Simulation-based optimization of IT security controls

Initial experiences with meta-heuristic solution procedures

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

14^{th} EU/ME Workshop

February 28 – March 1, 2013; Hamburg, Germany

Funded by the Austrian Science Fund under project number P 23122-N23 FWF

Agenda

Introduction

Framework

- Overview
- Knowledge base
- Attack patterns
- Simulation
- Optimization

Example scenarios

- Simple
- Advanced

Conclusions

Introduction
Current IT security management challenges

- Information systems are growing ever more complex
- Today's serious threats are not opportunistic, but
  - deliberate, targeted attacks
  - that exploit multiple attack vectors
    - software vulnerabilities
    - network vulnerabilities
    - insider knowledge and access
    - social engineering techniques
    - ...
- Human threat agents are heterogeneous

  hacktivists, script kiddies, insiders, advanced persistent threats ...

  → "secure against whom?"

Introduction
Current IT security management challenges

- Information systems are growing ever more complex
- Today's serious threats are not opportunistic, but
  - deliberate, targeted attacks
  - that exploit multiple attack vectors
    - software vulnerabilities
    - network vulnerabilities
    - insider knowledge and access
    - social engineering techniques
    - ...
- Human threat agents are heterogeneous

  hacktivists, script kiddies, insiders, advanced persistent threats ...

  → "secure against whom?"

Introduction
Current IT security management challenges

- Information systems are growing ever more complex
- Today's serious threats are not opportunistic, but
  - deliberate, targeted attacks
  - that exploit multiple attack vectors
    - software vulnerabilities
    - network vulnerabilities
    - insider knowledge and access
    - social engineering techniques
    - ...
- Human threat agents are heterogeneous

  hacktivists, script kiddies, insiders, advanced persistent threats ...

  → "secure against whom?"

Introduction
Current IT security management challenges

- Information systems are growing ever more complex
- Today's serious threats are not opportunistic, but
  - deliberate, targeted attacks
  - that exploit multiple attack vectors
    - software vulnerabilities
    - network vulnerabilities
    - insider knowledge and access
    - social engineering techniques
    - ...
- Human threat agents are heterogeneous

  hacktivists, script kiddies, insiders, advanced persistent threats ...

  $\rightarrow$ "secure against whom?"

Introduction
Core ideas

Security:

- is meaningless without defining "against whom"
- is the result of the combined effect of all implemented security controls
- involves tradeoffs between multiple monetary and non-monetary criteria

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

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

Introduction
Core ideas

Security:

- is meaningless without defining "against whom"
- is the result of the combined effect of all implemented security controls
- involves tradeoffs between multiple monetary and non-monetary criteria

