$b \succ c$
z	$a \succ b$

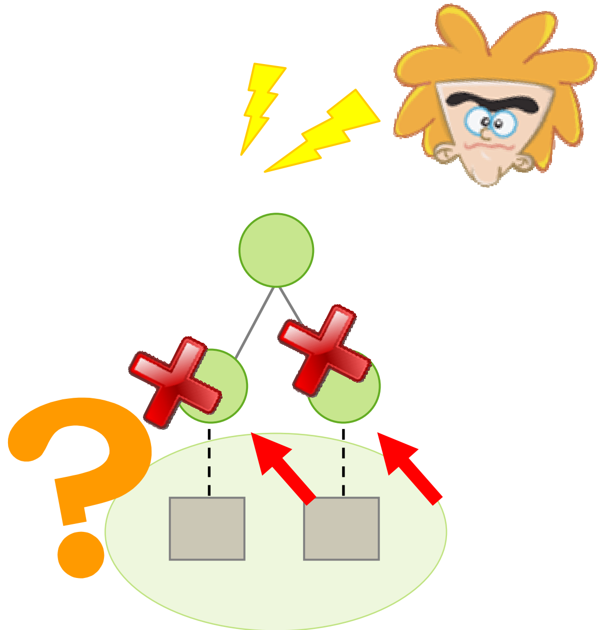


If we have any cycle we can:

- consider the preference between the parents of the variable to delete some edge
- use some algorithms as the Floyd's algorithm for remove cycles

or-composition

An `or`-attack is an attack that can be performed with different and alternative actions: the attacker can complete successfully any of its actions to obtain his goal

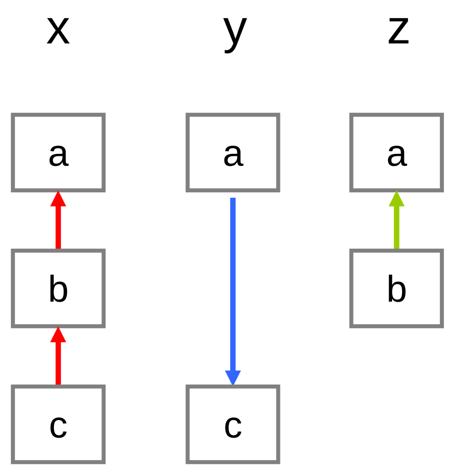


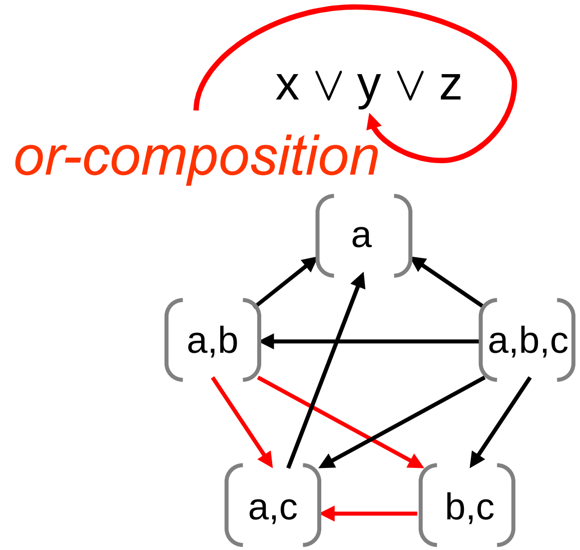
How to combine the preferences associated to each action that compose the attack and determine sets of countermeasures?

or-composition (example)

A = {x,y,z}
C = {a,b,c}

x	a $\succ$ b $\succ$ c
y	c $\succ$ a
z	a $\succ$ b



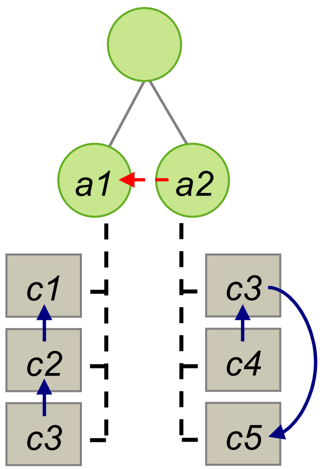


[a]
[a,b]
[a,c]
[b,c]
[a,b,c]

