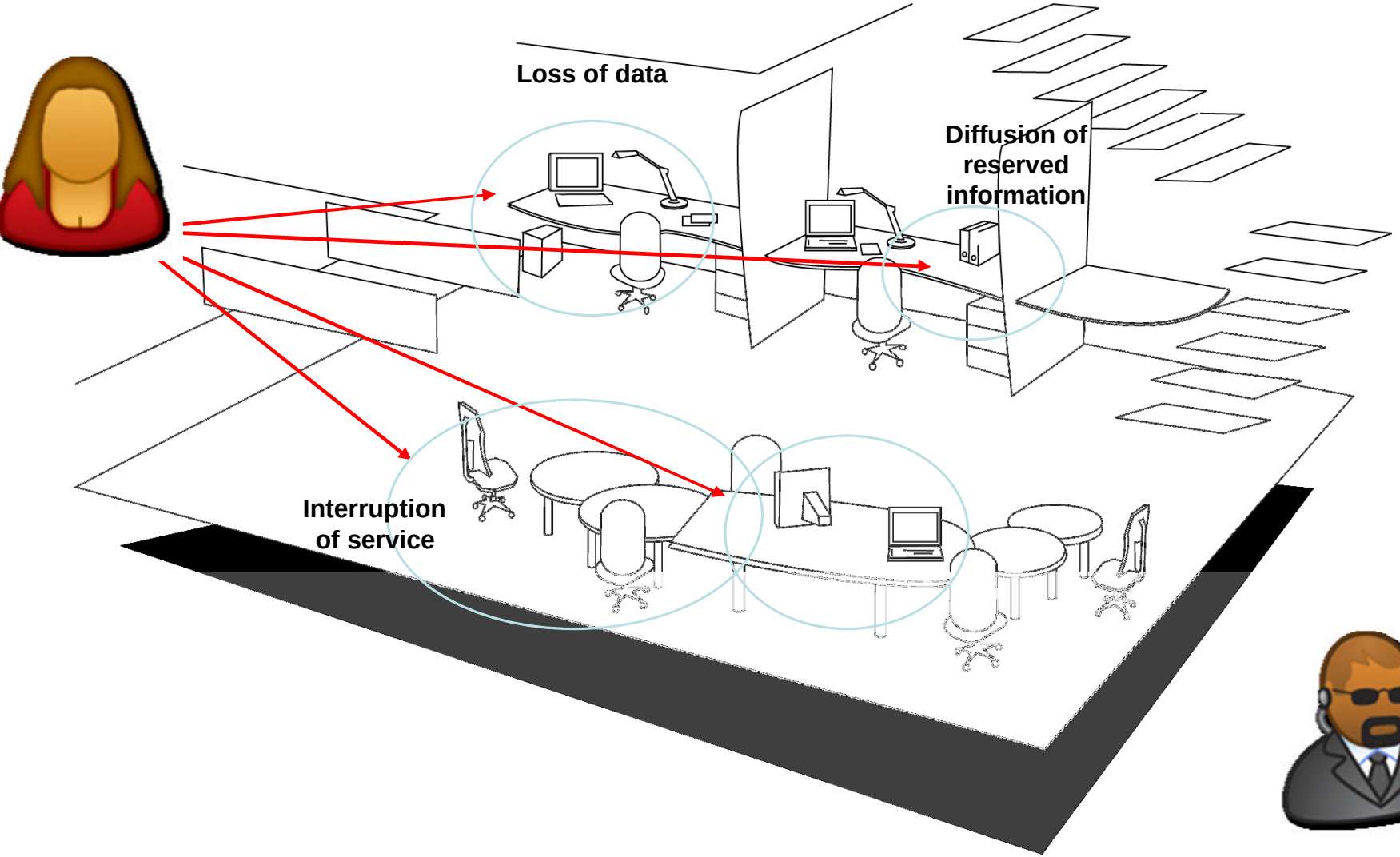
Defense trees for economic evaluation of security investments

Stefano Bistarelli **Fabio Fioravanti** **Pamela Peretti**

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

What is the problem?



How to protect an organization's asset?

Motivation

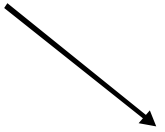
- Create a *process* to identify, describe and analyze the possible vulnerabilities of a system
- Provide an *economic balance* between the economic impact of risk and the cost of risk mitigation

Agenda

Background

- Qualitative approach
  - Attack trees
- Quantitative approach
  - Economic indexes

- **Defense trees = Attack tree + countermeasures**
- **Defense trees + quantitatives labels**



Economic evaluation of countermeasures

Qualitative approach

A relative evaluation of:

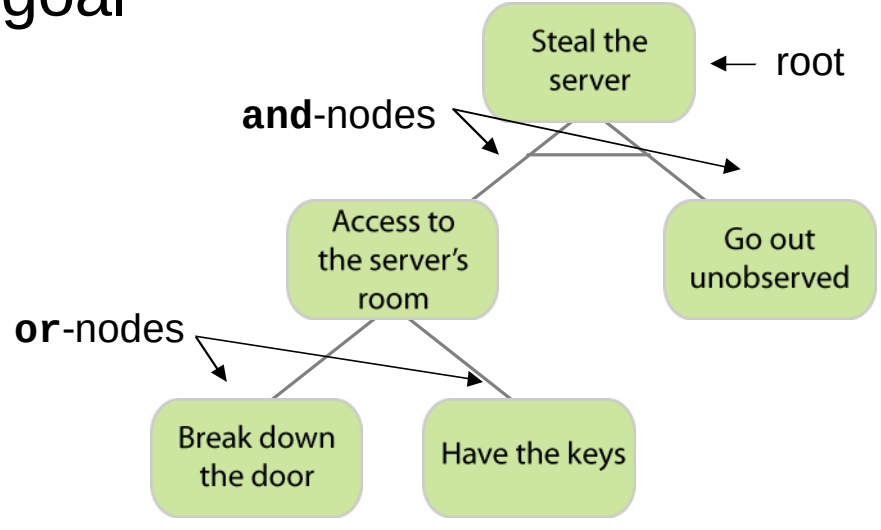
- assets
- threats and vulnerabilities
- countermeasures

Scenario analysis ⟶ **Attack trees**

Attack trees

An *attack tree* [Schneier00] is a tree-based structure where:

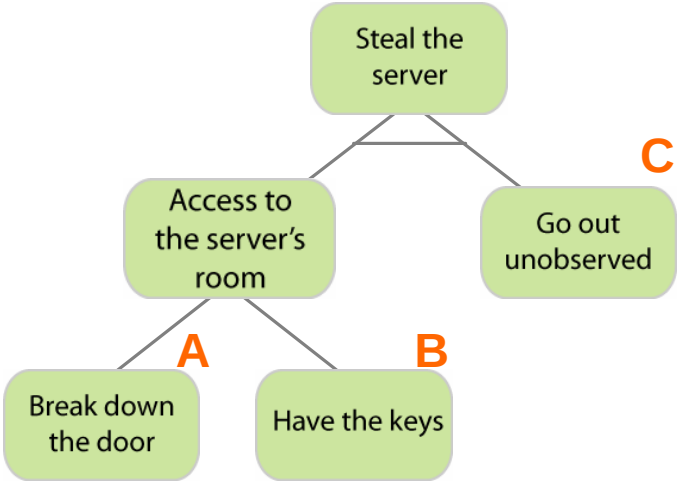
- the root is an asset of an IT system
- the paths from the root to the leaf are the way to achieve this goal
- the non-leaf nodes can be:
  - and-nodes
  - or-nodes

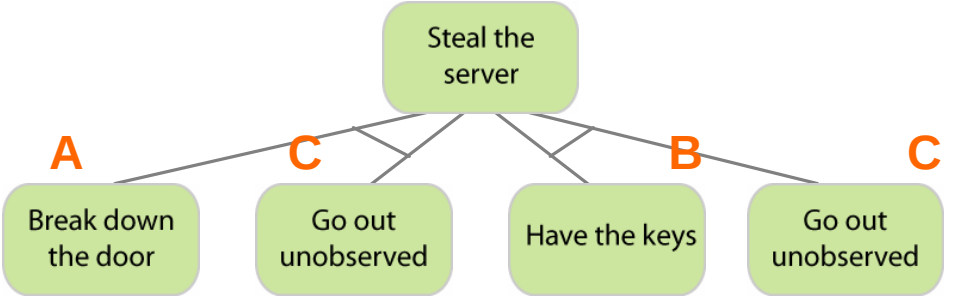


Attack trees

An attack tree can be transformed to its *Disjunctive Normal Form* [Mauw05]

((A *or* B) *and* C)=(A *and* C) *or* (B *and* C)