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

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

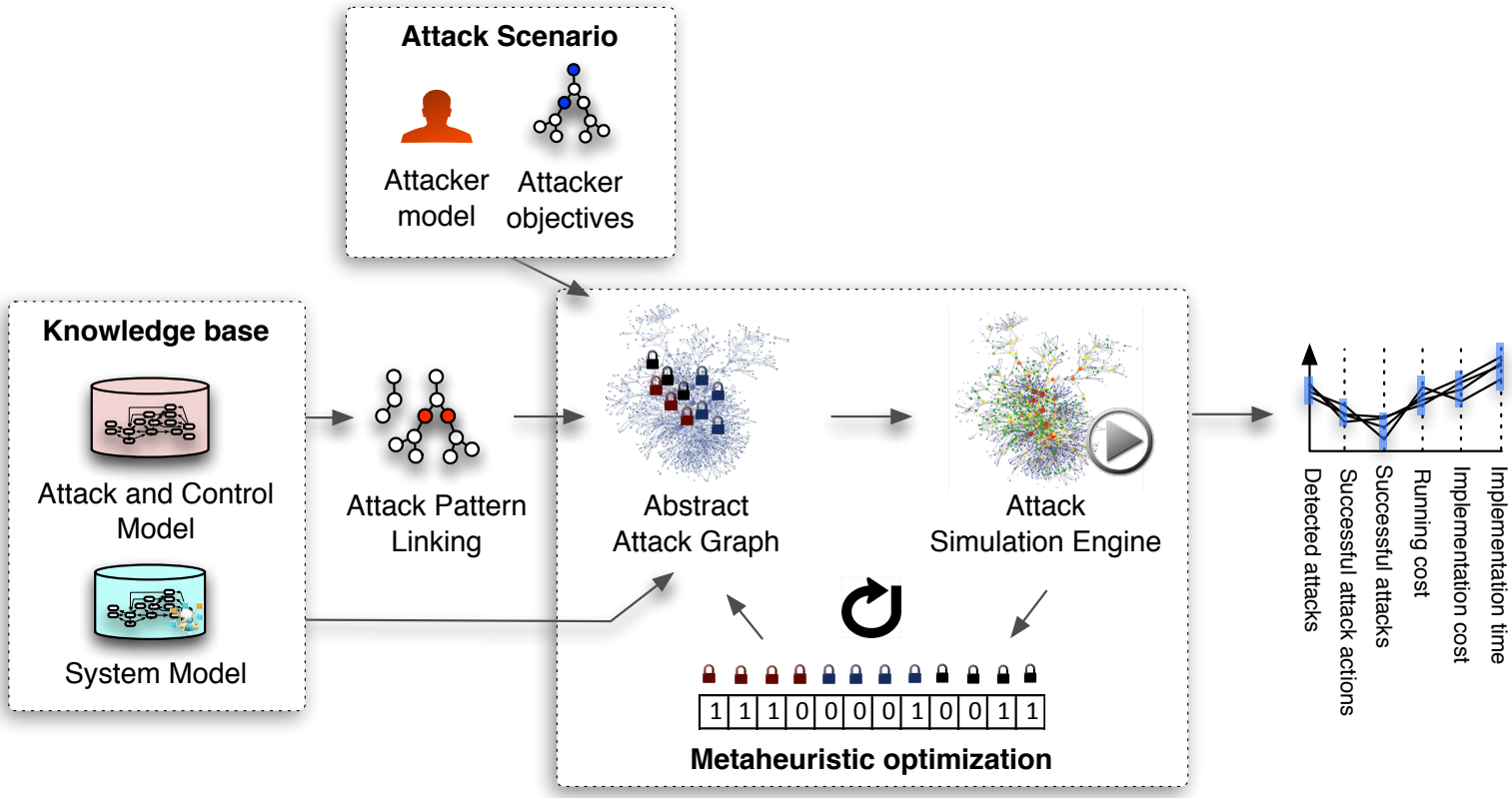
Framework
Overview

Objective: choose an “optimal" set of security controls

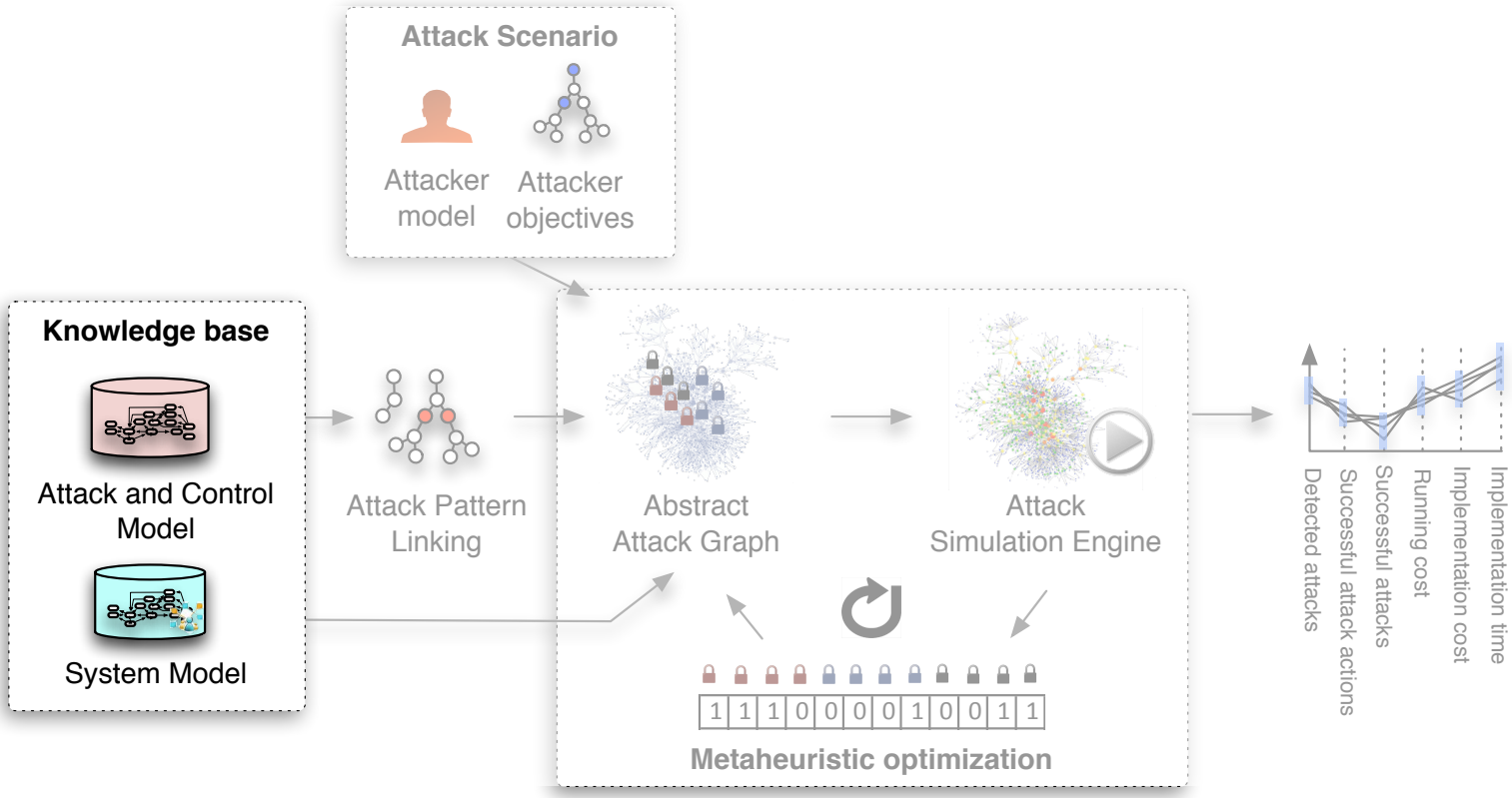
Approach:

1. Model
   - abstract causal structures (attack actions)
   - attack agent behavior
   - context (assets, employees . . .)
2. Apply control sets and simulating attacks
3. Identify efficient sets of controls through multi-criteria optimization