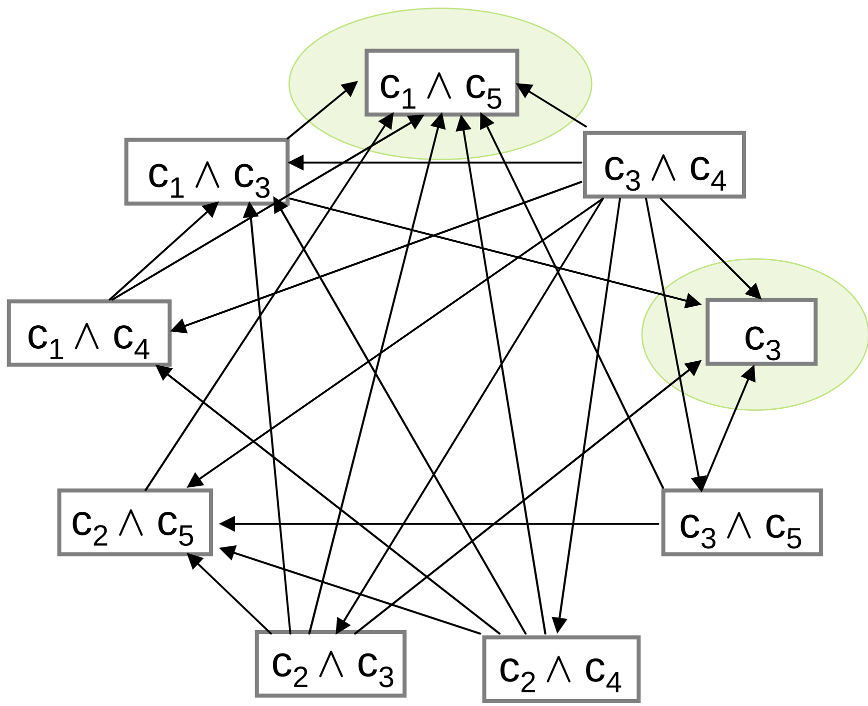
<a,a,a> *<a,a,b>*
<a,c,a> *<a,c,b>*
<b,a,a> *<b,a,b>*
<b,c,a> *<b,c,b>*
<c,a,a> *<c,a,b>*
<c,c,a> *<c,c,b>*

[b,c] $\succ$ [a,b]

or-composition: example



$a_1 \vee a_2$



Agenda

* Instruments
  * Defence trees
  * Cp-networks
* CP-defence trees
  * and-composition of attacks
  * or-composition of attacks
* From CP-defence trees to ASO programs:
  * Modelling defence tree
  * Modelling preferences among attacks and countermeasures
* Implementation

Answer Set Optimization

An answer set optimization program <P, Φ>, where P is a logic program and Φ is a set of preference rules.

- P defines the set of possible solutions,
- Φ establishes the preference order among them.

$a_{56} \leftarrow$

$a_5 \vee a_6 \leftarrow a_{56}$

$c_{10} \vee c_{11} \leftarrow a_5$

$c_{12} \vee c_{13} \leftarrow a_6$

$c_{13} > c_{12} \leftarrow a_6$

$c_{11} > c_{10} \leftarrow a_5$

The preference rule intuitively reads: *c_{13} is preferable over c_{12} if a_6 is true*