Quantitative approach

Assigns absolute numeric attribute values to:

- assets (asset value)
- threats and vulnerabilities (exposure factor, annualized rate of occurrence)
- countermeasures (cost, risk mitigated)

Economic Indexes

Economic Indexes

Return on Investment (ROI)

↓

a performance measure used to evaluate the efficiency of an investment

$$ROI = \frac{Gain\ from\ Investment - Cost\ of\ Investment}{Cost\ of\ Investment}$$

Agenda

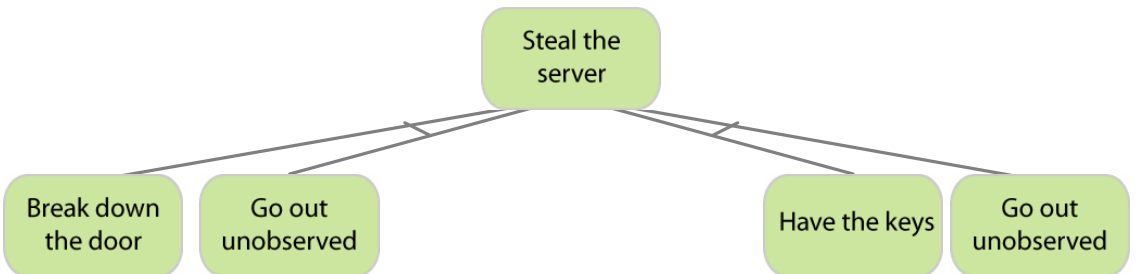
Background

- Qualitative approach
  - Attack trees
- Quantitative approach
  - Economic indexes

- **Defense trees = Attack tree + countermeasures**
- **Defense trees + quantitatives labels**

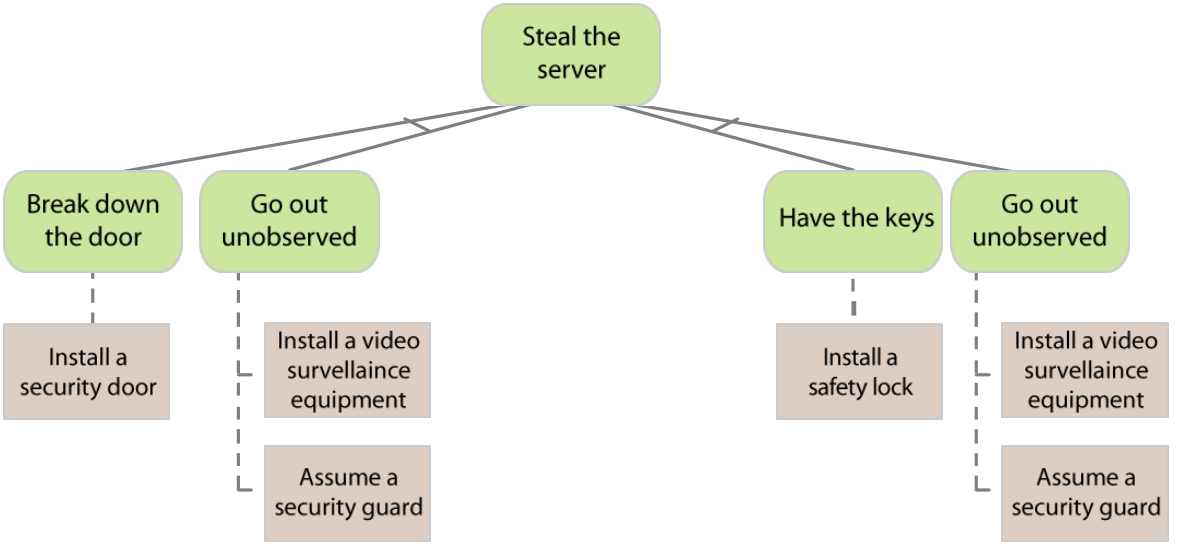
Building the defense tree

1. Create an *attack tree*,



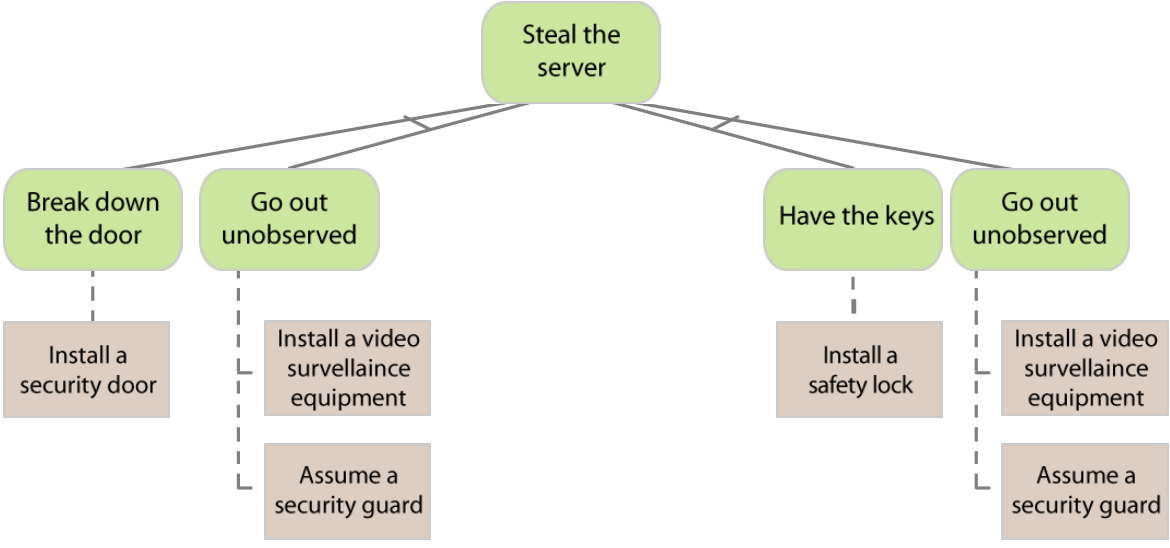
Building the defense tree

2. *Defense tree* = attack tree + countermeasures



Building the defense tree

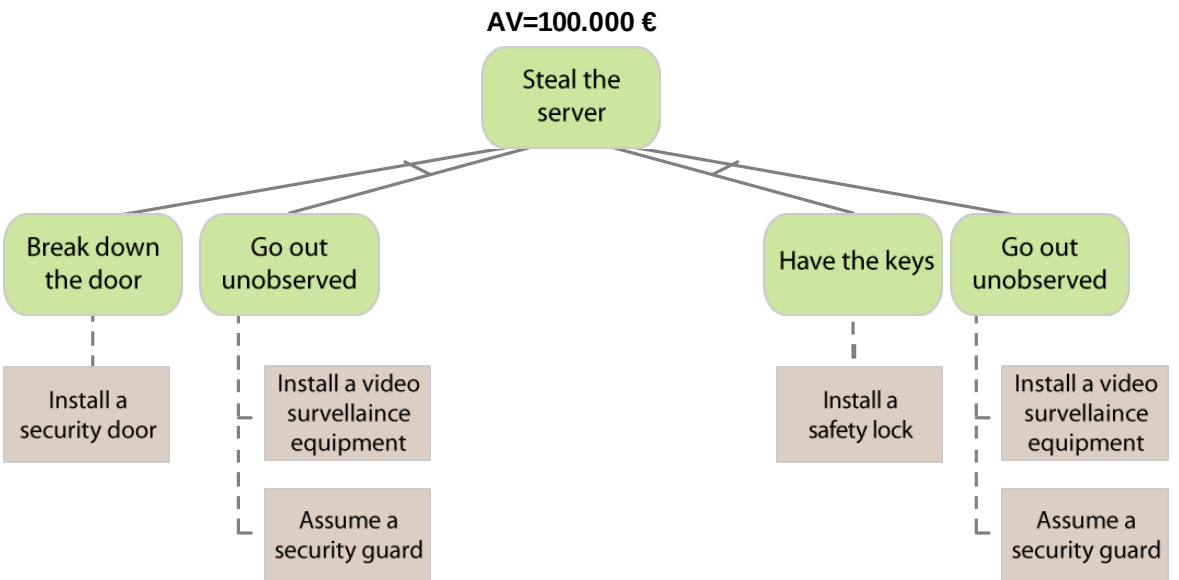
3. Label the defense tree using quantitative indexes and computing the Return on Investment