Framework
Overview



Framework
Overview

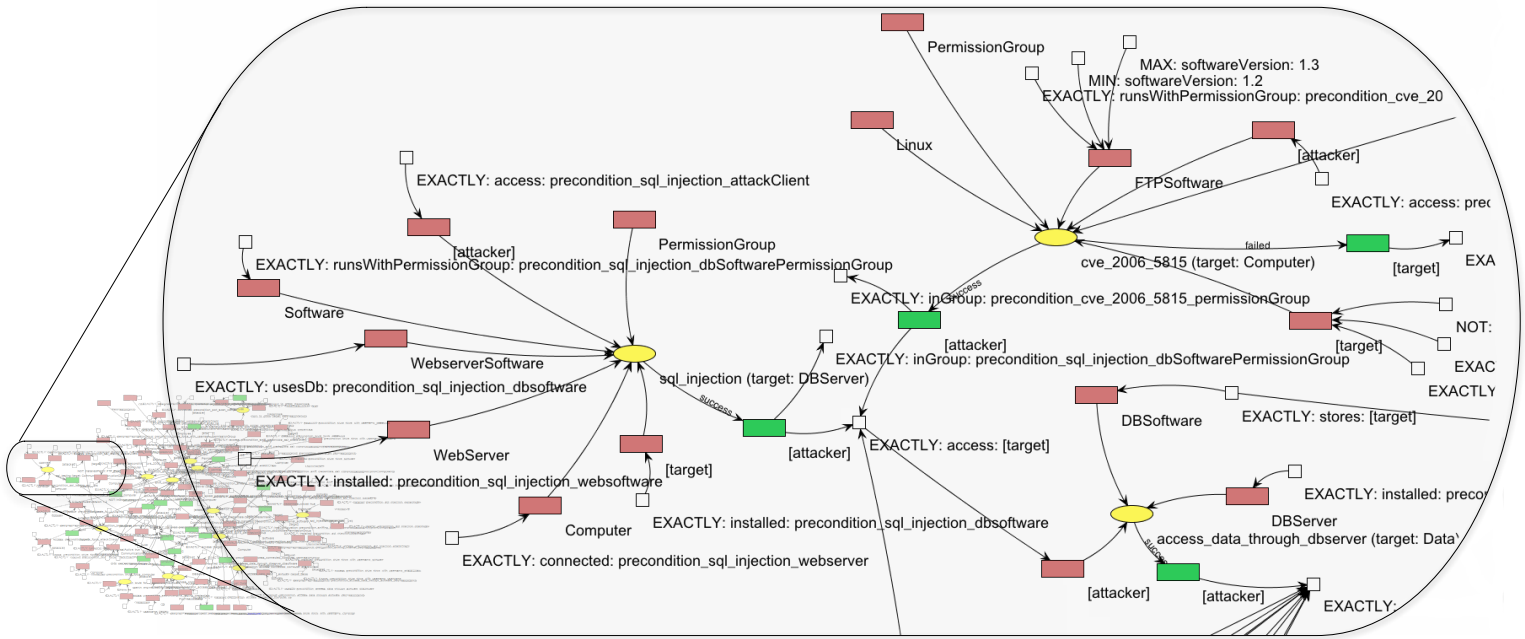


Framework
Knowledge base

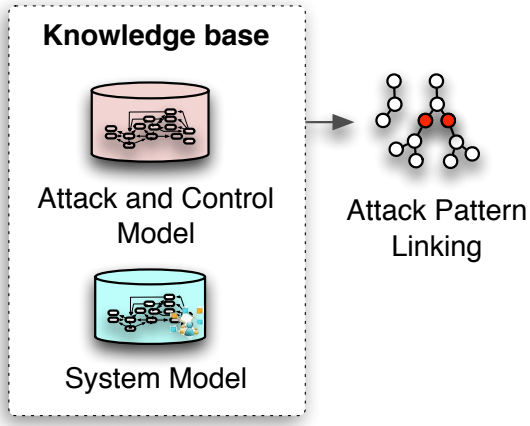
- Abstract attack knowledge (causal structure) + system structure knowledge
- Initial experiments with OWL ontologies
- Current rule-based implementation: SWI-Prolog[1]