~~$M_1 = \{ a_{56}, a_5, c_{10} \}$~~

~~$M_2 = \{ a_{56}, a_5, c_{11} \}$~~

~~$M_3 = \{ a_{56}, a_6, c_{12} \}$~~

$M_3 = \{ a_{56}, a_6, c_{13} \}$

Ranking: the first rule is more important than the second one

and-composition

P_x $r_{x1}: x \leftarrow$

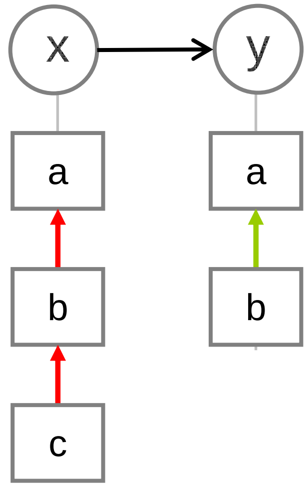
$r_{x2}: a \vee b \vee c \leftarrow x$

Φ $\rho_{x1}: a > b > c \leftarrow x$

P_y $r_{y1}: y \leftarrow$

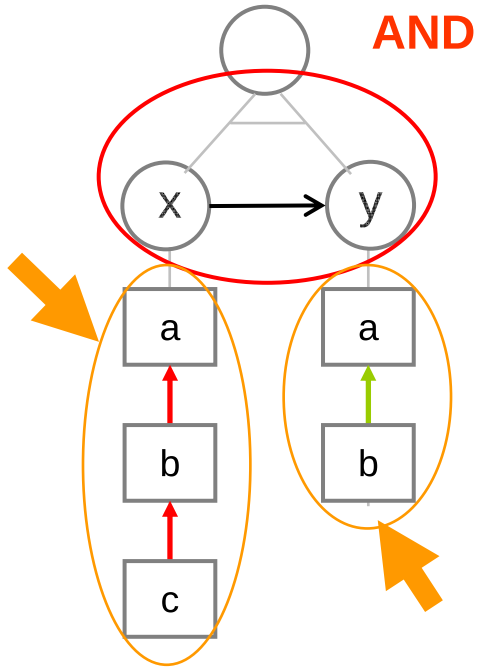
$r_{y2}: a \vee b \leftarrow y$

Φ $\rho_{y1}: a > b \leftarrow y$



and-composition

P_x	r_{x1}: x ←	P_{and}	r_1: root ←
	r_{x2}: a ∨ b ∨ c ← x		r_2: x ∨ y ← root
Φ	ρ_{x1}: a > b > c ← x		
P_y	r_{y1}: y ←	Φ	
	r_{y2}: a ∨ b ← y		
Φ	ρ_{y1}: a > b ← y		



The optimal answer set associated to <P_{and}, Φ> is the set M_4={root, x,a}

The preferred set of countermeasures is the set {a}.

or-composition

P_x $r_{x1}: x \leftarrow$

$r_{x2}: a \vee b \vee c \leftarrow x$

Φ $\rho_{x1}: a > b > c \leftarrow x$

OR

P_{or}

$r_1: root' \leftarrow$

$r_2: x \leftarrow root'$

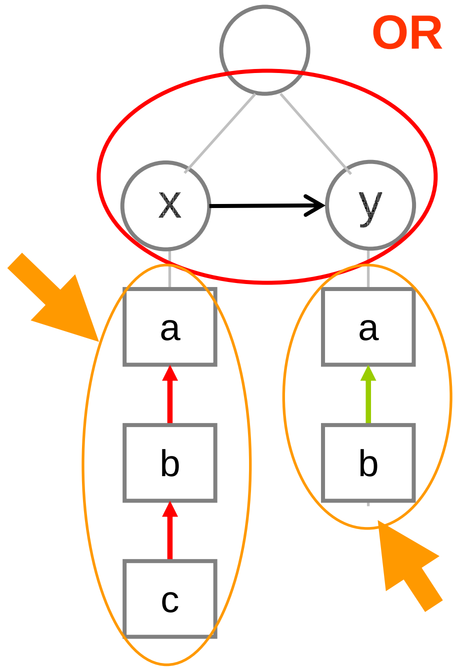
$r_3: y \leftarrow root'$

P_y $r_{y1}: y \leftarrow$

$r_{y2}: a \vee b \leftarrow y$

Φ $\rho_{y1}: a > b \leftarrow y$

Φ



The optimal answer set associated to <P_{or}, Φ> is M'_1={root', x, y, a}

The preferred set of countermeasures is the set {a}.

