A multi-objective decision support framework for simulation-based security control selection

Elmar Kiesling, Christine Strauß, Christian Stummer
Andreas Ekelhart, Stefan Fenz, Bernhard Grill

Fourth International Workshop on Organizational Security Aspects (OSA 2012)
held in conjunction with ARES 2012

August 22, 2012

FWF Funded by the Austrian Science Fund (FWF) under project number *P*23122 – *N*23.

Major challenges in security

- Systems are becoming more and more complex
- Today's serious threats are sophisticated, targeted multi-stage attacks that combine multiple attack vectors such as
  - Software vulnerabilities
  - Network vulnerabilities
  - Insider knowledge and access
  - Social engineering techniques
  - etc.
- Human threat sources are difficult to model
- Threat agents are heterogeneous (motivation, skills, resources etc.)

  e.g., hacktivists, script kiddies, insiders, resourceful external attackers etc.?

  $\rightarrow$ "secure against whom?" [?]

Security control selection: Requirements

"Optimal" investment in information security must ...

- consider that security depends on the combined effect of all implemented controls (which is generally not cumulative)
- recognize security as a tradeoff between multiple monetary and non-monetary criteria (e.g., cost vs. security benefits)
- cast the problem in terms that both CISOs and senior managers can relate to

No universal "best" solution:
Highly context-dependent, decisions must consider

1. "system" characteristics (physical and IT infrastructure, people etc.)
2. the threat model (including threat agent characteristics)
3. available resources
4. decision-makers' risk preferences

Framework for modeling and decision support

Objective: choose a set of security controls to implement by . . .

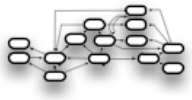
Modeling . . .

1. Abstract causalities in an attack ontology
2. Context (assets, employees etc.) in an "infrastructure" ontology
3. Behavior of threat agents

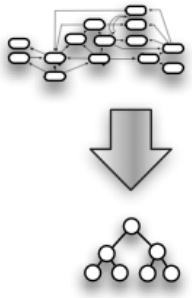
. . . and using these models to

1. Evaluate the overall security by simulating attacks
2. Identify efficient sets of controls through multi-criteria optimization (e.g. cost vs. simulation result security metrics)
3. Provide interactive decision-support to choose among efficient sets

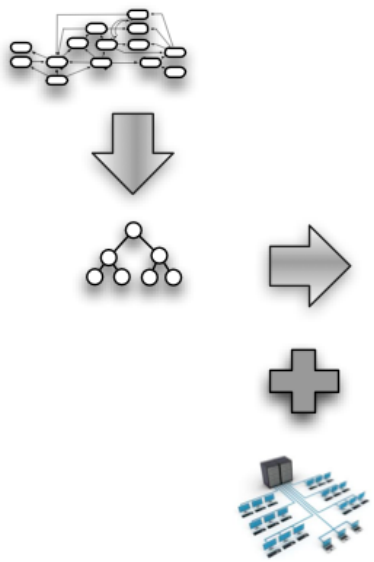
Moses^3 DSS framework - Process overview



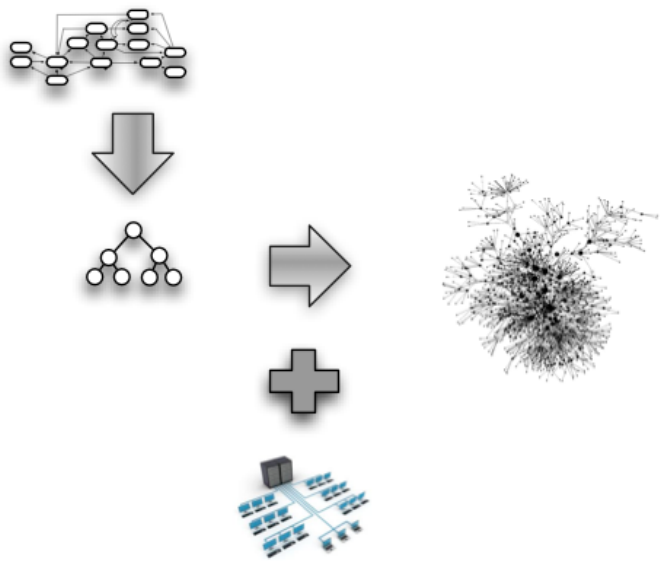
Moses^3 DSS framework - Process overview



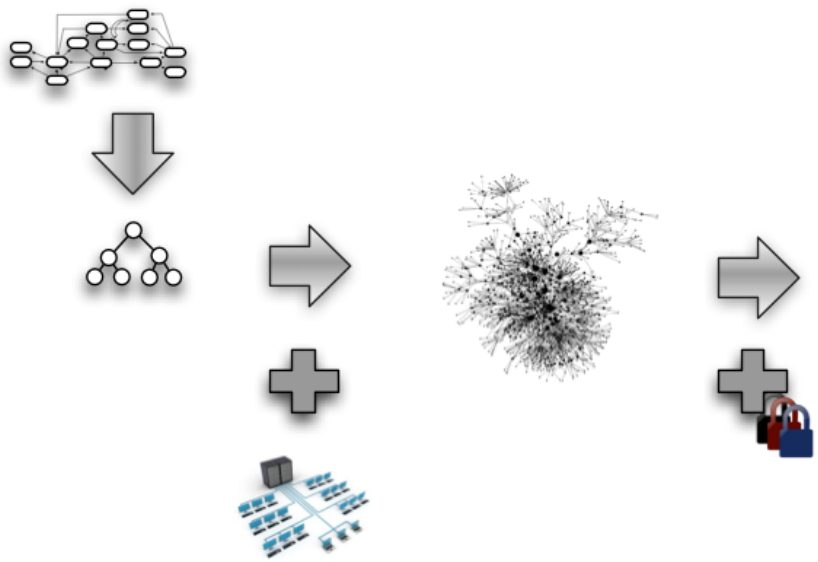
Moses^3 DSS framework - Process overview



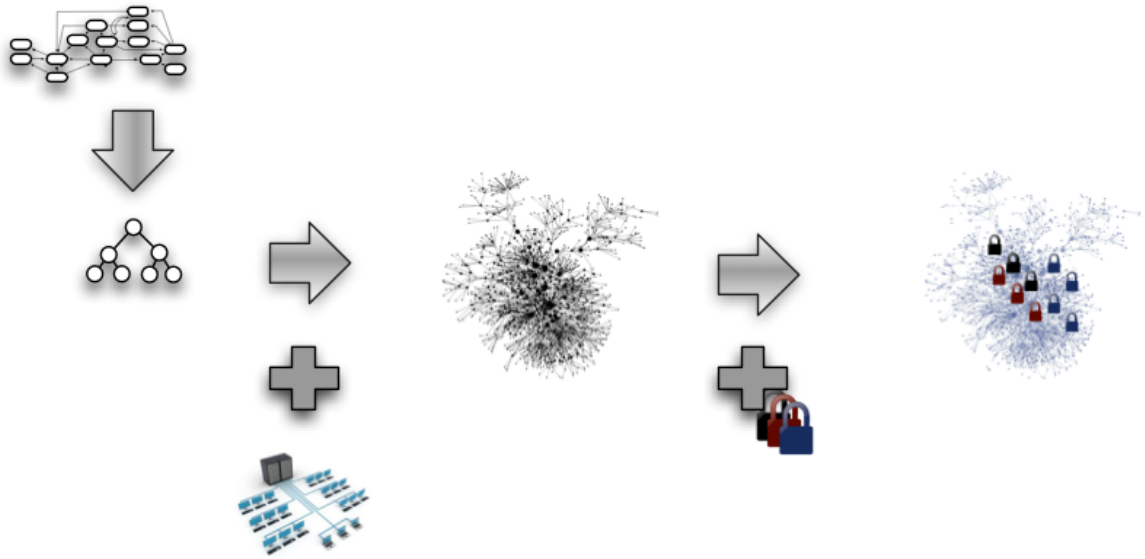
Moses^3 DSS framework - Process overview



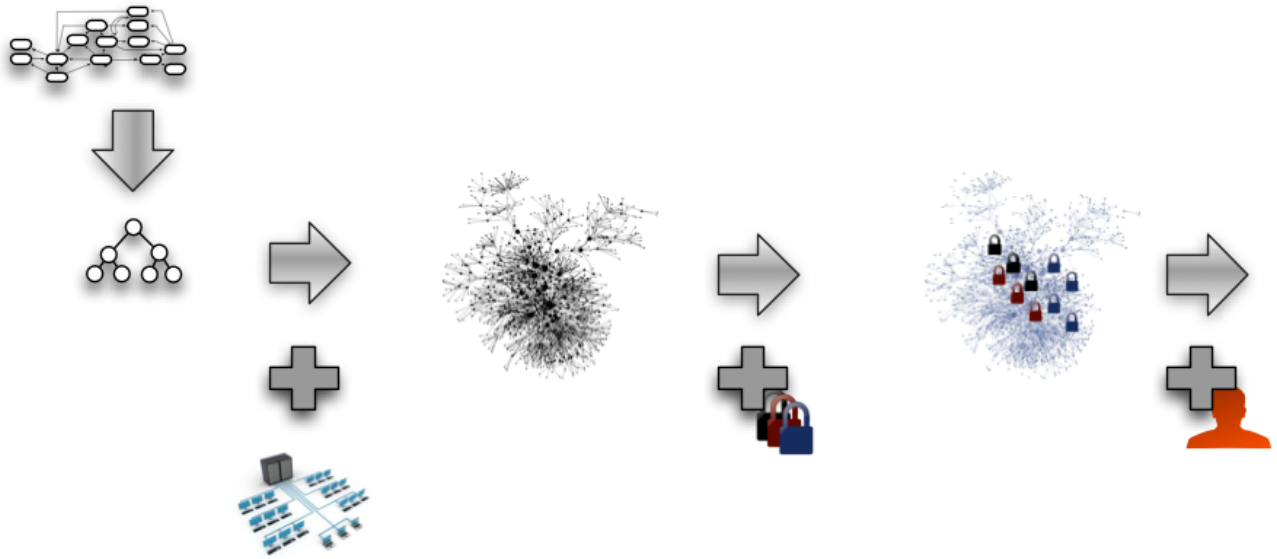
Moses^3 DSS framework - Process overview