4. Label the defense tree using quantitative indexes and computing the Return on Attack [Cremonini05]

Return On Investment

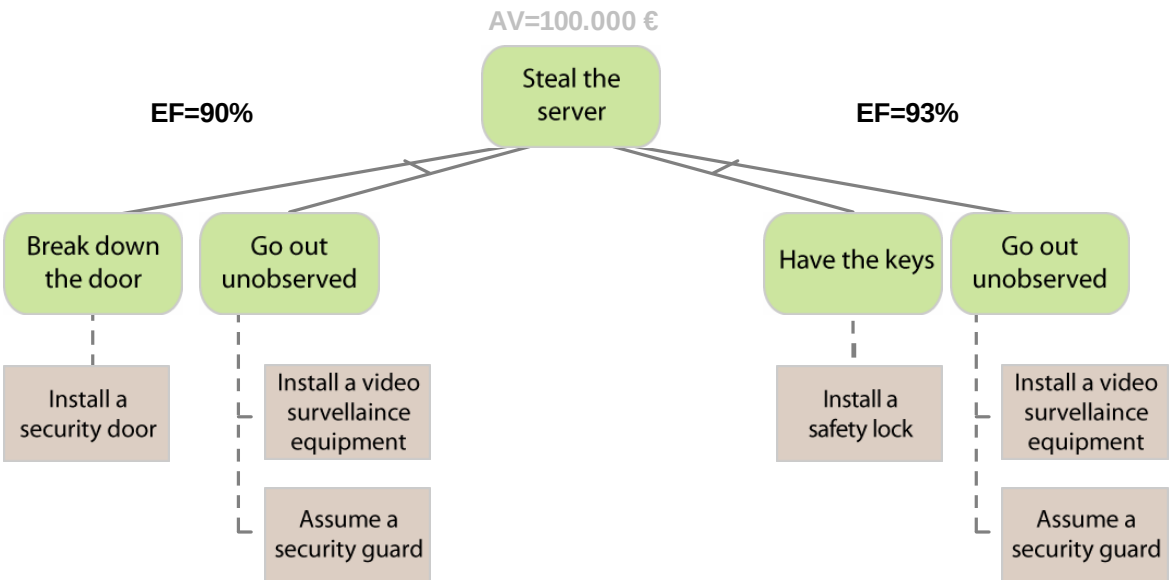
Asset Value (AV)



Return On Investment

AV Asset Value

Exposure Factor (EF)

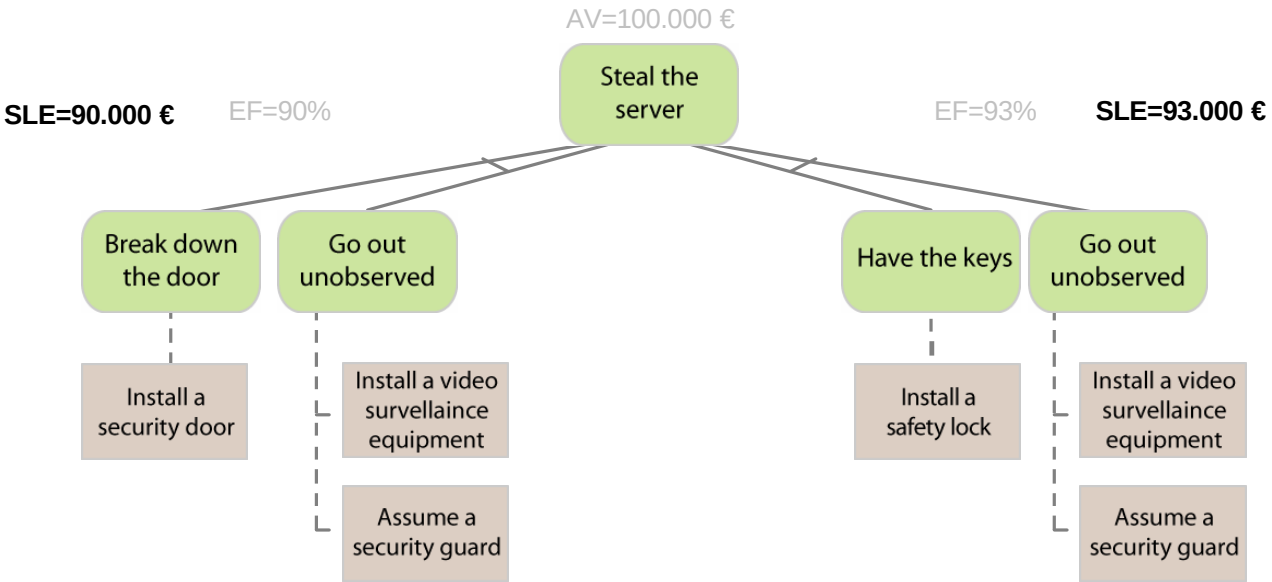


Return On Investment

AV Asset Value

EF Exposure Fact

Single Loss Exposure (SLE=AV × EF)



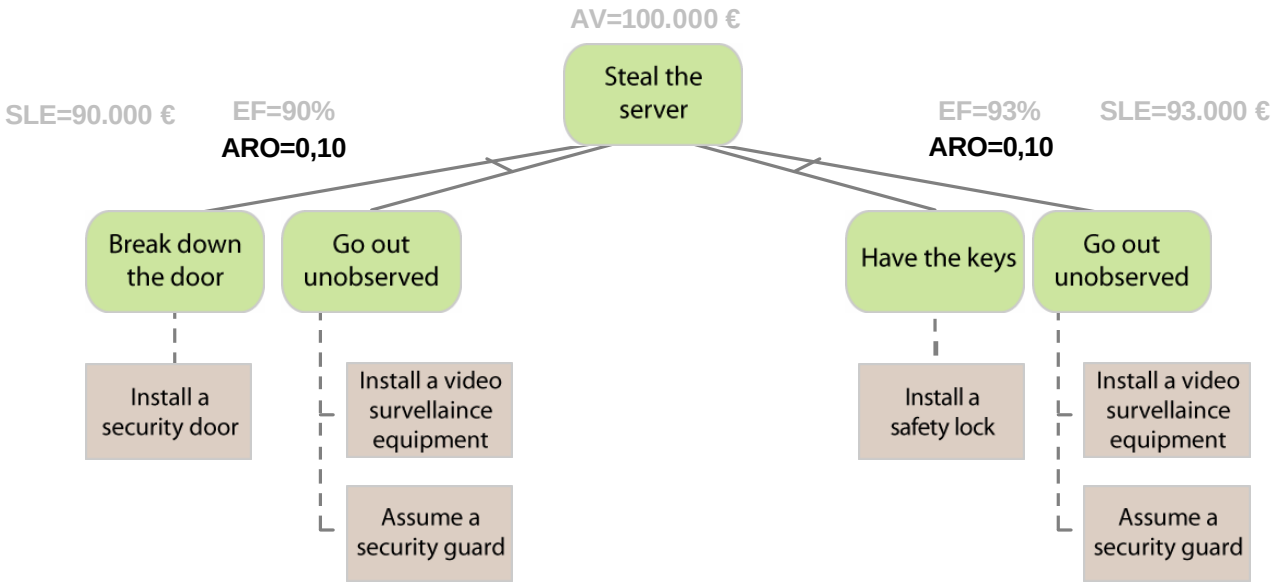
Return On Investment

Annualized Rate of Occurrence (ARO)

AV Asset Value

EF Exposure Fact

SLE Single Loss Exposure



Return On Investment

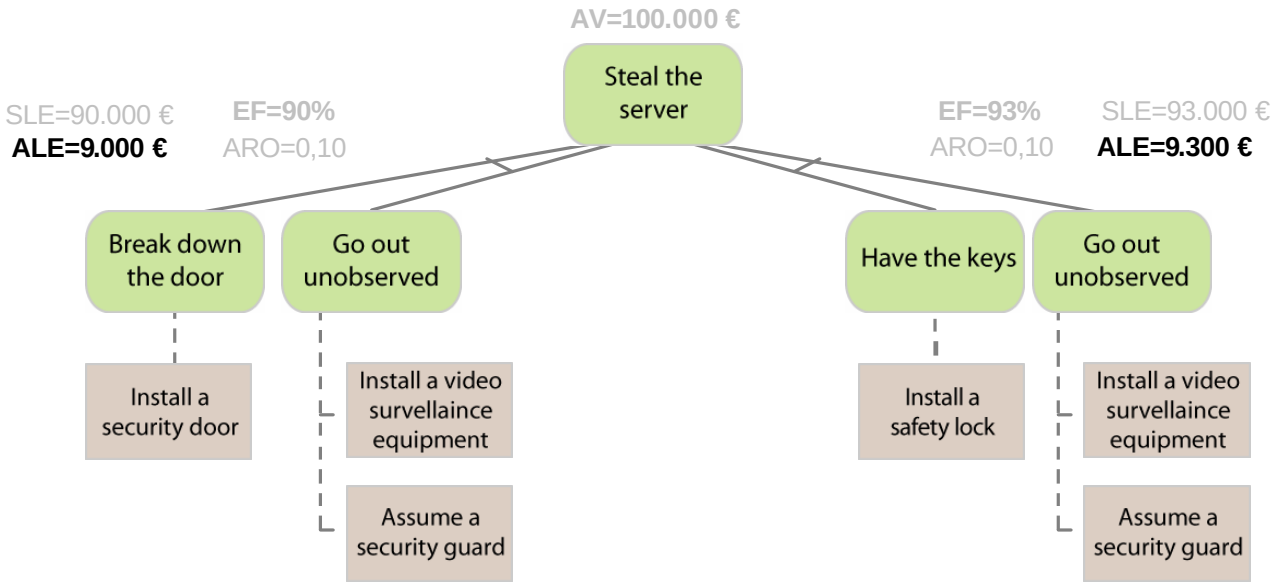
Annualized Loss Expectancy (ALE=SLE × ARO)

