École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

Selecting Appropriate Counter-Measures in an Intrusion Detection Framework

Frédéric CUPPENS, Sylvain GOMBAULT, Thierry SANS

Outline

- Cooperative intrusion detection
- Response and counter-measure
- Counter-measure taxonomy
- Modeling counter-measures
- Counter-measure selection
- Response mechanism
- Conclusion and future works

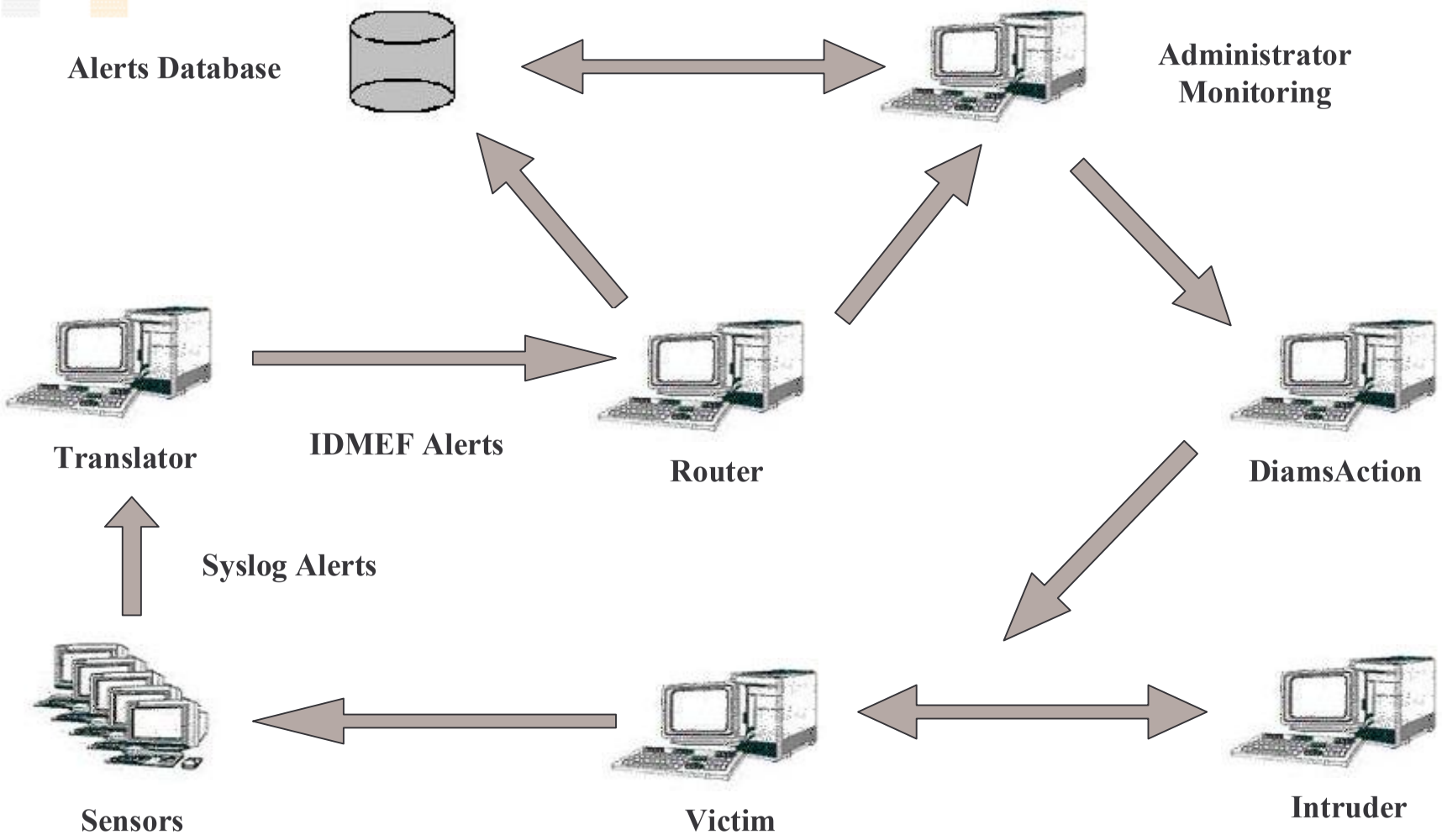
Cooperative intrusion detection

- Several approaches to design IDS (Intrusion Detection System)
  - Signature based (Misuse detection)
  - Behavior based (Anomaly detection)
  - Policy based

- Several types of IDS
  - Host based
  - Network based

- How to improve the global diagnosis ?
  - ➢ Use several IDS in a cooperative framework.