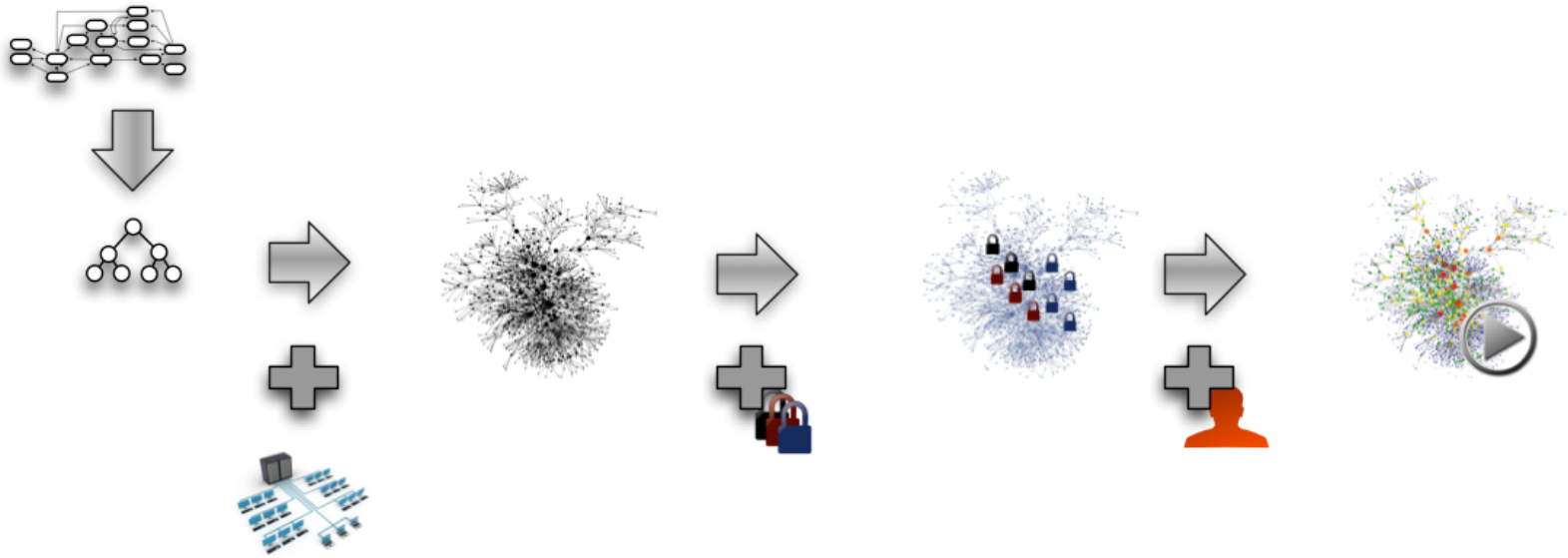
Moses^3 DSS framework - Process overview



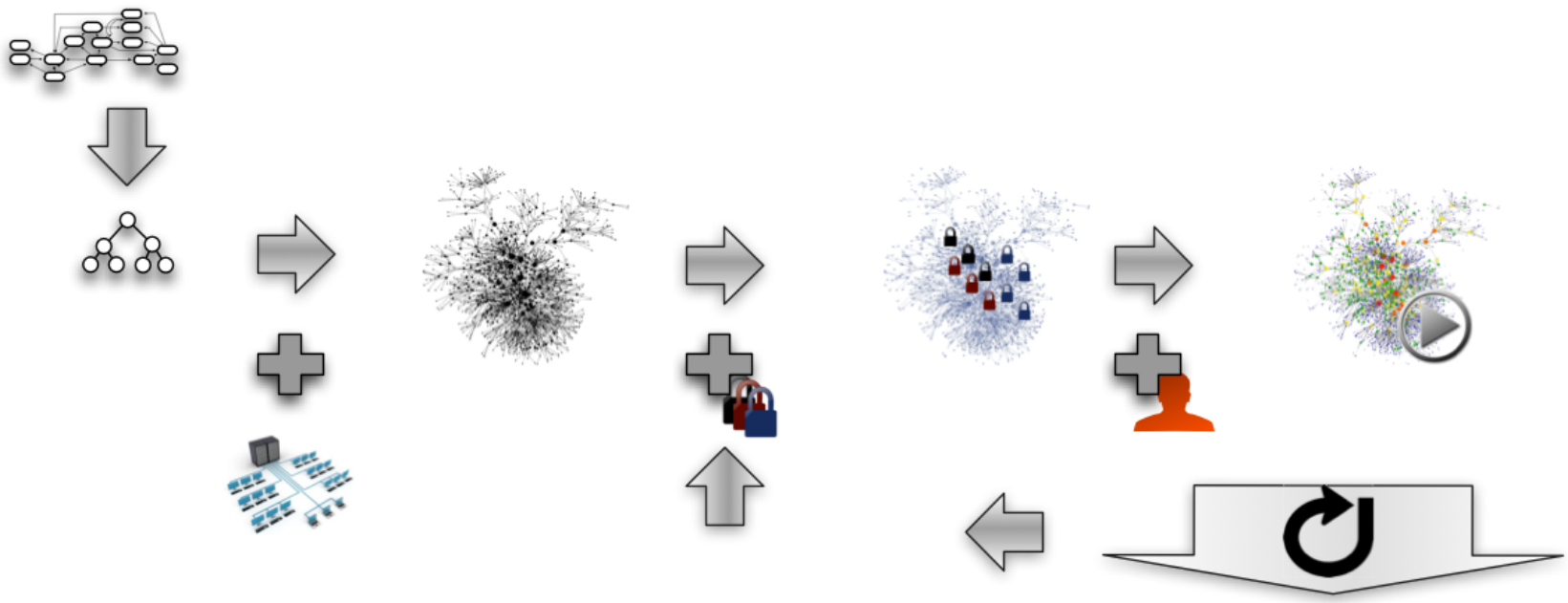
Moses^3 DSS framework - Process overview



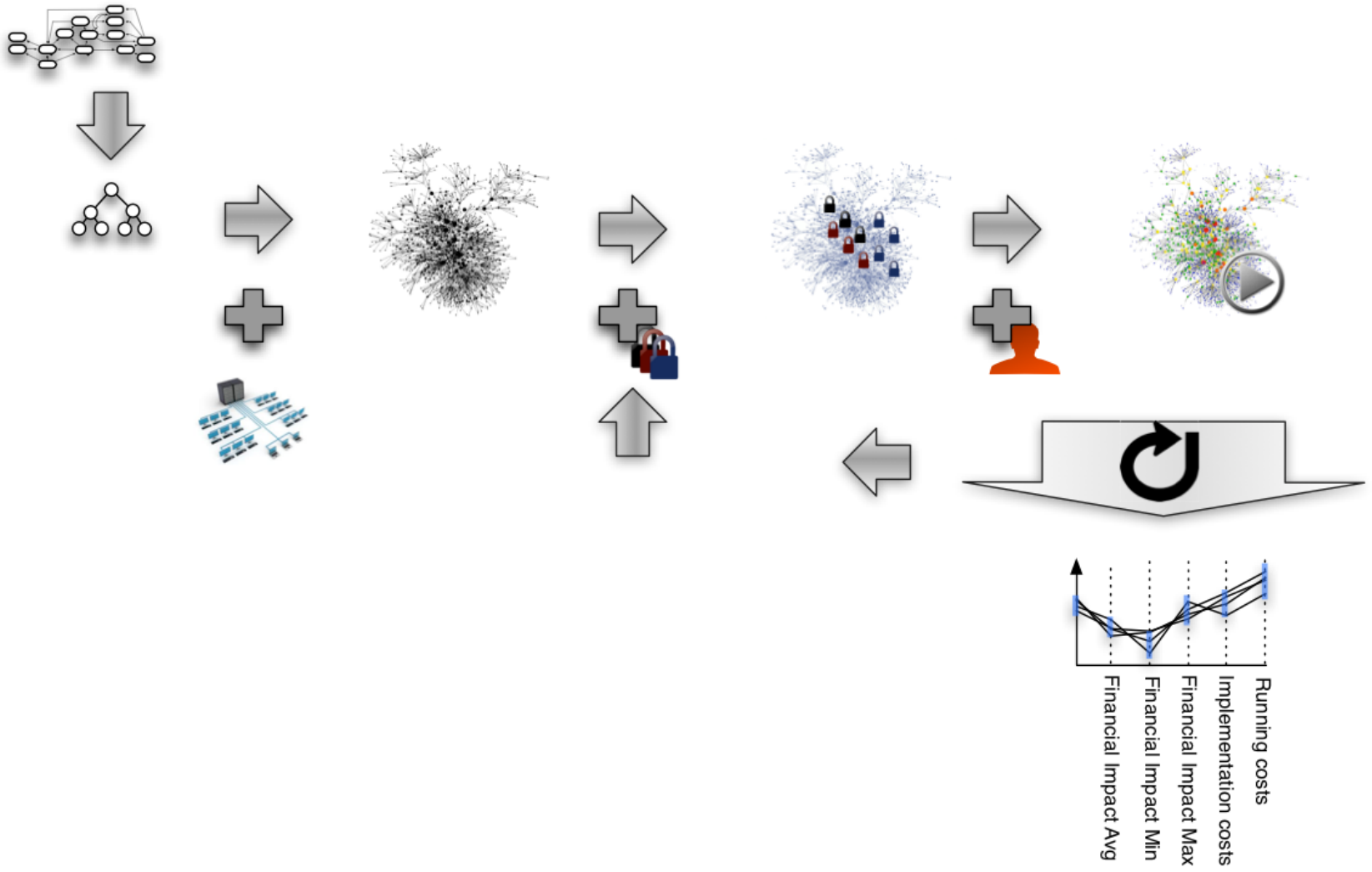
Moses^3 DSS framework - Process overview