AV Asset Value

EF Exposure Fact

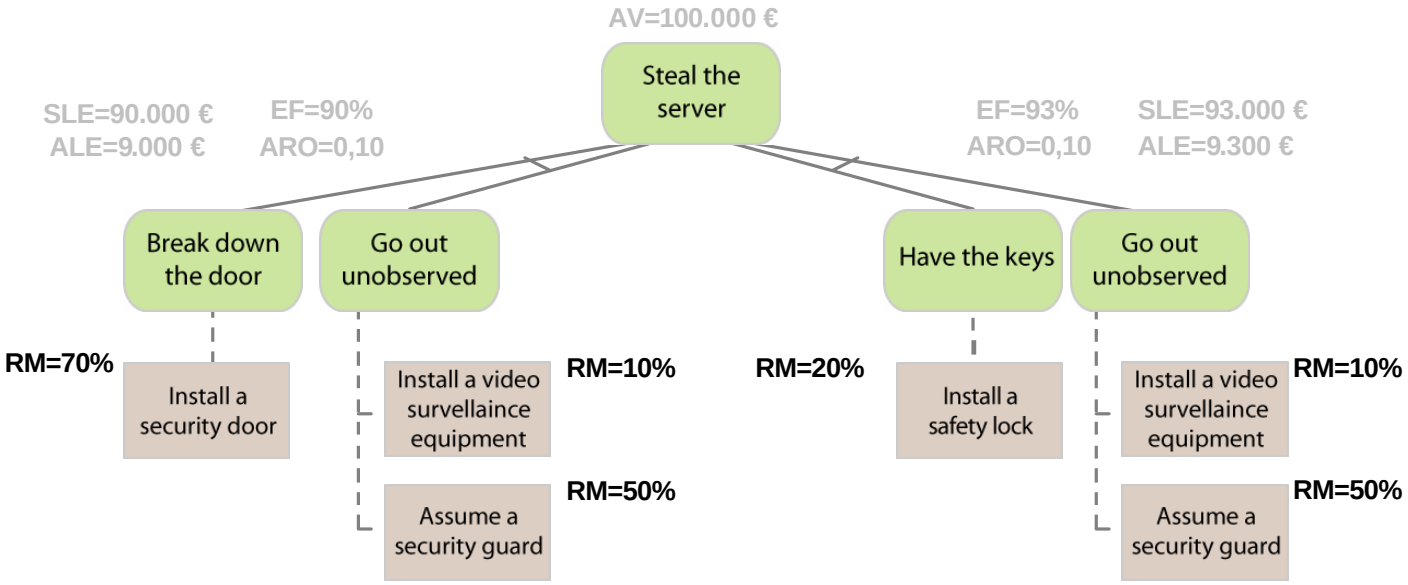
SLE Single Loss Exposure

ARO Annualized Ra of Occurrence



Return On Investment

Risk Mitigated by a countermeasure (RM)



AV Asset Value

EF Exposure Fact

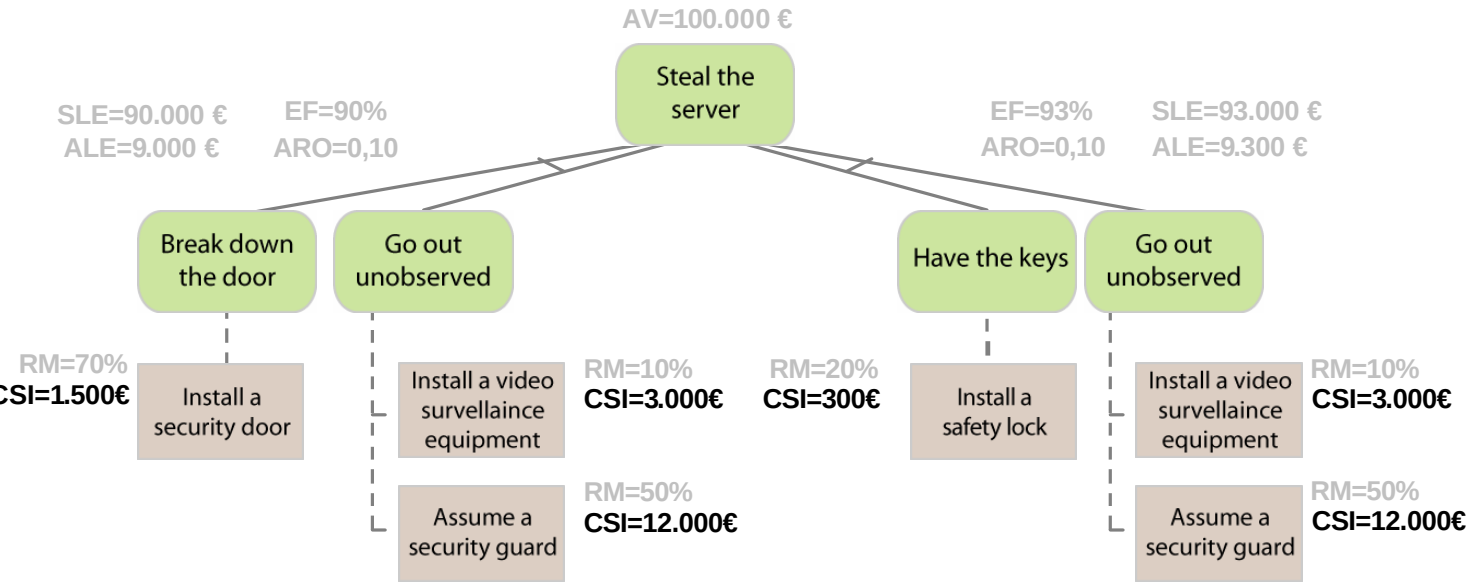
SLE Single Loss Exposure

ARO Annualized Ra of Occurrence

ALE Annualized Lo Expectancy

Return On Investment

Cost of a Security Investment (CSI)