[1] http://www.swi-prolog.org/man/clpfd.html

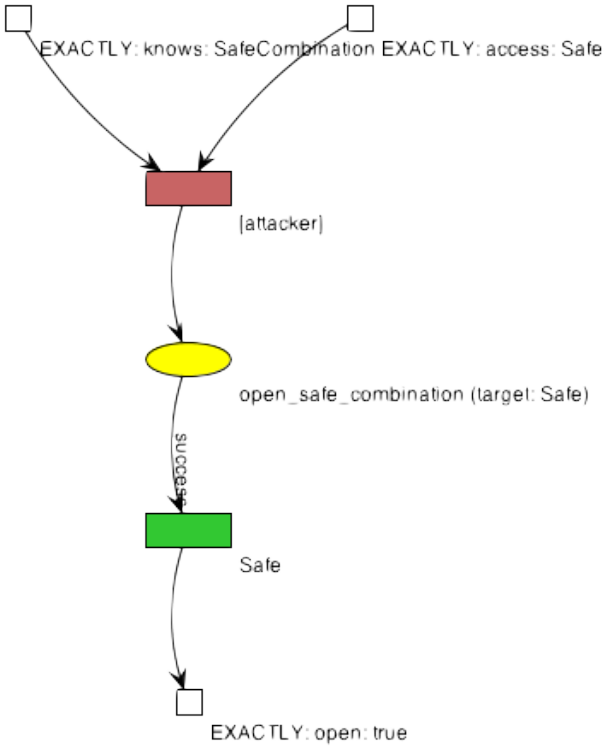
Framework
Knowledge base



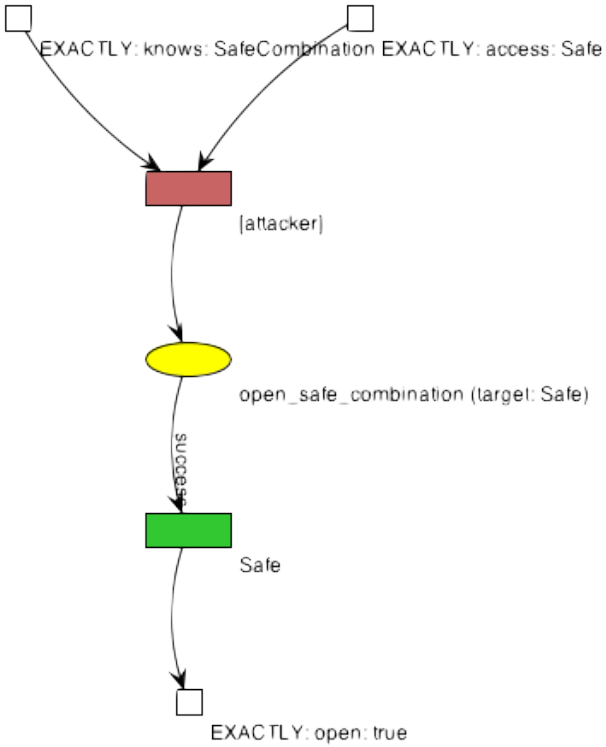