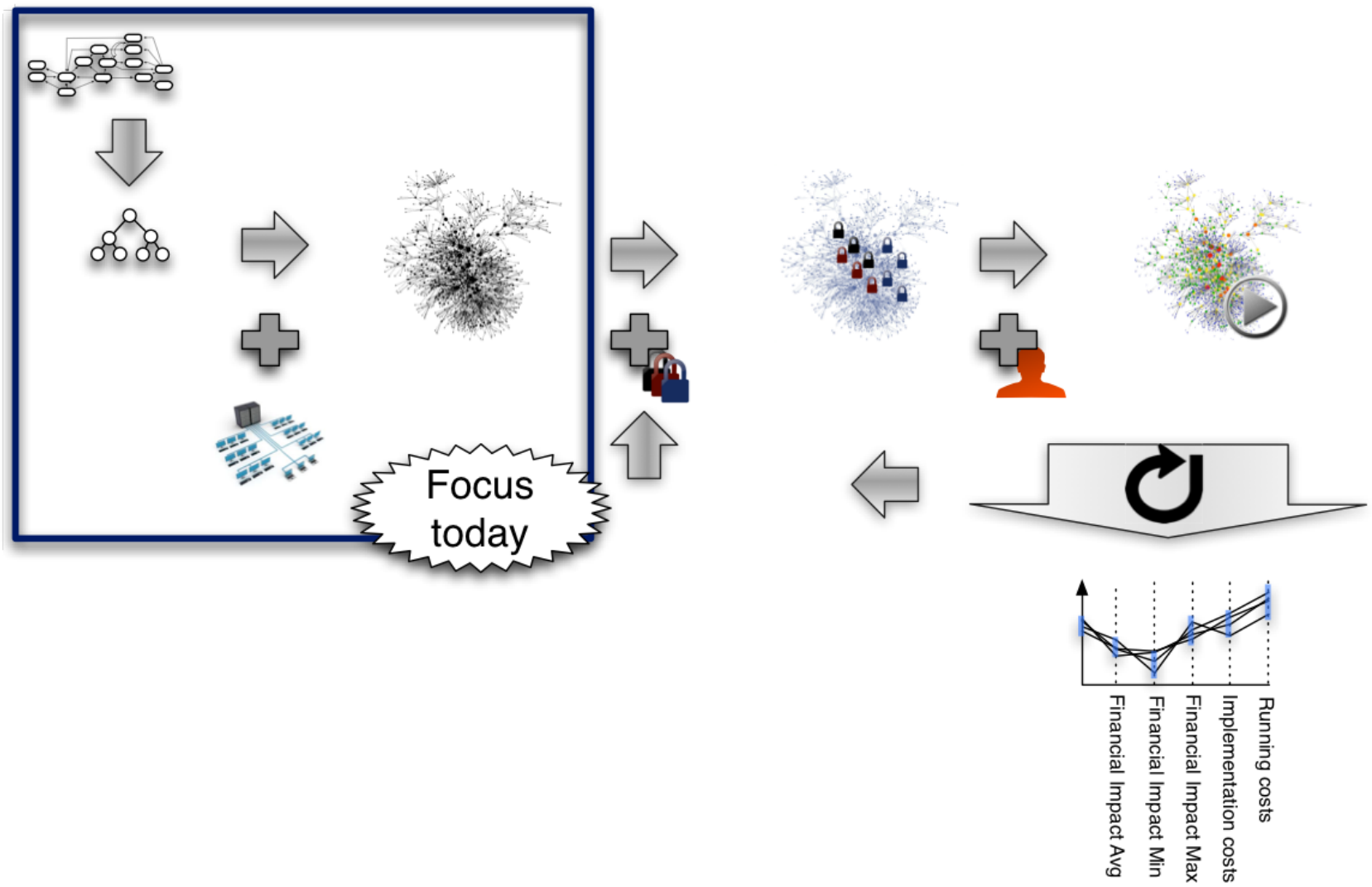
Moses^3 DSS framework - Process overview



Moses^3 DSS framework - Process overview



Moses^3 DSS framework - Process overview



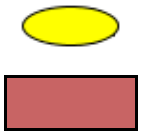
Attack model

Attack ontology

- Abstract causalalities defined independently from concrete infrastructure
- New attack patterns emerge when new actions are added
- Ontology helps to maintain terminological consistency
- Reasoner can be used to infer abstract and concrete attack paths
- May be reused (by multiple organizations)

Attack graphs

- Abstract possible routes of attack for a given target condition
- Constructed by querying the attack ontology
- Depth-first search starting from the target condition