AV Asset Value

EF Exposure Fact

SLE Single Loss Exposure

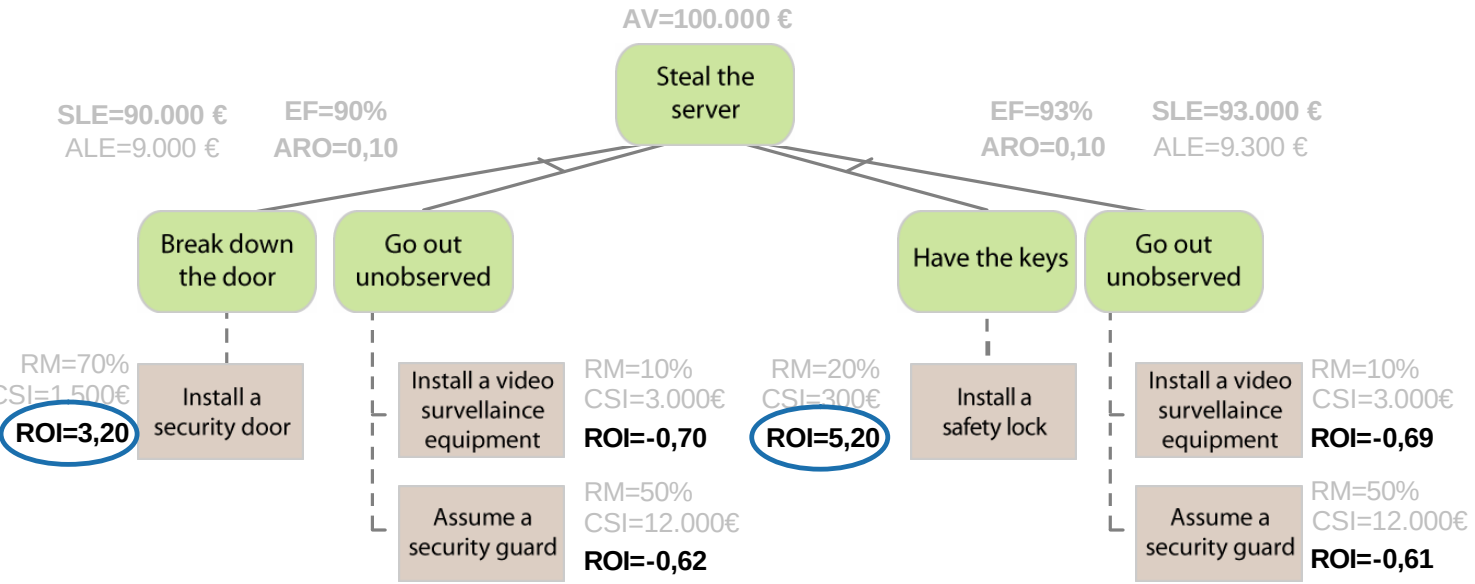
ARO Annualized Ra of Occurrence

ALE Annualized Lo Expectancy

RM Risk Mitigated

Return On Investment

$$ROI = \frac{(ALE \times RM) - CSI}{CSI}$$



AV Asset Value

EF Exposure Fact

SLE Single Loss Exposure

ARO Annualized Ra of Occurrence

ALE Annualized Lo Expectancy

RM Risk Mitigated

CSI Cost Security Investment

F.W.

- Consider **EF** as Uncertain variable with values in an interval (70<**EF**<95) (and similar for **RM**)
- Compute ROI/ROA indexes as intervals
- Study operations between intervals and notions of
  - Optimistic combination
  - Pessimistic combination
  - Robustness

  (See works by Gervet-Yorke-Smith)

AV Asset Value

EF Exposure Fact

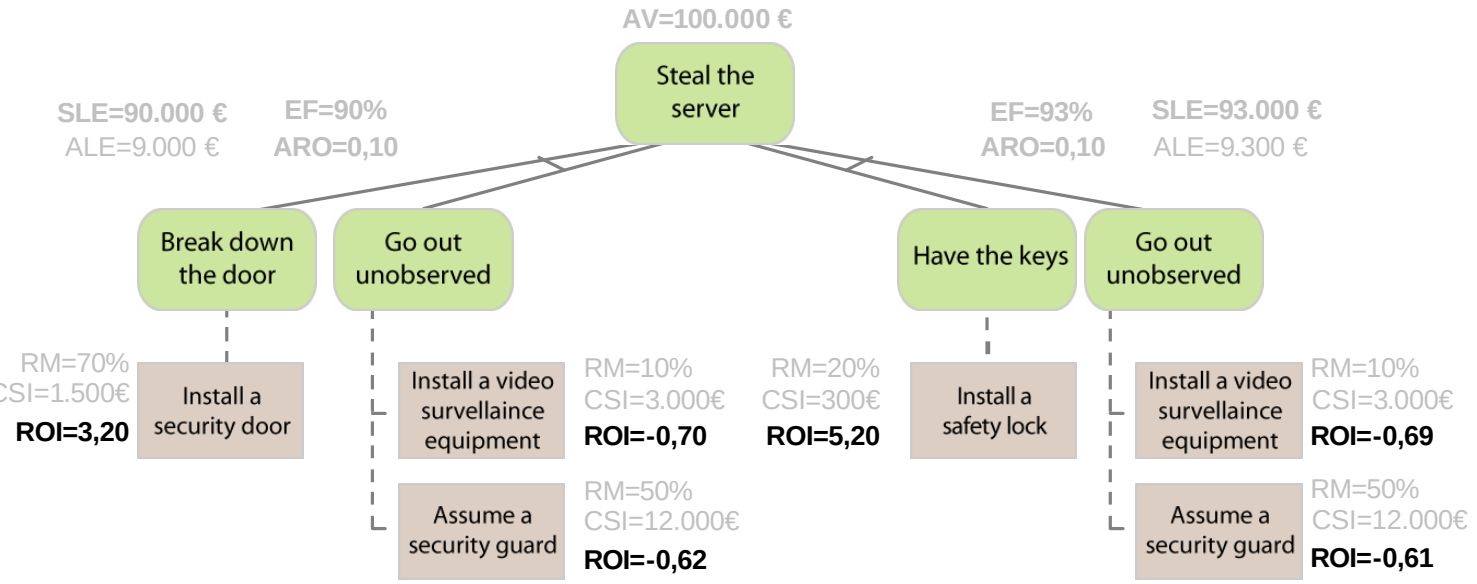
SLE Single Loss Exposure

ARO Annualized Ra of Occurrence

ALE Annualized Lo Expectancy

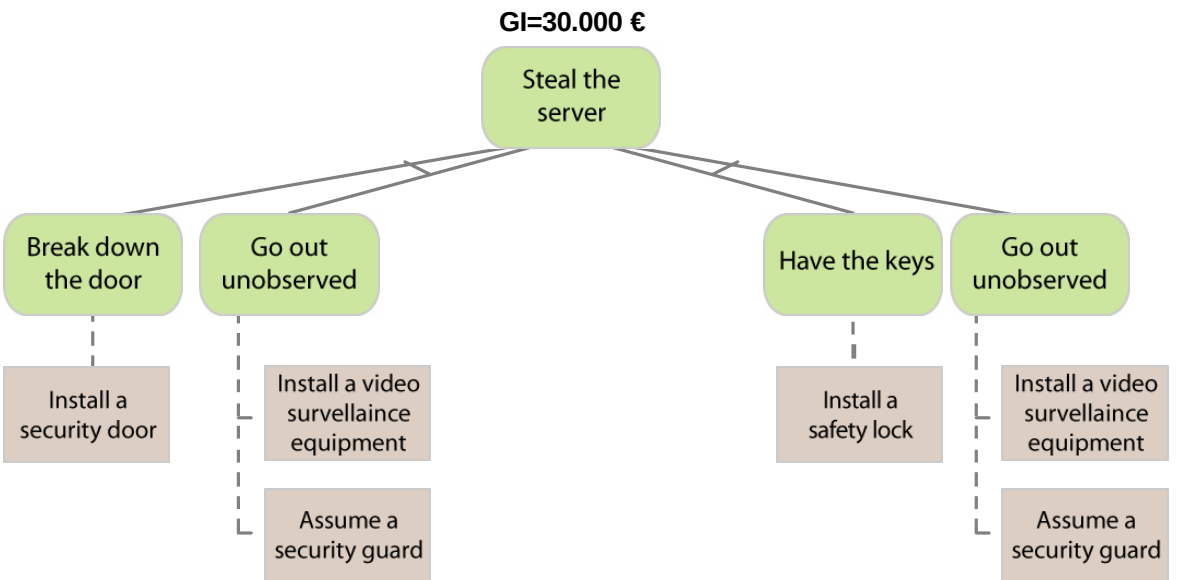
RM Risk Mitigated

CSI Cost Security Investment



Return On Attack

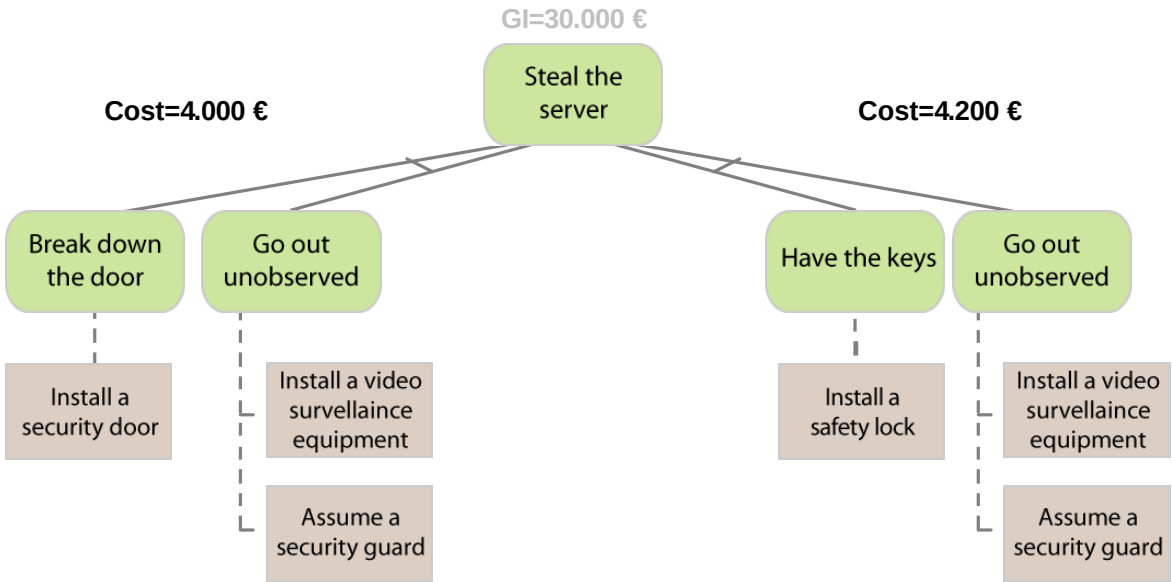
Gain that an attacker expects from an attack