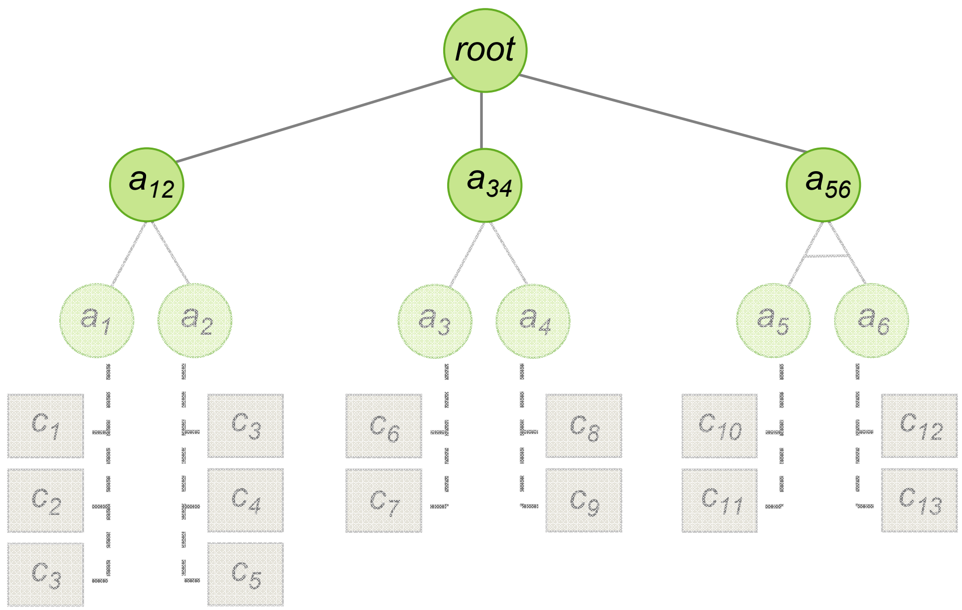
ASO and CP-defence tree

root ←

a_{12} ← root

a_{34} ← root

a_{56} ← root



ASO and CP-defence tree

Logic programming

root ←

a_{12} ← root

a_{34} ← root

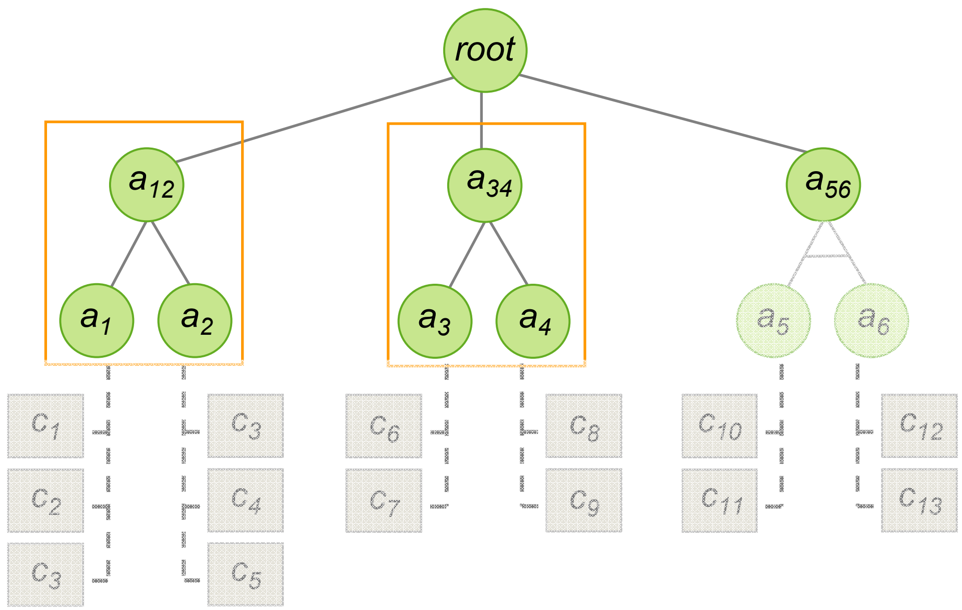
a_{56} ← root

a_1 ← a_{12}

a_2 ← a_{12}

a_3 ← a_{34}

a_4 ← a_{34}



ASO and CP-defence tree

Logic programming

root ←

a_{12} ← root

a_{34} ← root

a_{56} ← root

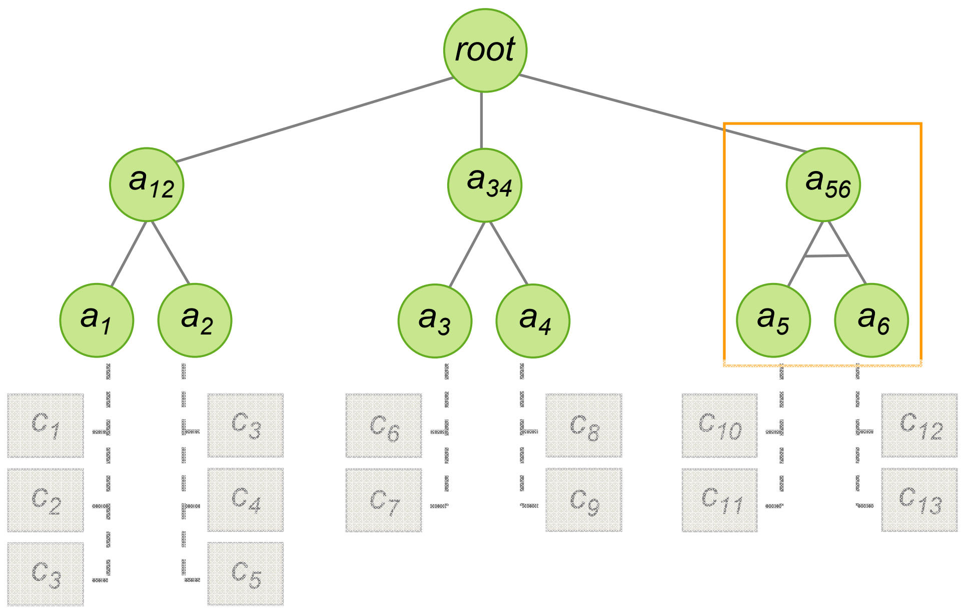
a_1 ← a_{12}

a_2 ← a_{12}

a_3 ← a_{34}

a_4 ← a_{34}

$a_5 \vee a_6$ ← a_{56}



ASO and CP-defence tree

Logic programming

$root \leftarrow$

$a_{12} \leftarrow root$

$a_{34} \leftarrow root$

$a_{56} \leftarrow root$

$a_1 \leftarrow a_{12}$

$a_2 \leftarrow a_{12}$