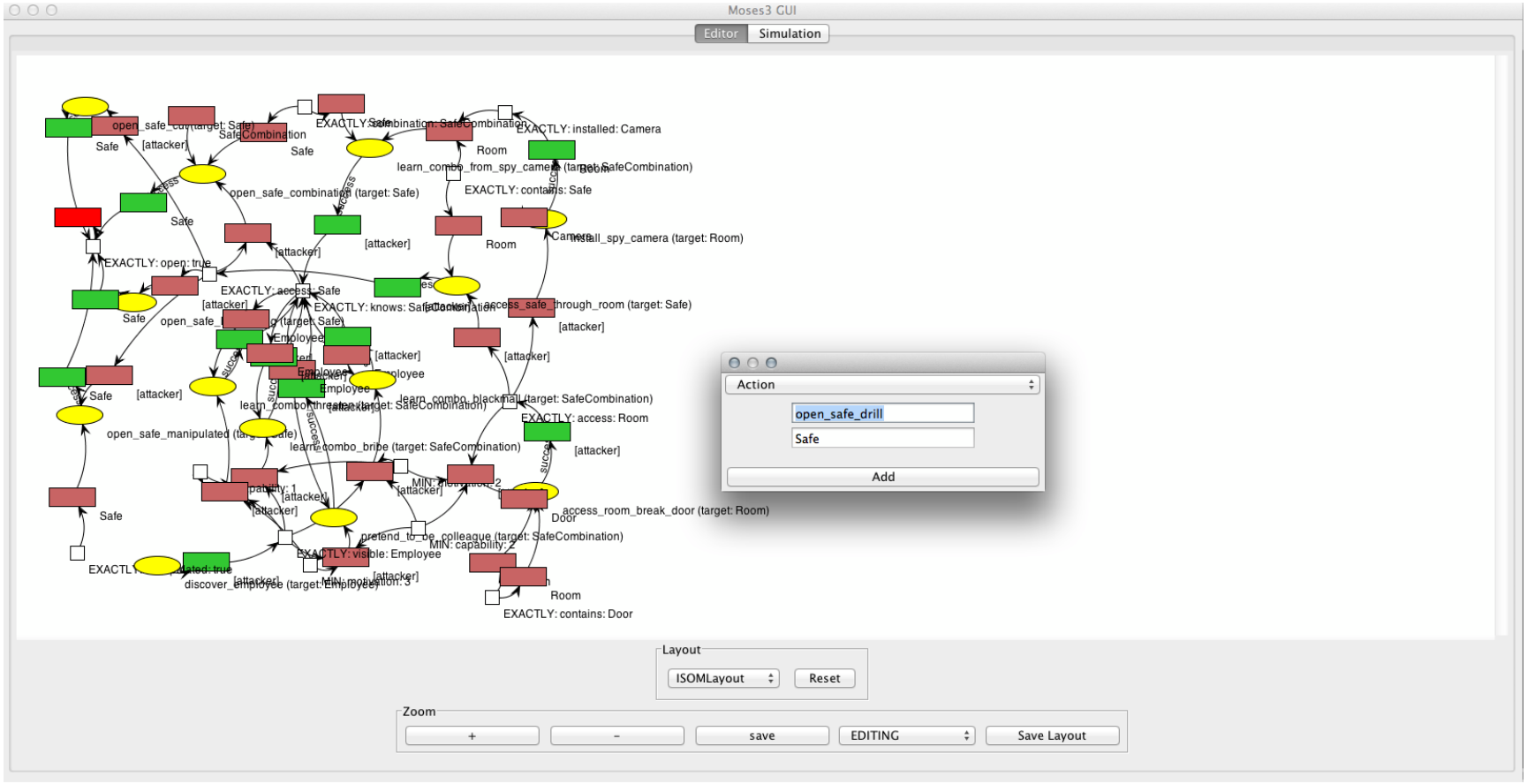

Atomic attack actions

Pre-Conditions

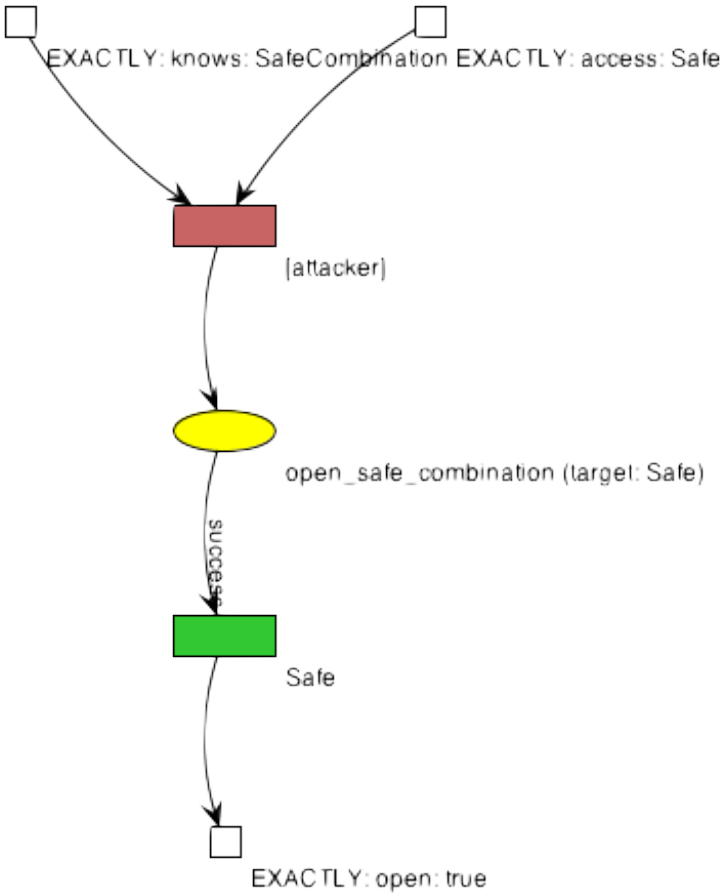

Condition properties


Post-Conditions

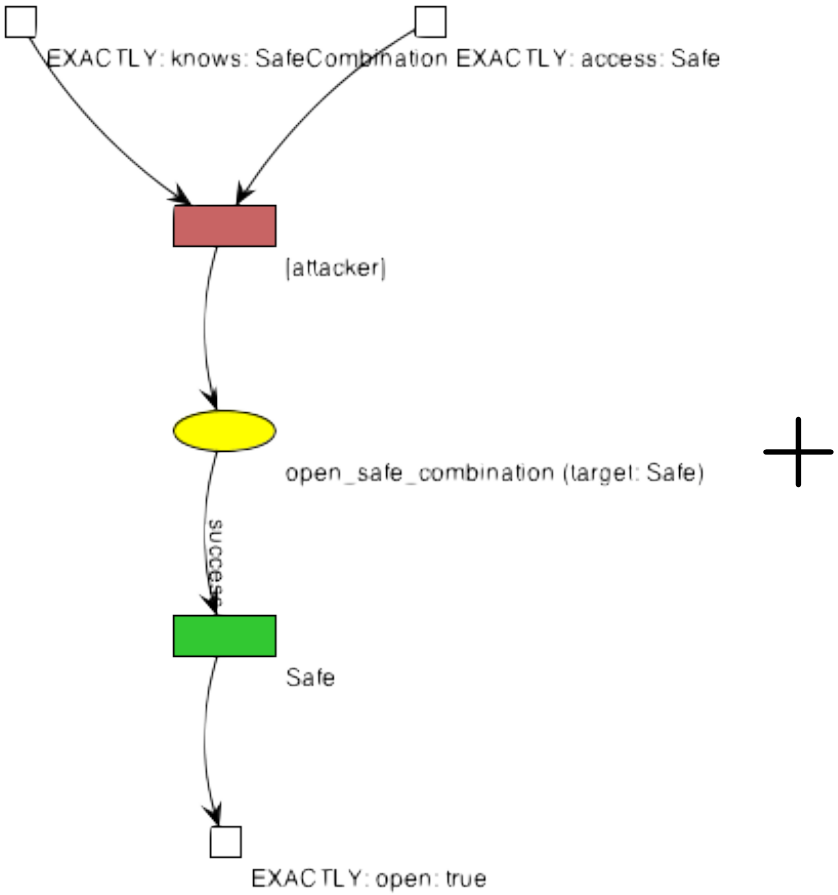
Attack model editor



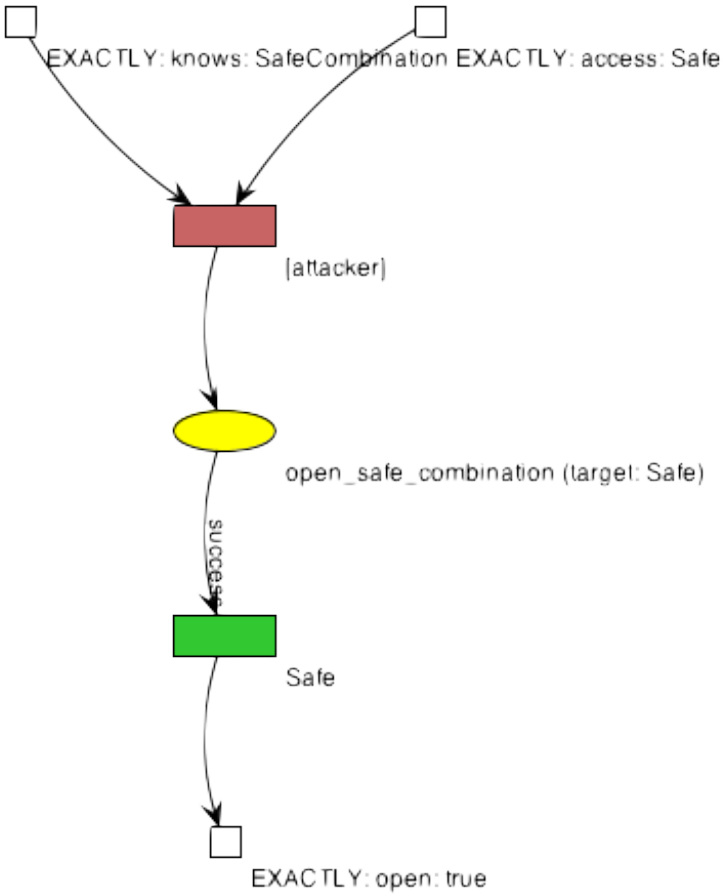
Generic graph elements: Example

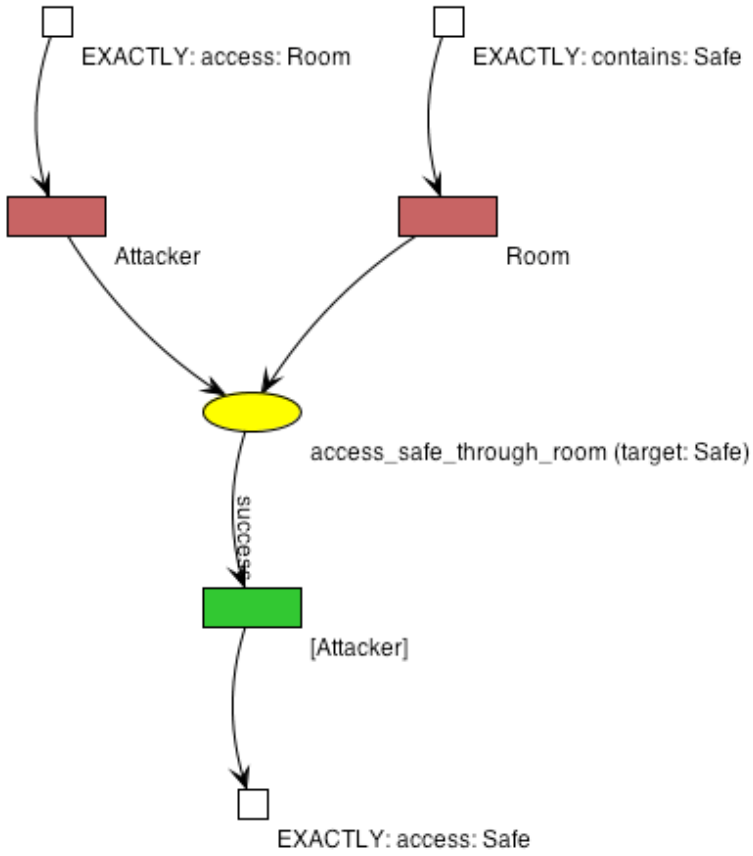


Generic graph elements: Example

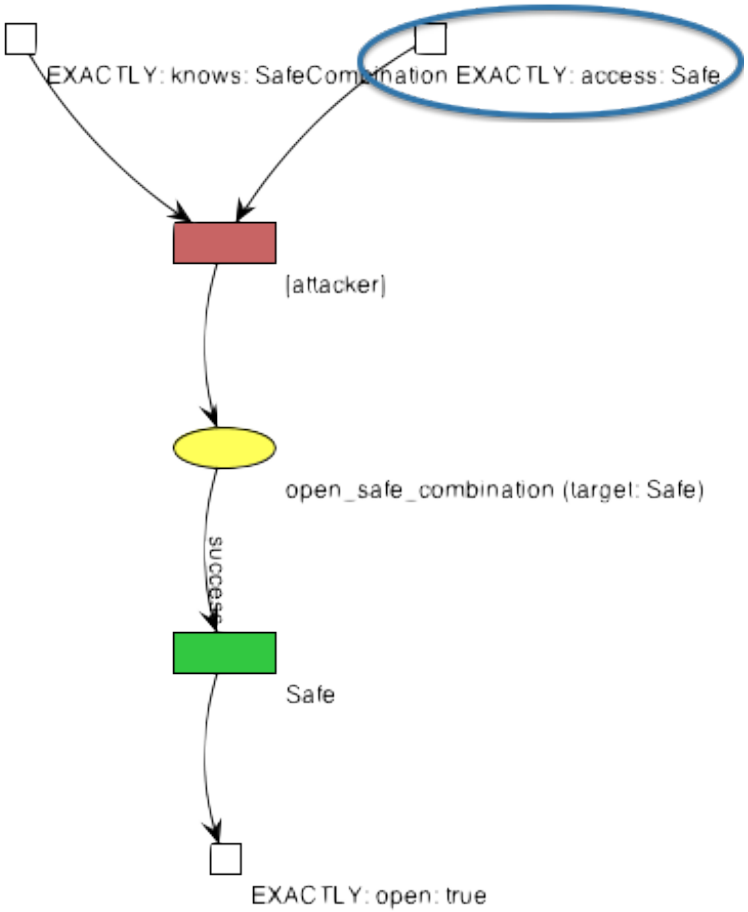


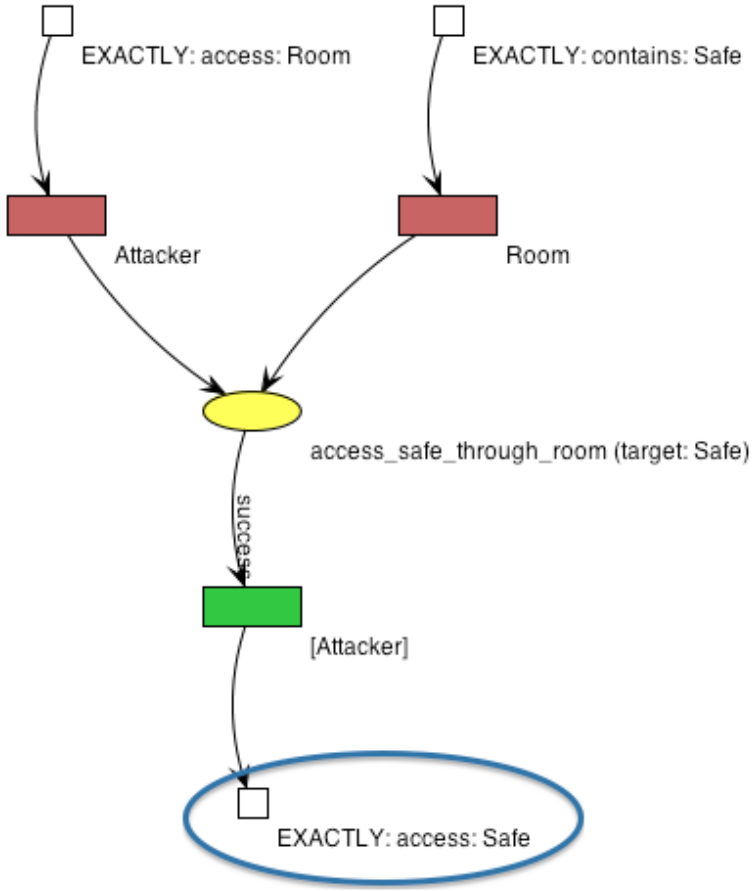
Generic graph elements: Example



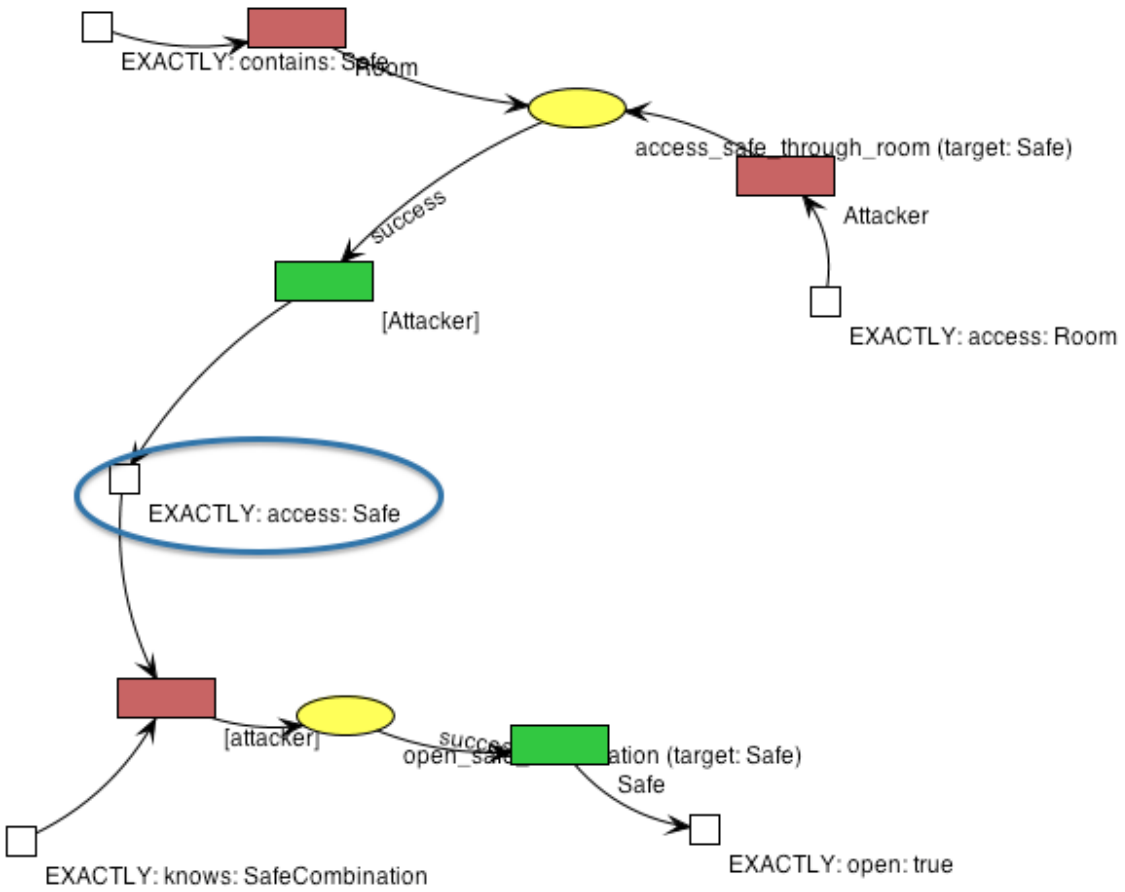


Generic graph elements: Example





Generic graph elements: Example



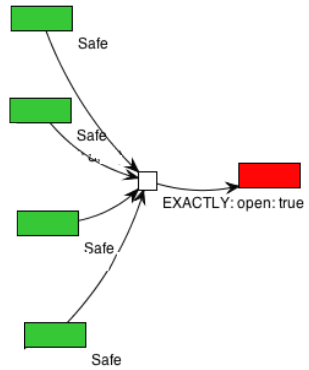
Generic attack graphs: Safe Example

```
Target condition requires property condition open:true on Safe
 '-  Target condition open:true is enabled by action_open_safe_combination
   | action_open_safe_combination has preconditions on [attacker]
   '- [attacker] precondition requires knows:SafeCombination

   '- action_learn_combo_blackmail fulfills knows:SafeCombination