Return On Attack

GI expected gain

Cost of an attack

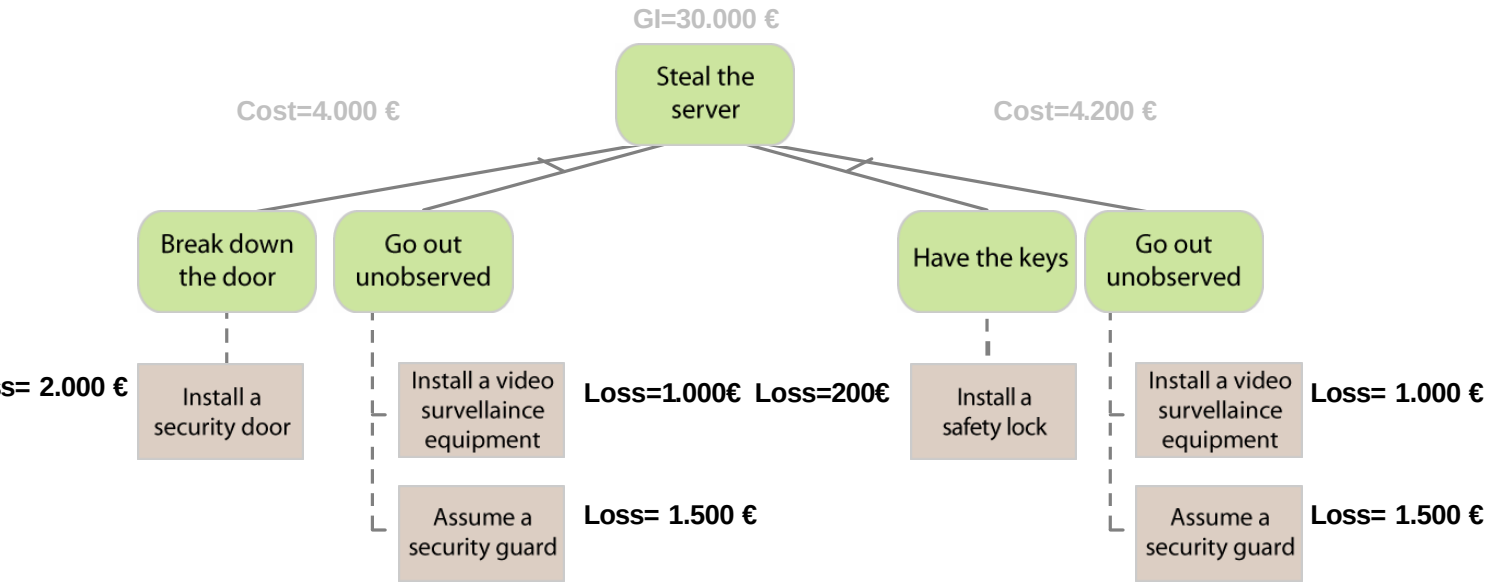


Return On Attack

GI expected gain

Cost cost before S

Additional cost *(loss)* caused by a countermeasure S



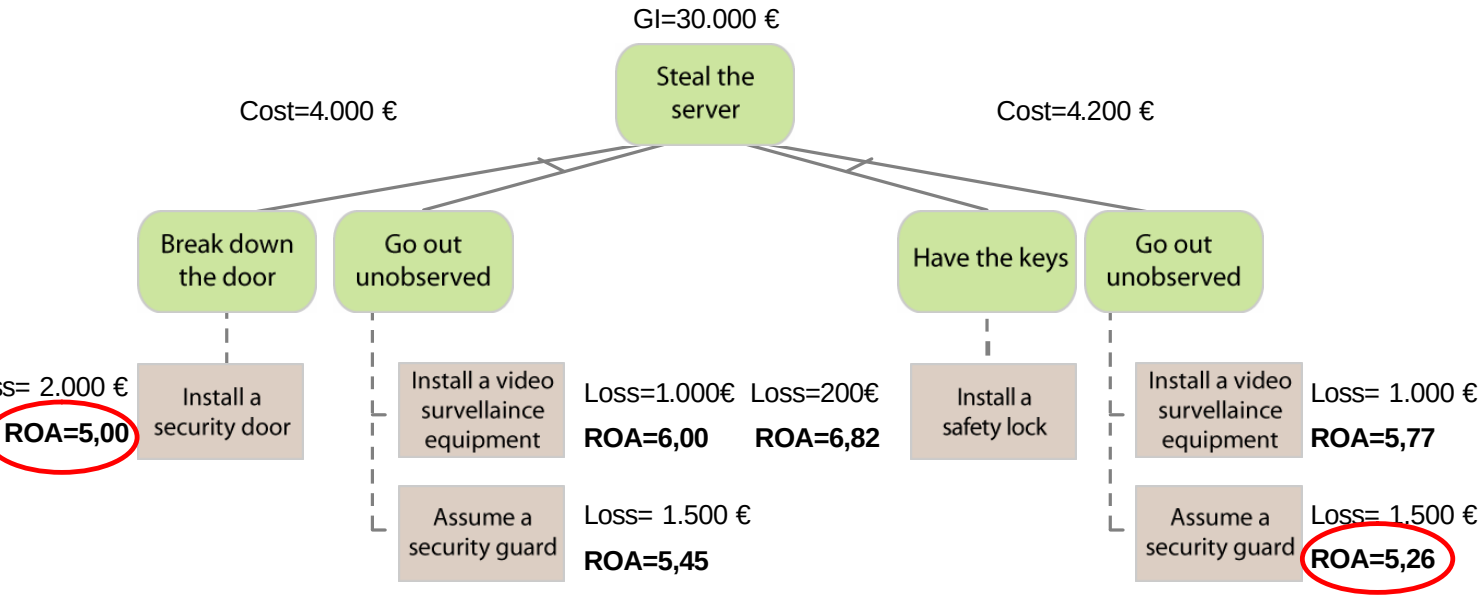
Return On Attack

$$ROA = \frac{GI}{cost\ before\ S + loss\ caused\ by\ S}$$

GI expected gain

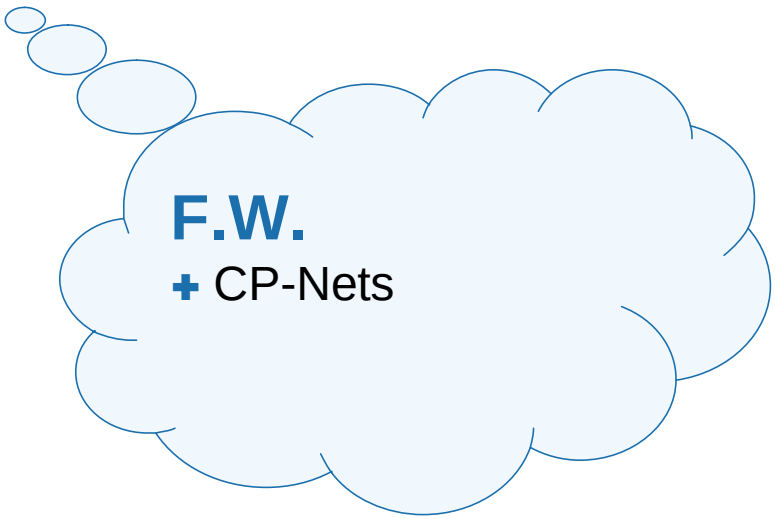
Cost cost before S

Loss loss caused by



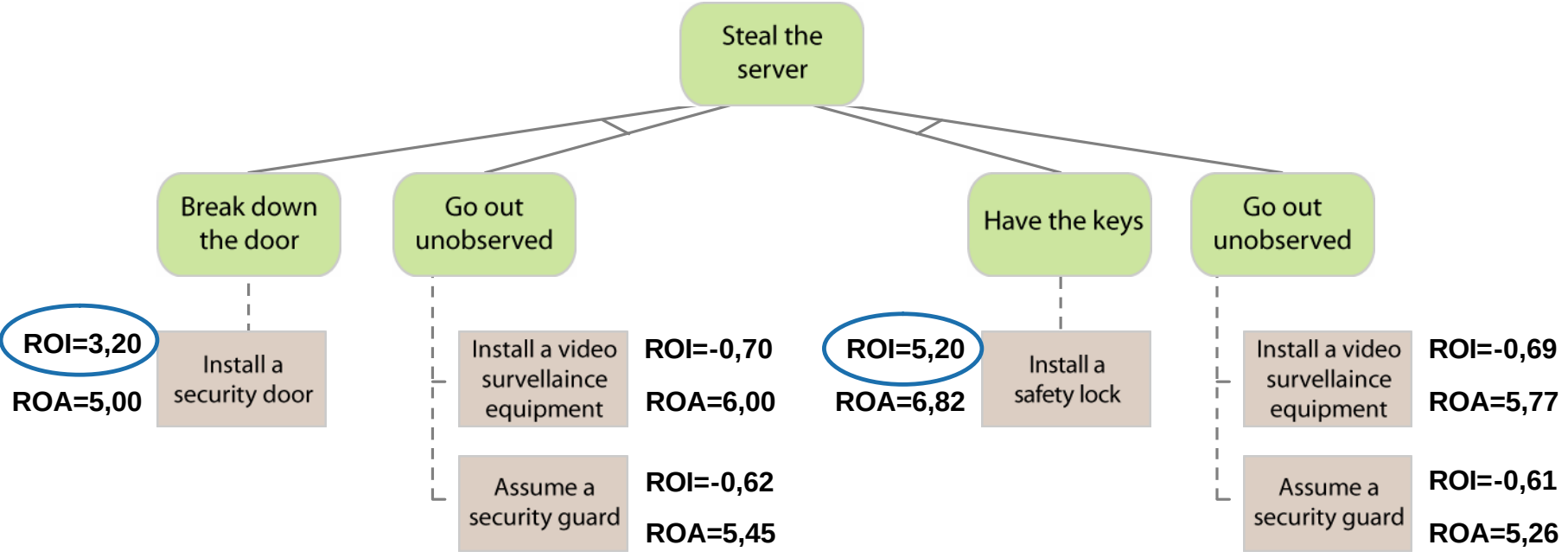
Putting together the evaluations

- Maximize ROI
- minimize ROA
- max ROI min ROA
- a Pareto-optimal solution
- maximize a user-defined function of ROI and ROA