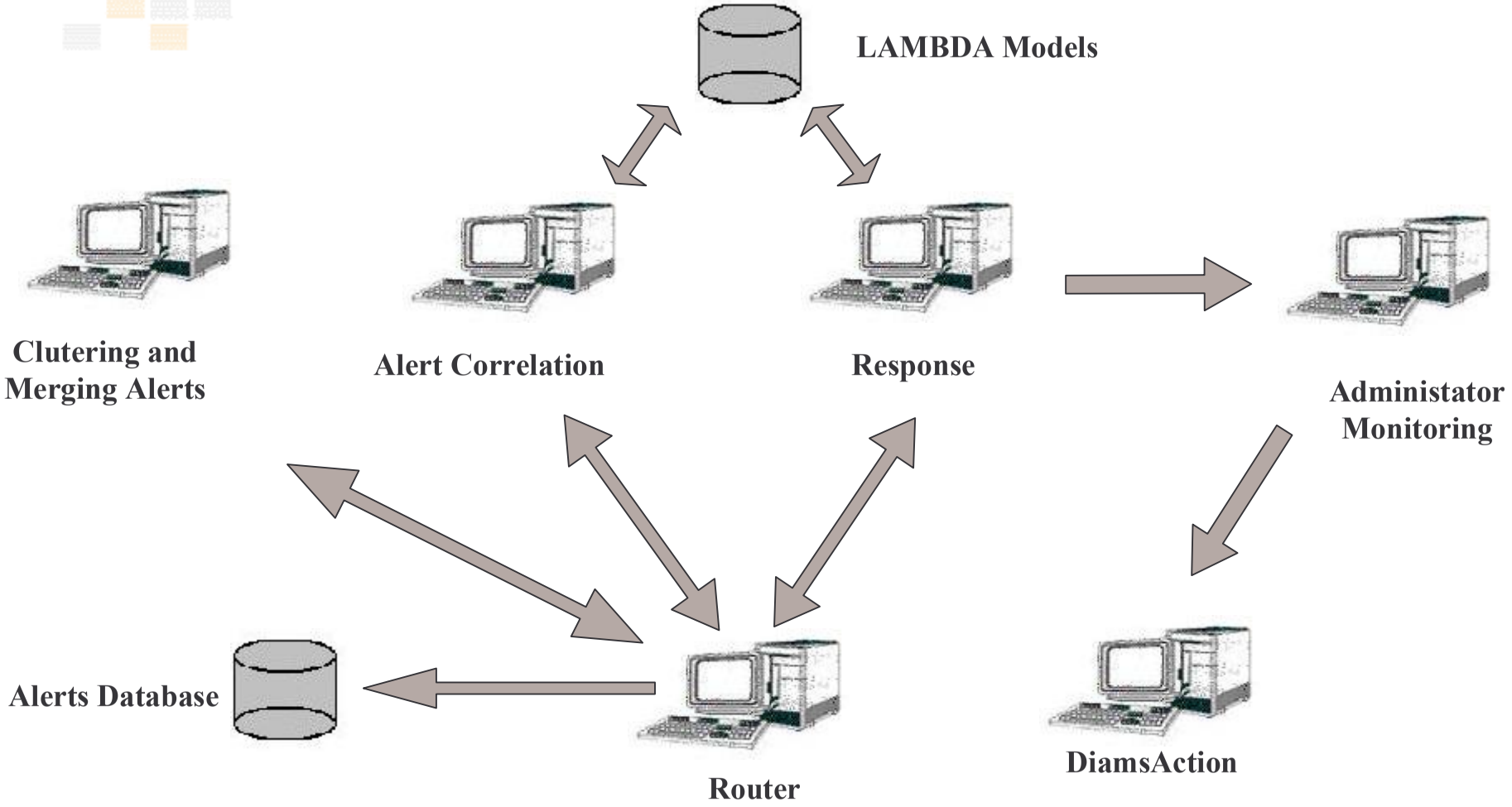
DIAMS : A cooperative intrusion detection framework



Cooperative intrusion detection

- How to reduce the number of alerts ?
  - Clustering and merging alerts
- How to obtain a real diagnosis of the intrusion ?
  - Correlation
- How to select the best counter-measure for a detected intrusion ?
  - Response

CRIM : Correlation and intention recognition module



Response and counter-measure

- Counter-measure: Action performed in order to prevent an intrusion.
  - Design a library of counter-measures

- Response: Mechanism used to select the best counter-measures when an intrusion objective is identified by the correlation process.
  - The security administrator can decide to apply or not counter-measures.