    | action_learn_combo_blackmail has preconditions on [attacker]
    '- [attacker] precondition requires MIN: capability: 2
    '- [attacker] precondition requires MIN: motivation: 2
    '- [attacker] precondition requires visible: Employee
    '- action_discover_employee fulfills visible: Employee
    | action_learn_combo_blackmail has preconditions on Employee
    '- Employee precondition requires knows: SafeCombination

   '- action_learn_combo_bribe fulfills knows: SafeCombination
    | action_learn_combo_bribe has preconditions on [attacker]
    '- [attacker] precondition requires MIN: capability: 1
    '- [attacker] precondition requires MIN: motivation: 2
    '- [attacker] precondition requires visible: Employee
    '- action_discover_employee fulfills visible: Employee
    | action_learn_combo_bribe has preconditions on Employee
    '- Employee precondition requires knows: SafeCombination
     ...
```

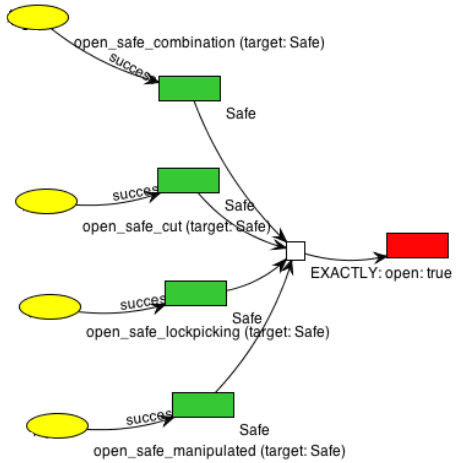
Listing: Attack action backward chaining example