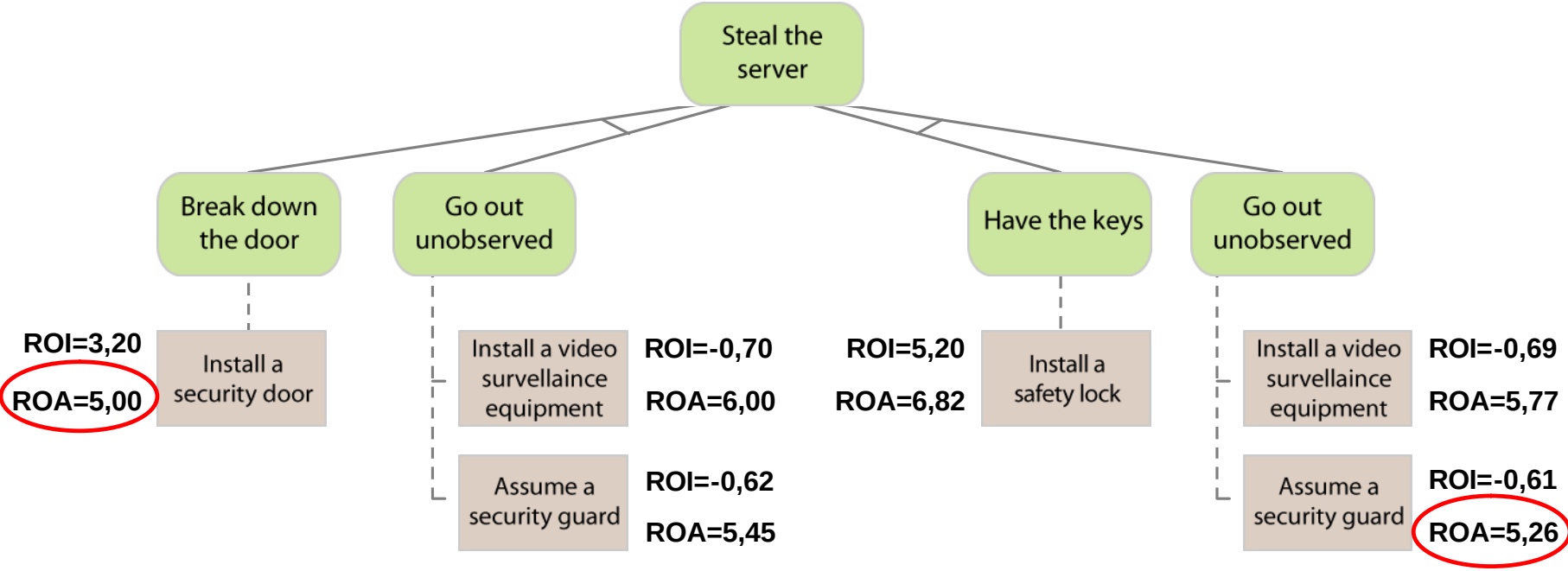
Putting together the evaluations

- Maximize ROI



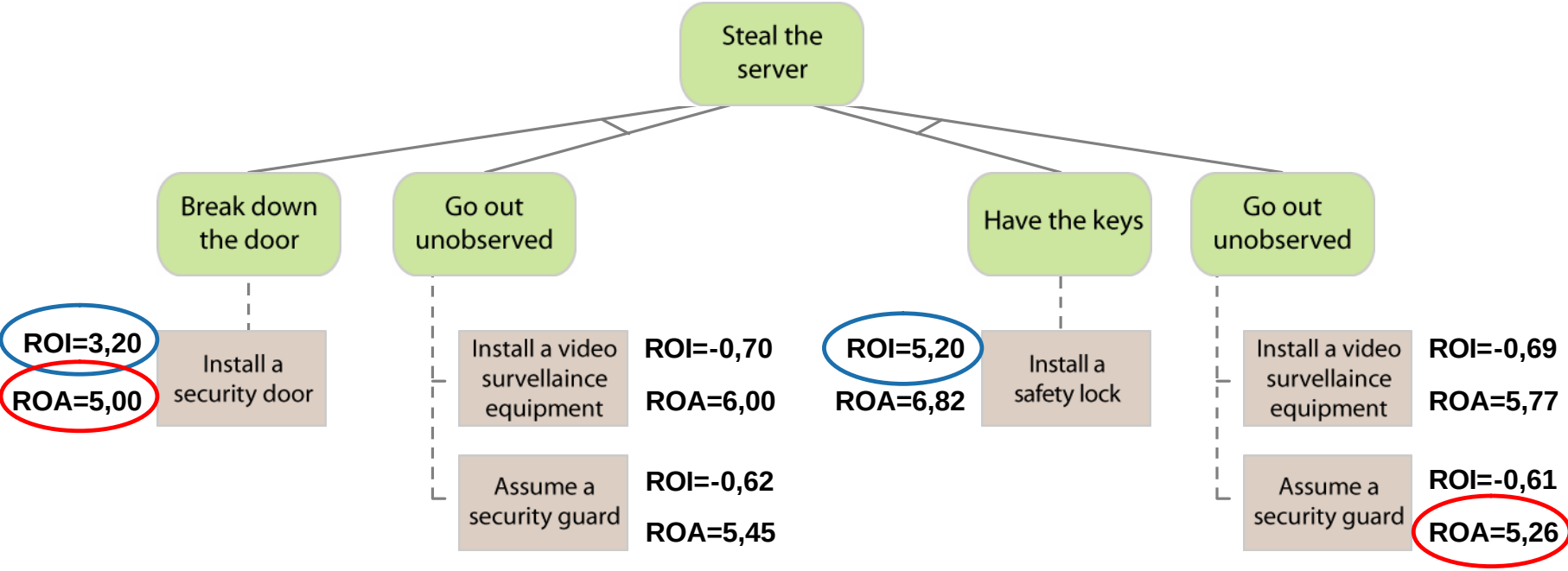
Putting together the evaluations

- Minimize ROA



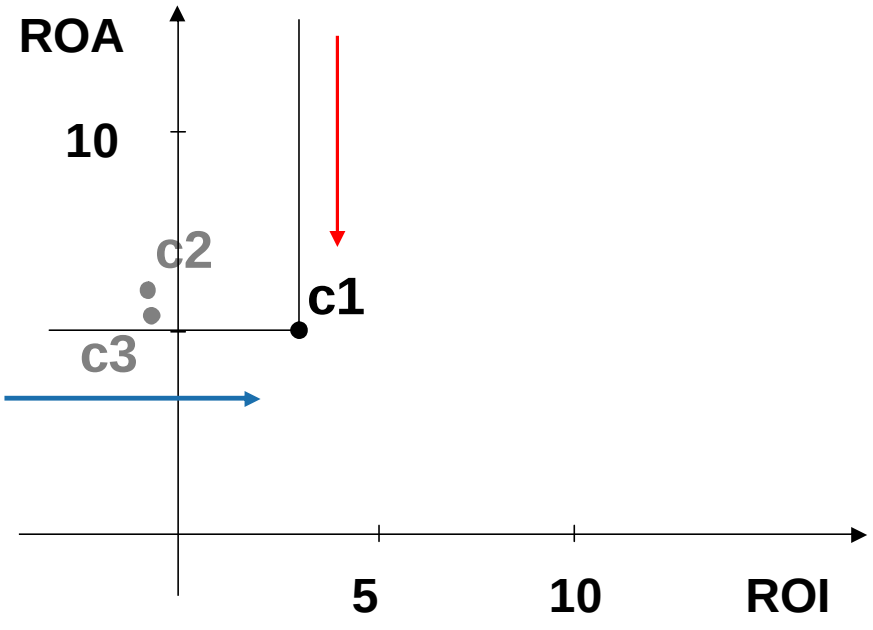
Putting together the evaluations

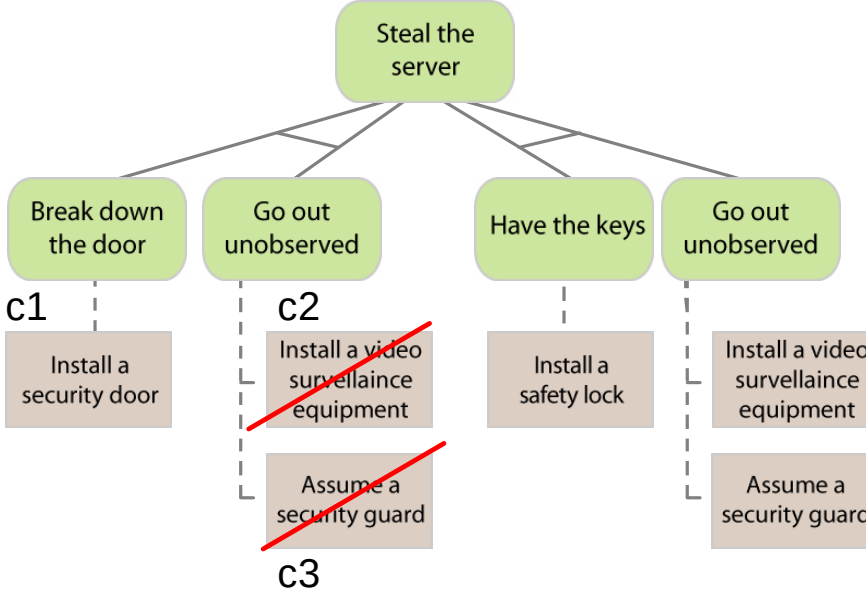
- max ROI min ROA



Putting together the evaluations

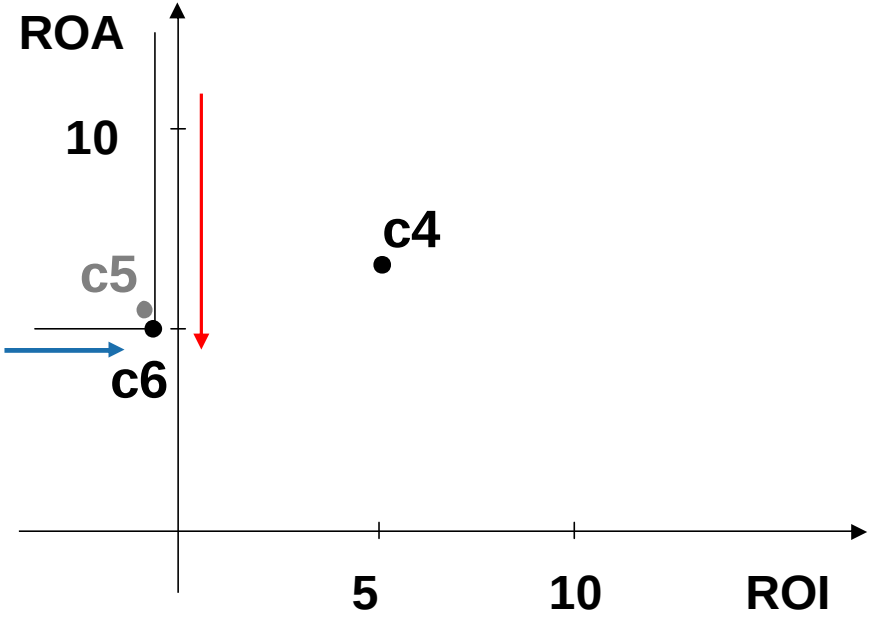
The *Pareto-optimal* countermeasure for the first attack

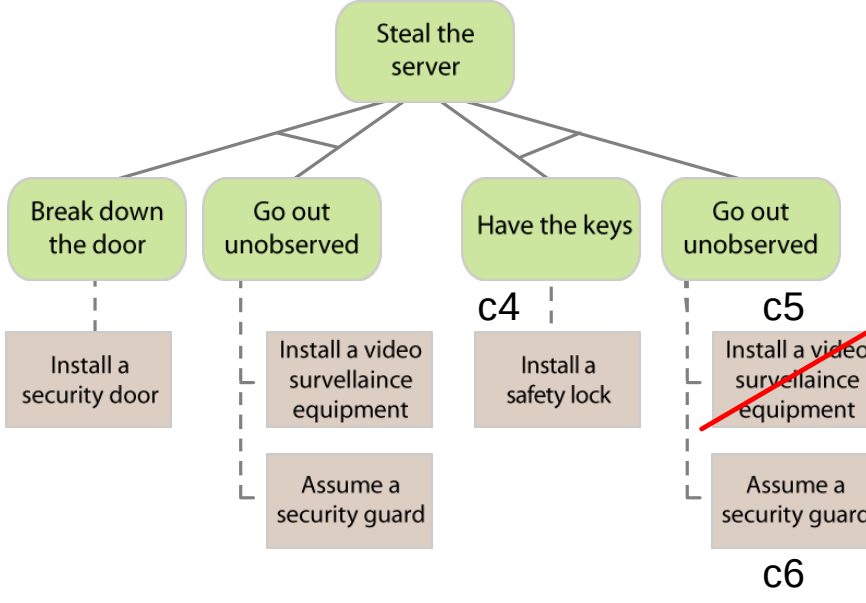




Putting together the evaluations

The Pareto-optimal countermeasure for the second attack

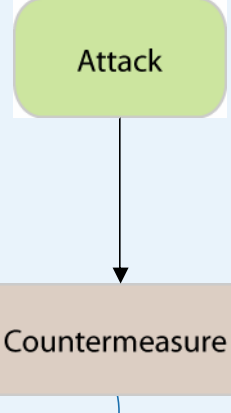




F.W. CP-Nets

- Relations between possibilistic logic and cp-nets