Framework
Overview



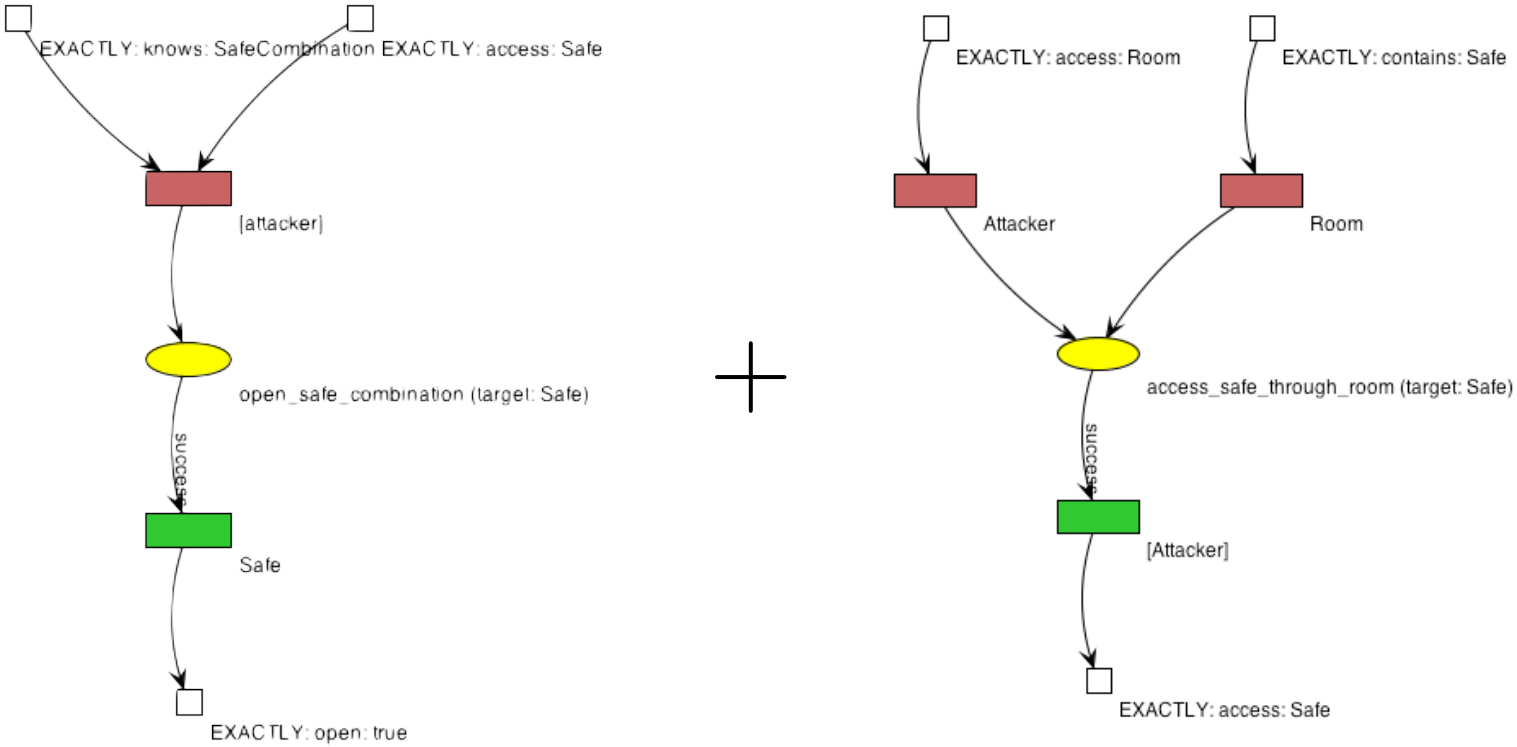
Framework
Attack pattern linking



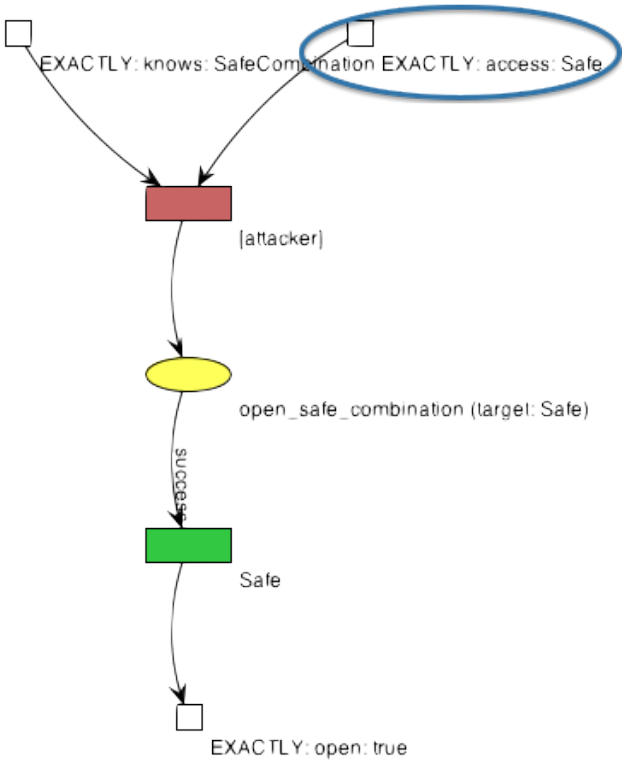
Framework