secure sba-research.org

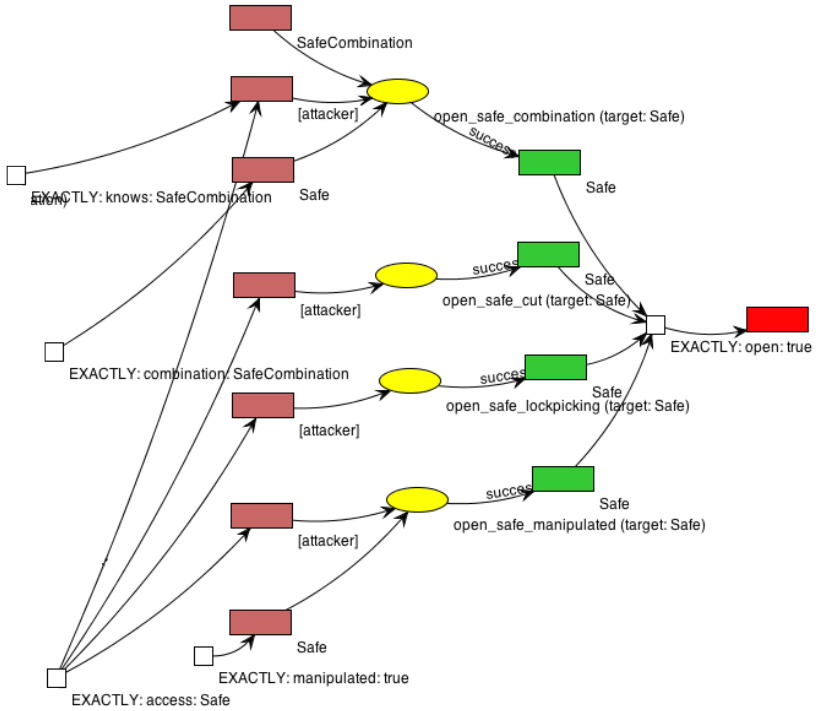
Generic attack graphs: Safe Example



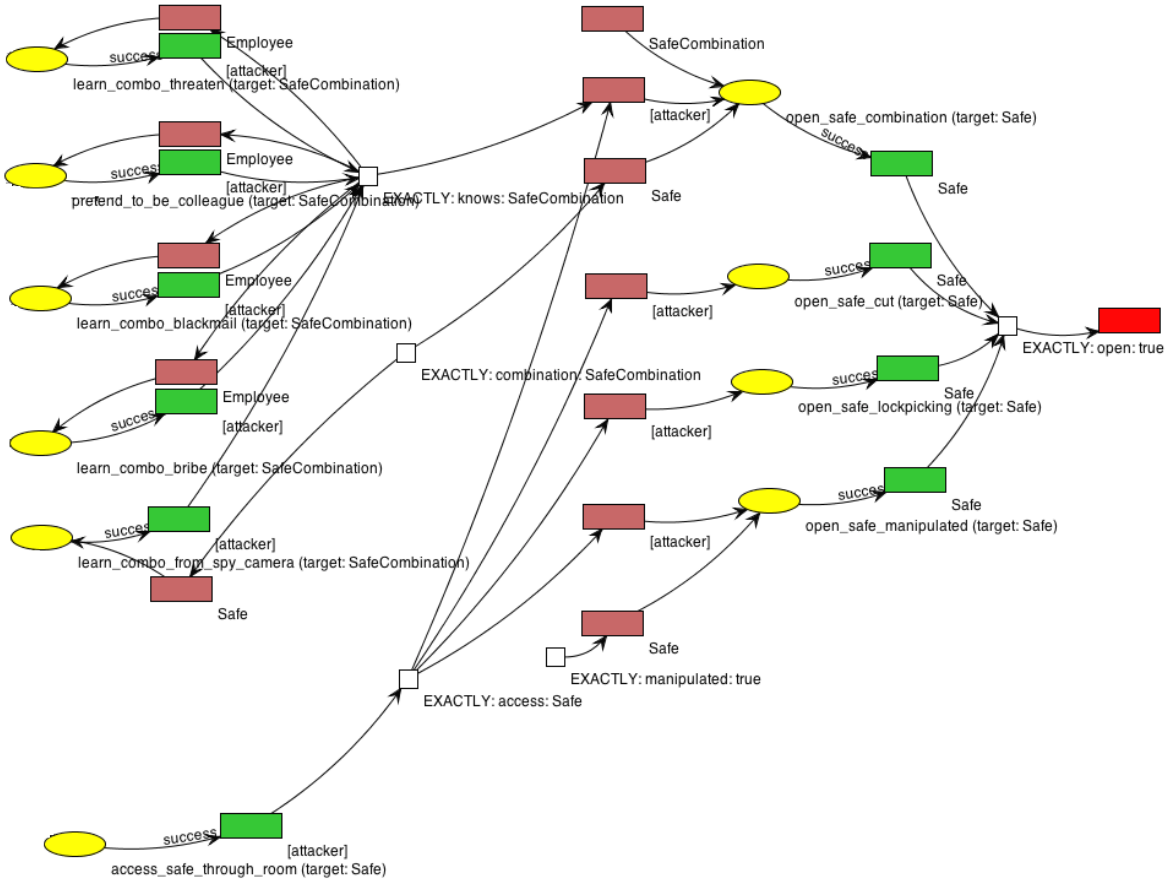
Generic attack graphs: Safe Example



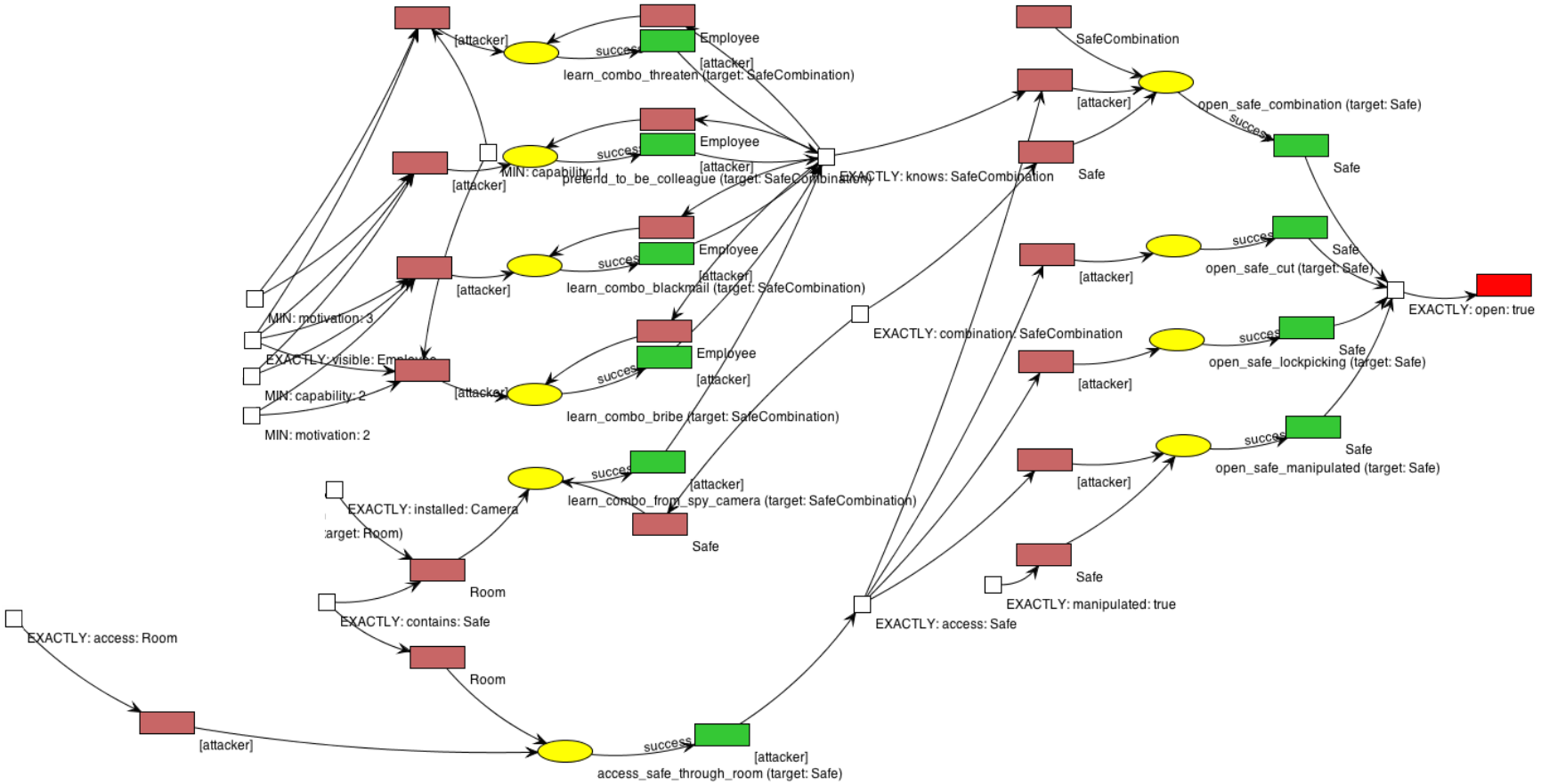
Generic attack graphs: Safe Example



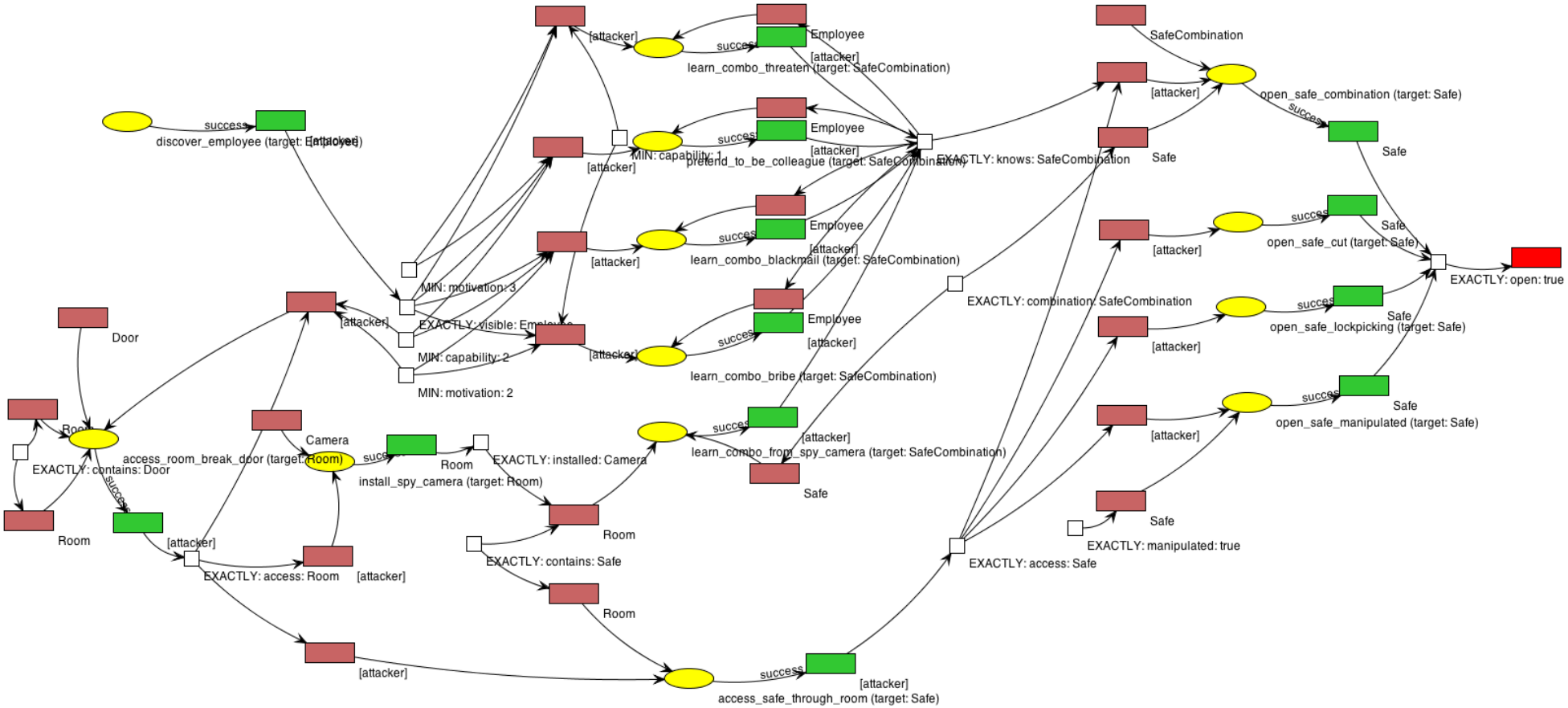
Generic attack graphs: Safe Example



Generic attack graphs: Safe Example



Generic attack graphs: Safe Example



Infrastructure model and attack mapping

Infrastructure model

- Specified in a seperate ontology
- Defines assets (physical entities, employees, information etc.)
- Establishes the context for attacks
- Protégé or through dedicated Editor

Attack mapping

- Query ontology with a particular target condition and a particular attacker profile
- Match abstract attack actions with concrete infrastructure entities to infer possible routes of attack

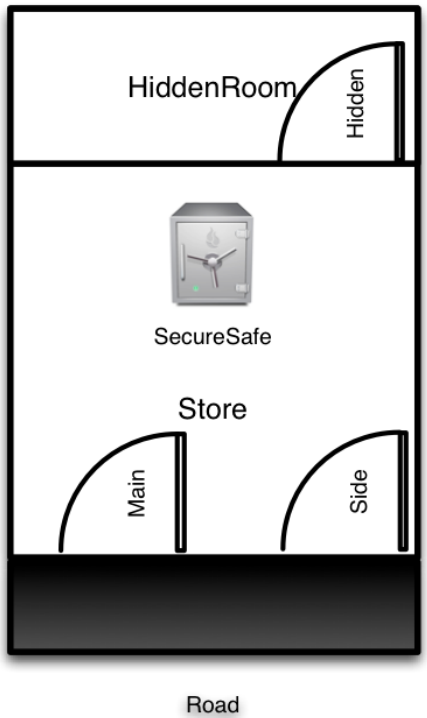
```
Prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
Prefix : <http://moses3.infrastructure.owl#>
Prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>
 SELECT  ?target ?precondition_safecombination_opensafecombination WHERE { ?target rdf:type :Safe .
 :Attacker1 :knows ?precondition_safecombination_opensafecombination .
 :Attacker1 :access ?target .
 ?precondition_safecombination_opensafecombination rdf:type :SafeCombination .
 ?target :combination ?precondition_safecombination_opensafecombination . }
```

Listing: Example attack mapping query

Concrete attack model: Safe Example Scenario

Concepts and Individuals in infrastructure ontology:

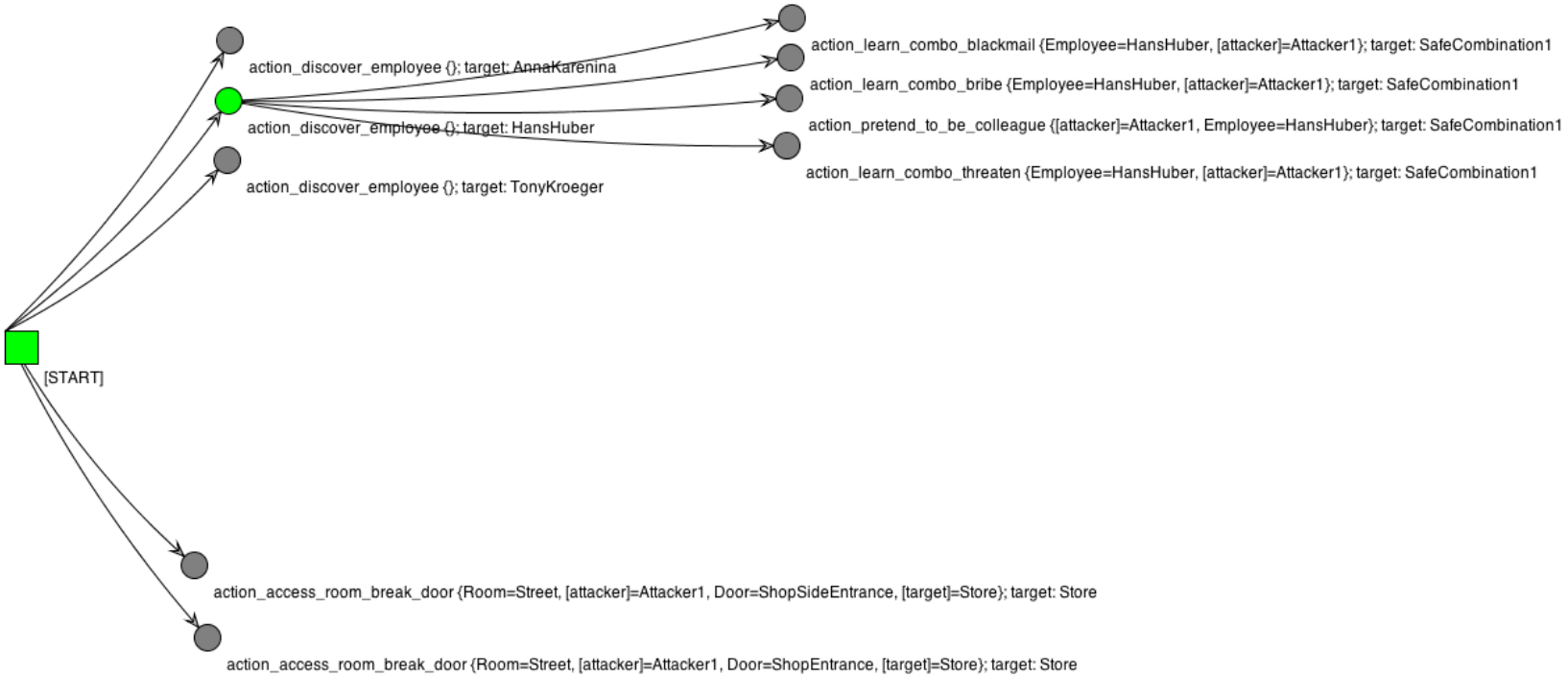
1. Employees:
   - *AnnaKarenia*
   - *HansHuber*
   - *TonyKroeger*
2. Rooms:
   - *HiddenRoom*
   - *Store*
   - *Street*
3. Doors:
   - *ShopEntrance*
   - *ShopHiddenDoor*
   - *ShopSideEntrance*
4. Safe: *SecureSafe*
5. SafeCombination: *SafeCombination*1