- Uncertainties of attacks modelled as probability/possibility distribution

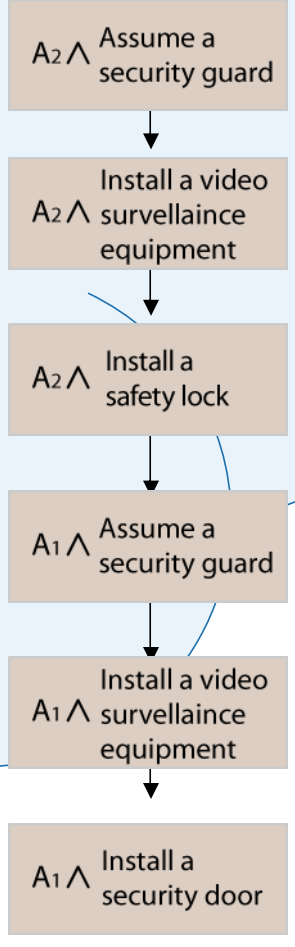
(See: CP-Net, Possibility Theory (Prade, Dubois), Uncertainty and CP-Net (?Brent Phd Thesis?))



$A_1 \succ A_2$

A_1	$c_1 \succ c_2 \succ c_3$
A_2	$c_4 \succ c_2 \succ c_3$

$c_4 \succ c_1 \succ c_2 \succ c_3$



Conclusion and Future Work

- From Attack to Defense trees
- Defense trees + quantitative labels
  - ROI
  - ROA

- Evaluation of multiple attacks and countermeasure
- Heuristics to find the best configuration
  - Minimum (cost) set cover
- Game Theory analysis
- *Defense Graphs*
- Constraint intervals to represent uncertain indexes (RM, ARO, EF)