Counter-measure taxonomy

- Information
  - Raise an alert to the security administrator
- Deterrence
  - Action performed against the intruder in order to stop his/her intrusion
- Correction
  - Action to modify system state to correct an identified vulnerability or misuse configuration
- Compensation
  - Action performed to block the attack but without correction

Modeling Counter-measures

- In CRIM, LAMBDA (Language to Model a dataBase for Detection of Attacks) is used to model both attacks and intrusion objectives.
  - Use LAMBDA to model counter-measures

- LAMBDA specification of counter-measure
  - Example : TCP-Reset

***counter-measure close-remote-access*(Source,Target)**	
pre :	remote-access(Source,Target)
action :	TCP-Reset (Source,Target)
post :	not(remote-access(Source,Target))
verification :	not(TCP-connection(Source,Target))

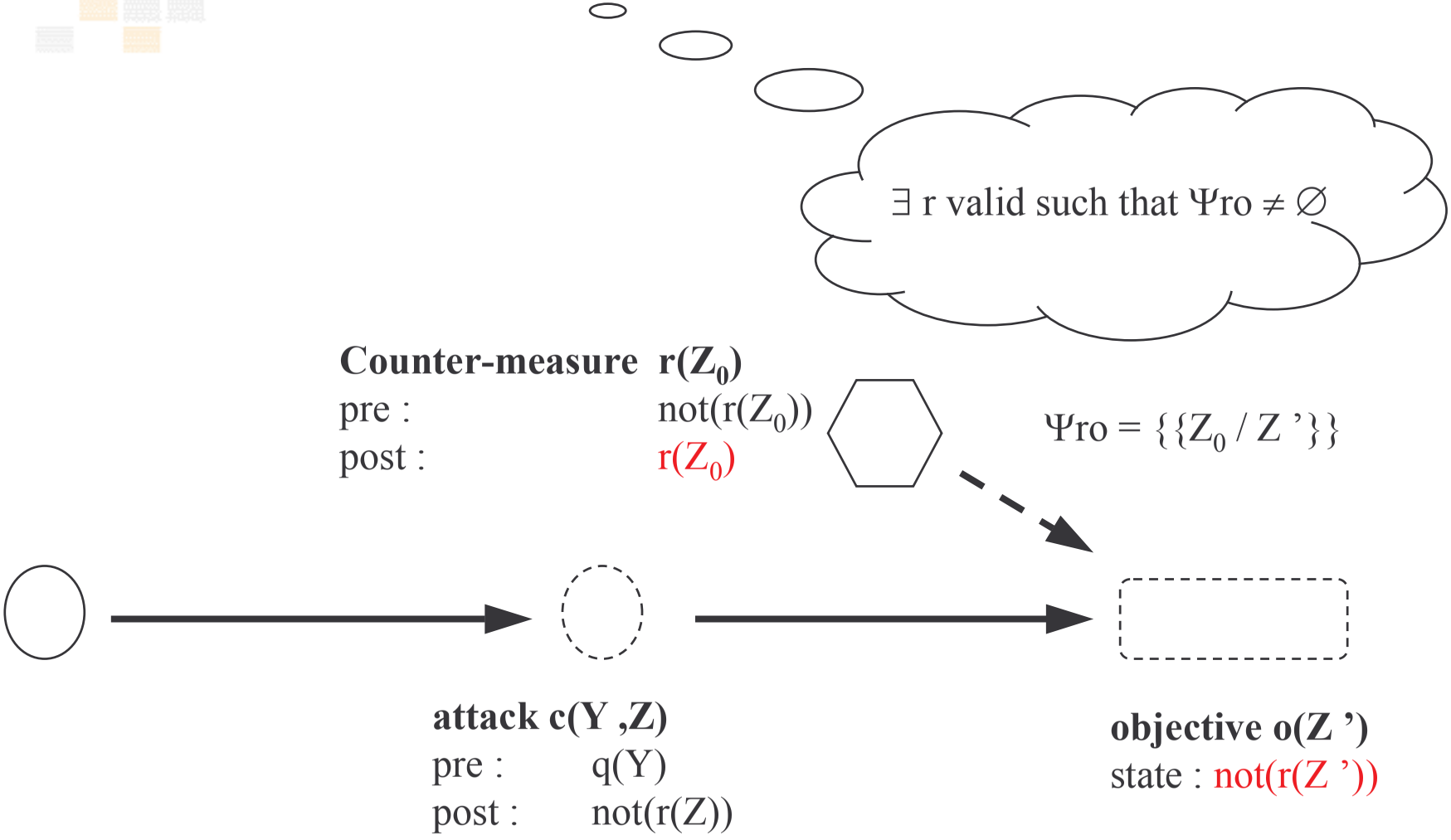
Counter-measure selection

- Response mechanism is used to choose the best counter-measure in the counter-measure library to prevent the intrusion objective or future attacks.
  - Use anti-correlation to select counter-measures