Attack pattern linking

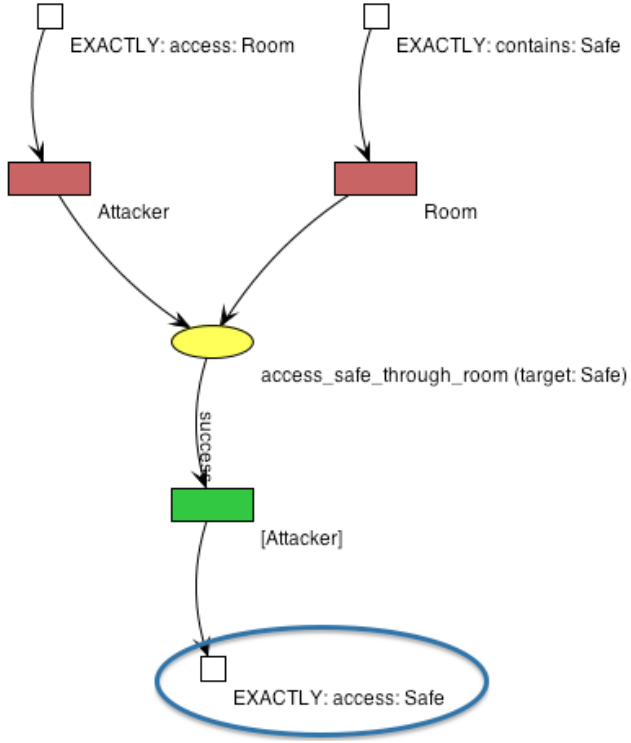


Framework
Attack pattern linking

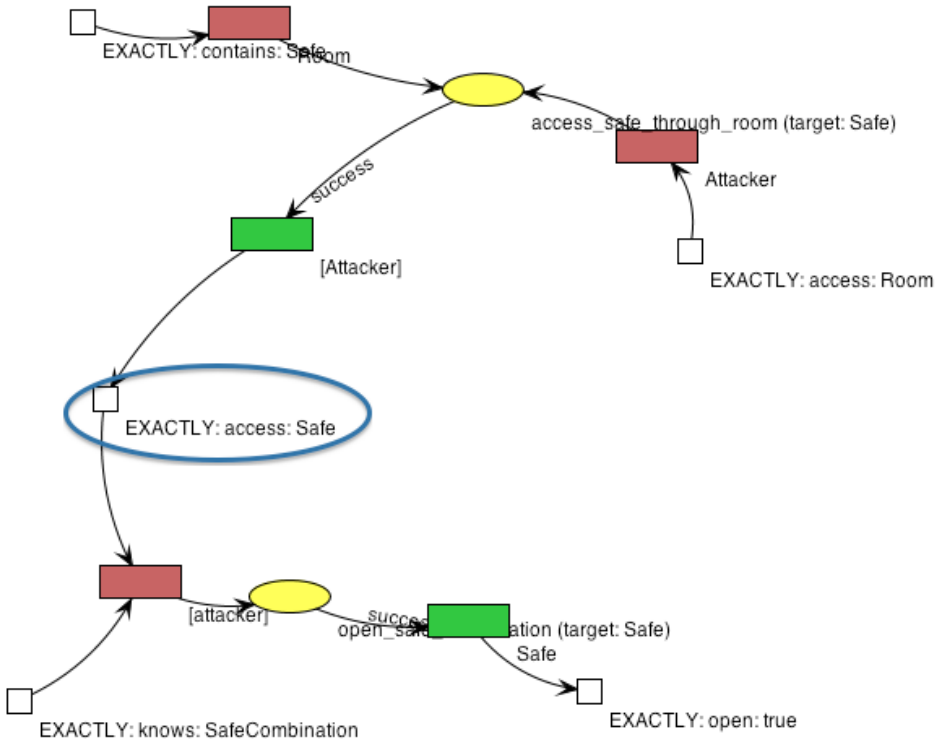