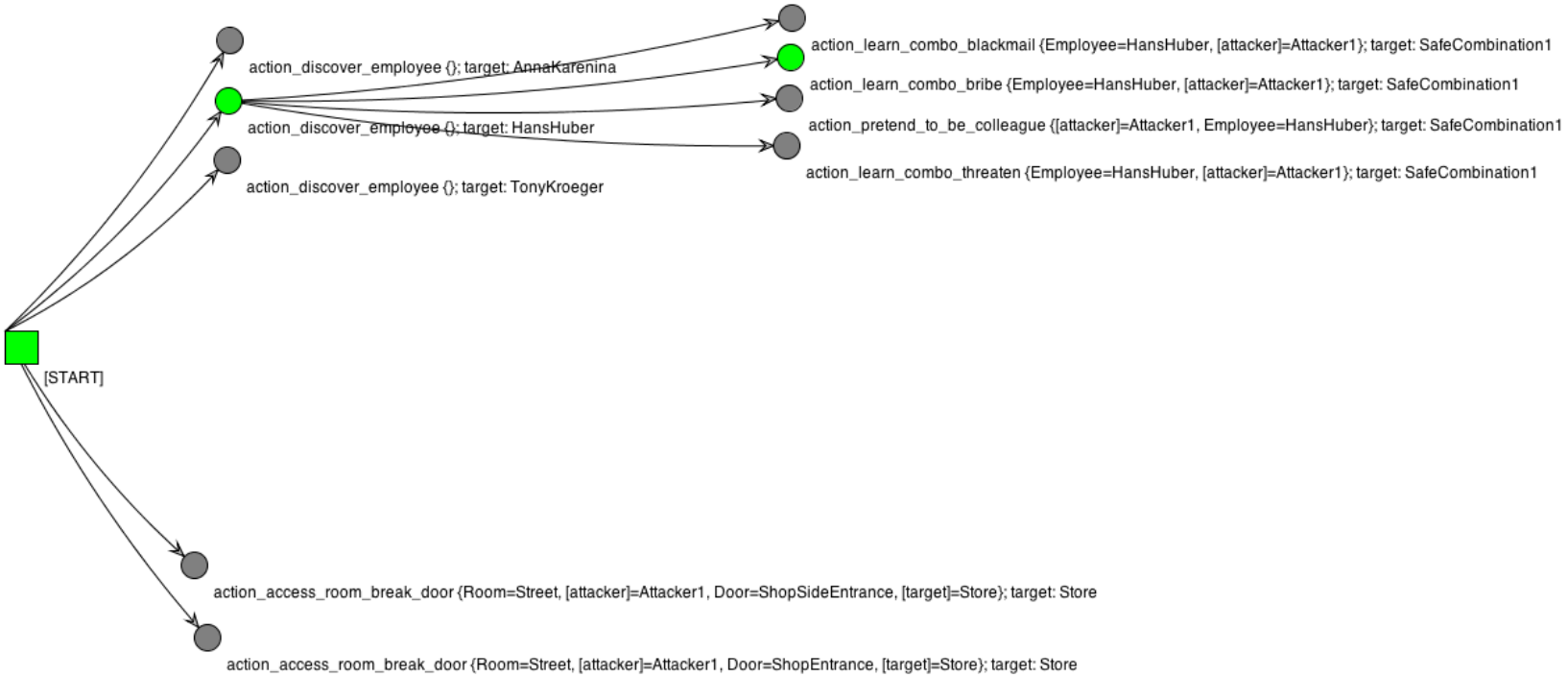
secure
sba-research.org

Concrete attack graphs - Safe Example

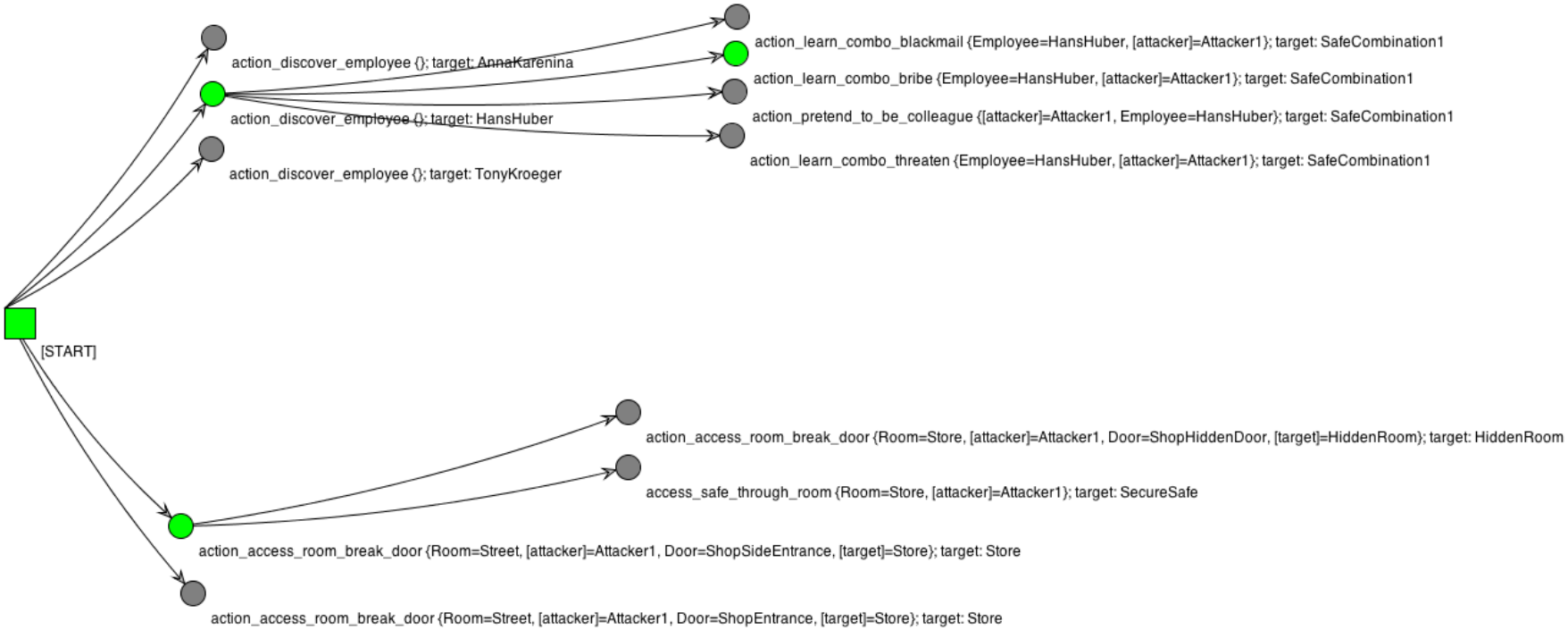
Concrete attack graphs - Safe Example



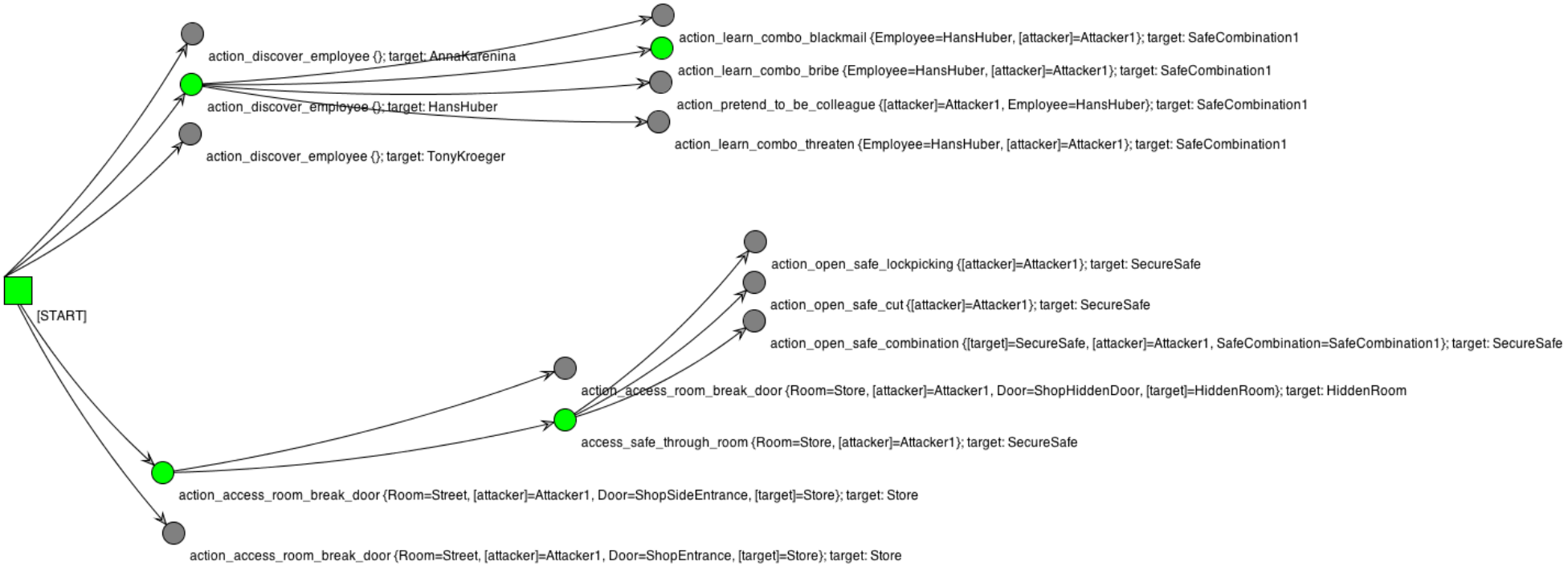
Concrete attack graphs - Safe Example



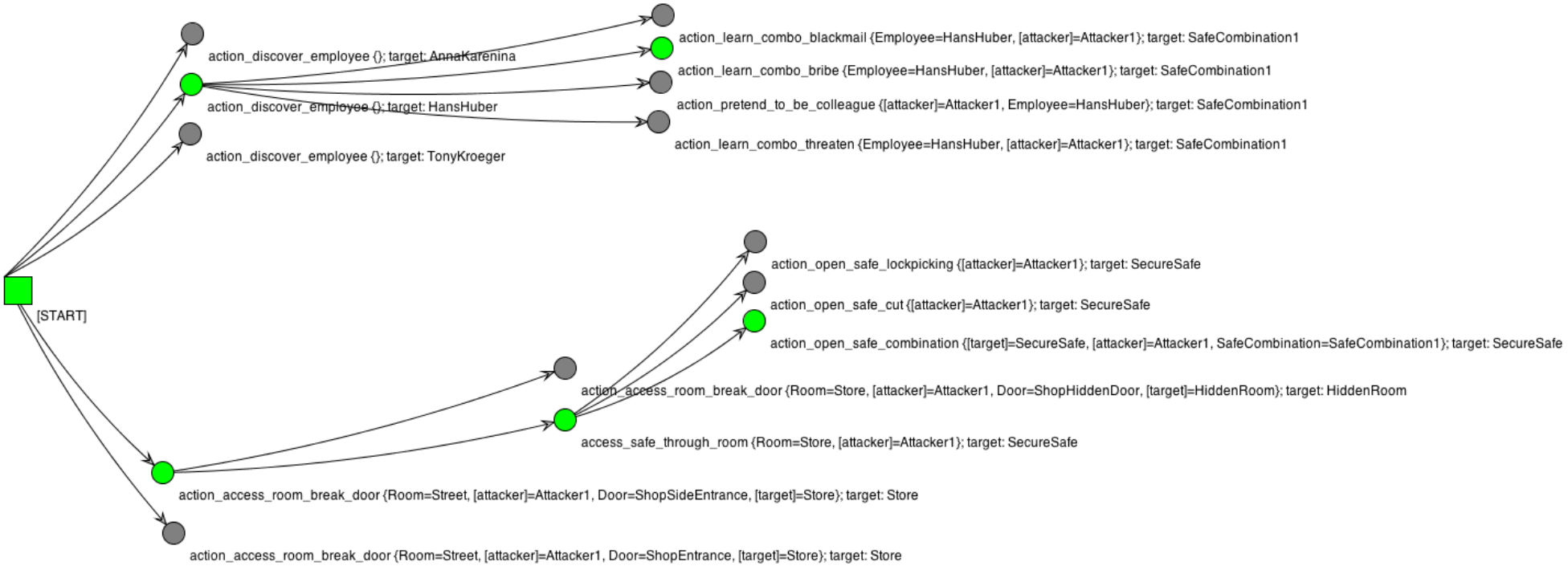
Concrete attack graphs - Safe Example



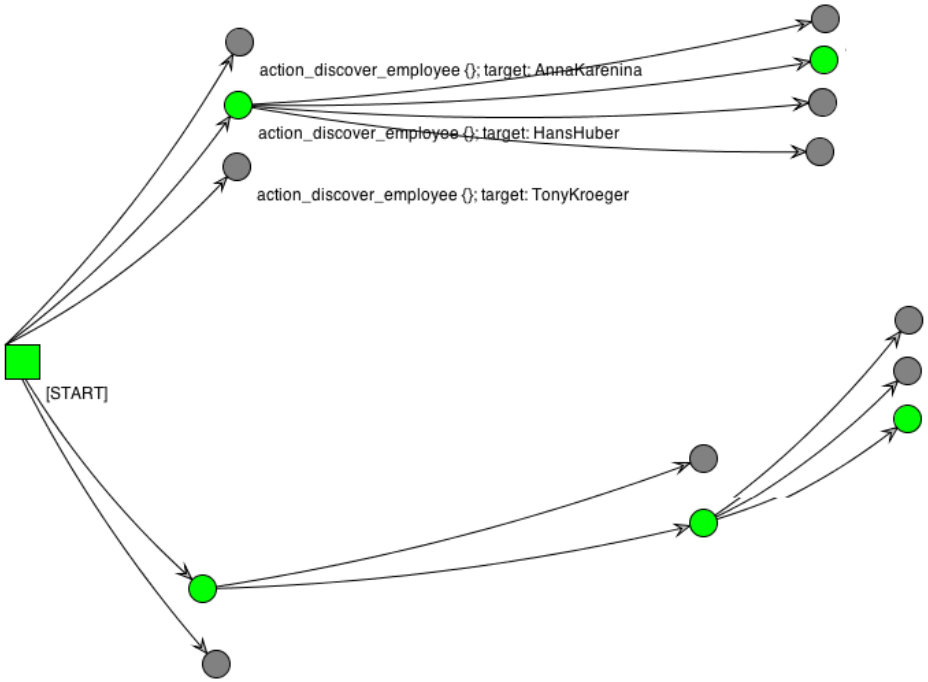
Concrete attack graphs - Safe Example



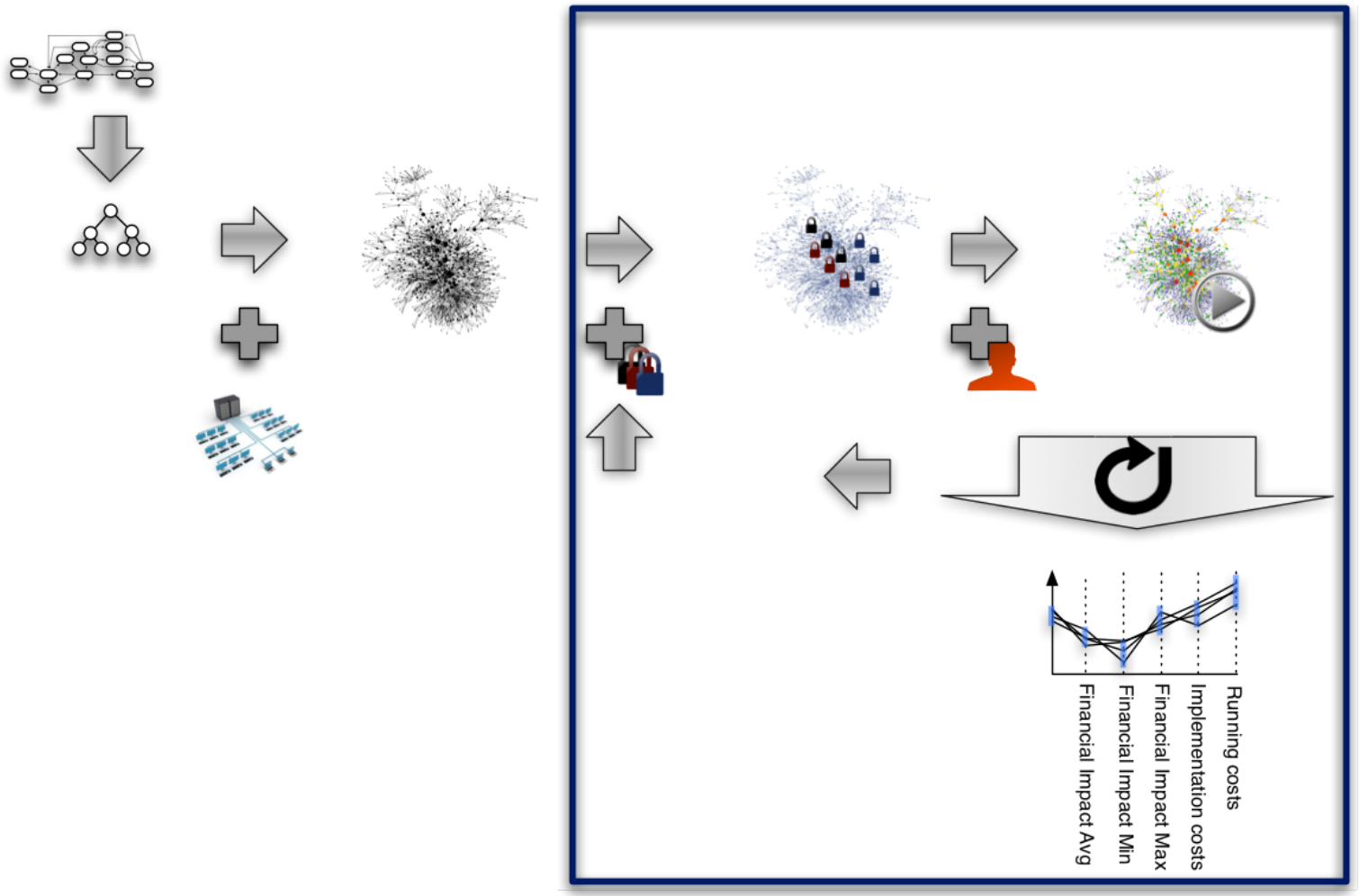
Concrete attack graphs - Safe Example



Concrete attack graphs - Safe Example



Outlook


Financial Impact Avg
Financial Impact Min
Financial Impact Max
Implementation costs
Running costs

Outlook

Current research

- Attack models and infrastructure scenarios (for limited domains)
- Threat agent model
  - Cognitive model (attack map)
  - Behavioral model (i.e., selection of attack actions)
- Modeling of security controls

Future work

- Harness existing attack knowledge (e.g. CAPEC)
- Simulation: dynamic and probabilistic aspects
- Multiobjective optimization of control bundles

Q&A

ekiesling@sba-research.org

Approaches to security control selection

Fixing of individual vulnerabilities (e.g. prioritized by "severity"):

- tends to focus only on technical vulnerabilities
- "vulnerabilities" are not always readily identifyable, but may emerge as a result of complex interactions
- may lead to reactive "ad-hoc" approach to security
  $\rightarrow$ "hamster wheel of pain" [?]

Standards and best practices

- are a significant improvement over reactive approaches but ...
- ... frequently provide only general, high-level recommendations
- ... are limited in their potential to support organization-specific threat scenarios
- ... are not necessarily applicable to and sufficient for the actual risk an organization faces