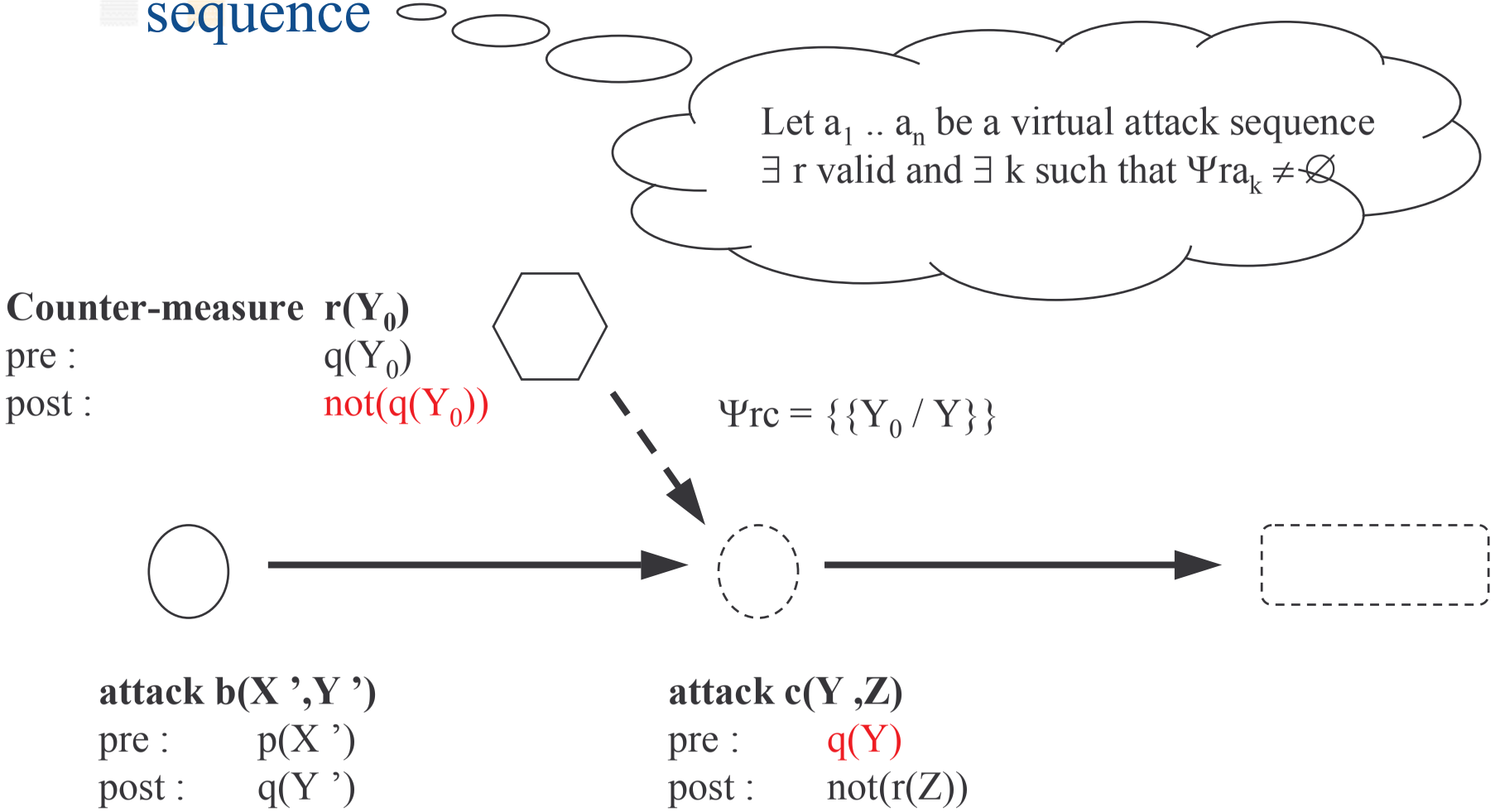
- Anti-correlation: Two actions are anti-correlated when post-condition of the first action disable the pre-condition of the second action

$\exists$ E_a and E_b such that:
$(E_a \in post_a \wedge not(E_b) \in pre_b)$ or $(not(E_a) \in post_a \wedge E_b \in pre_b)$
and E_a and E_b are unified through a most global unifier θ.
Ψ_{ab} is the anti-correlation unifier: set of possible unifiers θ between $post_a$ and pre_b.

Response mechanism applied to intrusion objective



Response Mechanism applied to a virtual attack sequence



Conclusion

- Unique specification language, LAMBDA is used to model both:
  - Attacks
  - Objectives
  - Counter-measures

- Logical model for:
  - Alert correlation
  - Selection of appropriate counter-measures (anti-correlation)

Works in progress

- Improve clustering and merging alerts algorithm
- Improve correlation with weighted correlation
- Model complex scenarios
  - Mitnick attack, DDOS, ...
- Investigate firewall re-configuration as possible counter-measures

Future works

- Tests of performances
- Take care of availability requirements when selecting counter-measures