$a_3 \leftarrow a_{34}$

$a_4 \leftarrow a_{34}$

$a_5 \vee a_6 \leftarrow a_{56}$

$c_1 \vee c_2 \vee c_3 \leftarrow a_1$

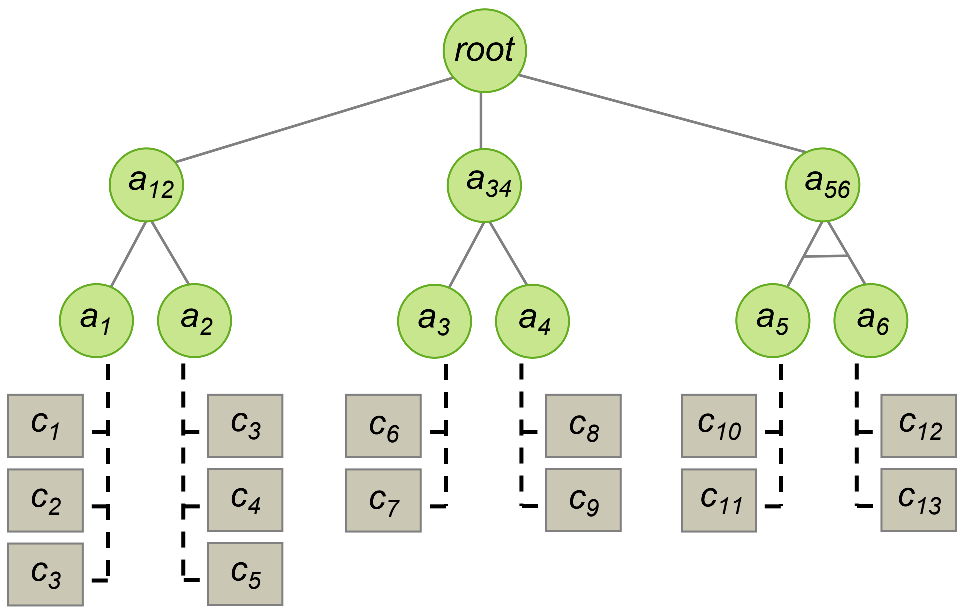
$c_3 \vee c_4 \vee c_5 \leftarrow a_2$

$c_6 \vee c_7 \leftarrow a_3$

$c_8 \vee c_9 \leftarrow a_4$

$c_{10} \vee c_{11} \leftarrow a_5$

$c_{12} \vee c_{13} \leftarrow a_6$



ASO and CP-defence tree

Conditional preference rules

$c_1 > c_2 > c_3 \leftarrow a_1$

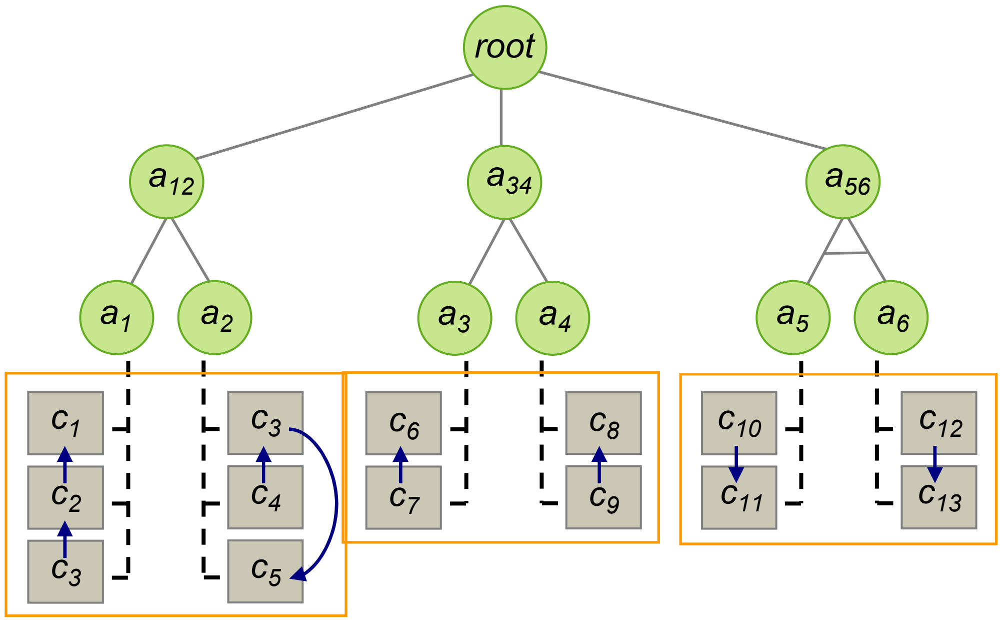
$c_5 > c_3 > c_4 \leftarrow a_2$

$c_6 > c_7 \leftarrow a_3$

$c_8 > c_9 \leftarrow a_4$

$c_{11} > c_{10} \leftarrow a_5$

$c_{13} > c_{12} \leftarrow a_6$



ASO and CP-defence tree

Ranking of preference rules

Φ_1 $c_1 > c_2 > c_3 \leftarrow a_1$

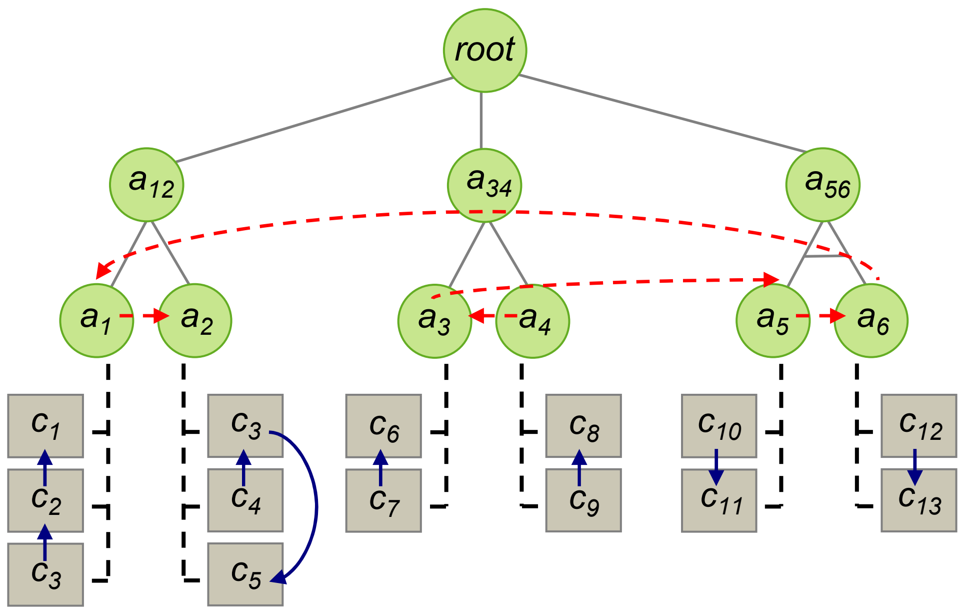
Φ_2 $c_5 > c_3 > c_4 \leftarrow a_2$

Φ_3 $c_6 > c_7 \leftarrow a_3$

Φ_4 $c_8 > c_9 \leftarrow a_4$

Φ_5 $c_{11} > c_{10} \leftarrow a_5$

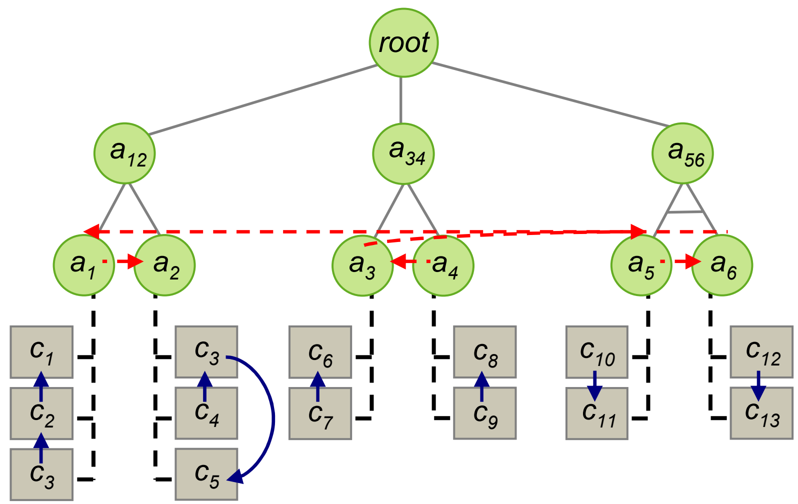
Φ_6 $c_{13} > c_{12} \leftarrow a_6$



ASO and CP-defence tree

$root \leftarrow$
$a_{12} \leftarrow root$
$a_{34} \leftarrow root$
$a_{56} \leftarrow root$
$a_1 \leftarrow a_{12}$
$a_2 \leftarrow a_{12}$
$a_3 \leftarrow a_{34}$
$a_4 \leftarrow a_{34}$
$a_5 \vee a_6 \leftarrow a_{56}$

$c_1 \vee c_2 \vee c_3 \leftarrow a_1$
$c_3 \vee c_4 \vee c_5 \leftarrow a_2$
$c_6 \vee c_7 \leftarrow a_3$
$c_8 \vee c_9 \leftarrow a_4$
$c_{10} \vee c_{11} \leftarrow a_5$
$c_{12} \vee c_{13} \leftarrow a_6$



$\Phi_1 \quad c_5 > c_3 > c_4 \leftarrow a_2$
$\Phi_2 \quad c_1 > c_2 > c_3 \leftarrow a_1$
$\Phi_3 \quad c_{13} > c_{12} \leftarrow a_6$
$\Phi_4 \quad c_{11} > c_{10} \leftarrow a_5$
$\Phi_5 \quad c_6 > c_7 \leftarrow a_3$
$\Phi_6 \quad c_8 > c_9 \leftarrow a_4$

$M = \{ root, a_{12}, a_{34}, a_{56}, a_1, a_2, a_3, a_4, c_1, c_5, c_6, c_8, a_6, c_{13} \}$

Best set of countermeasures: $\{c_1, c_5, c_6, c_8, c_{13}\}$

Agenda

- Instruments
  - Defence trees
  - Cp-networks
- CP-defence trees
  - and-composition of attacks
  - or-composition of attacks
- From CP-defence trees to ASO programs:
  - Modelling defence tree
  - Modelling preferences among attacks and countermeasures
- Implementation

Implementation