Framework
Attack pattern linking

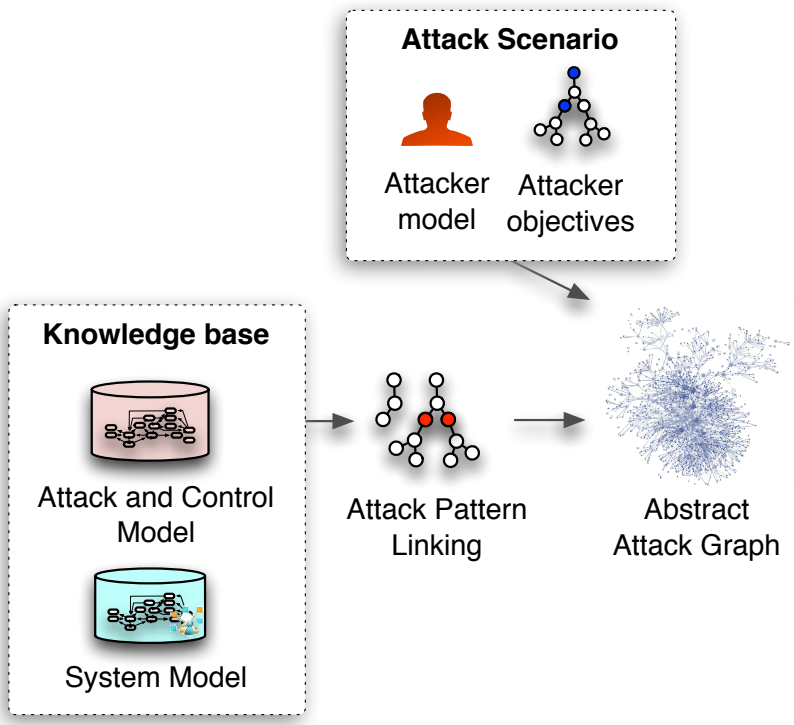




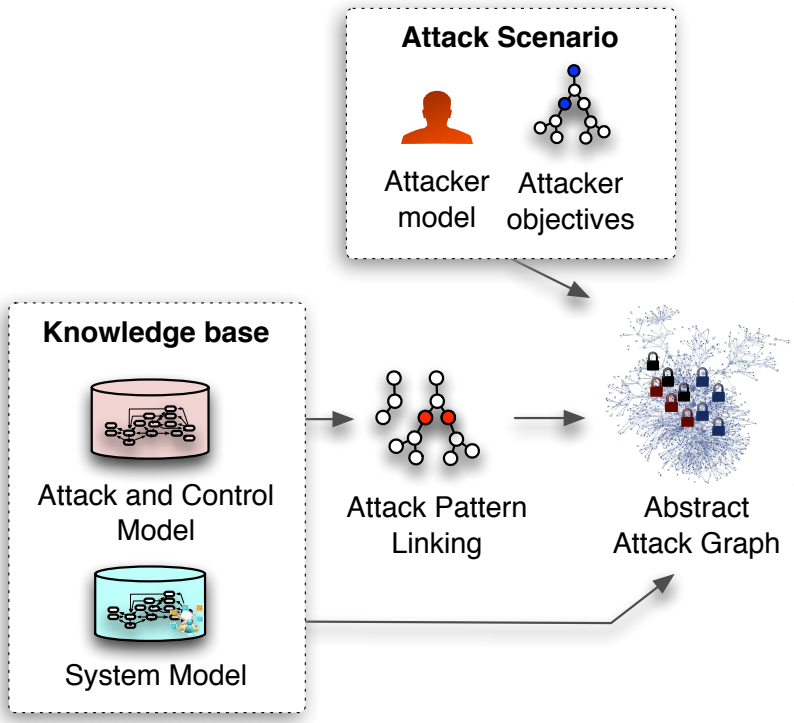
Framework
Attack pattern linking



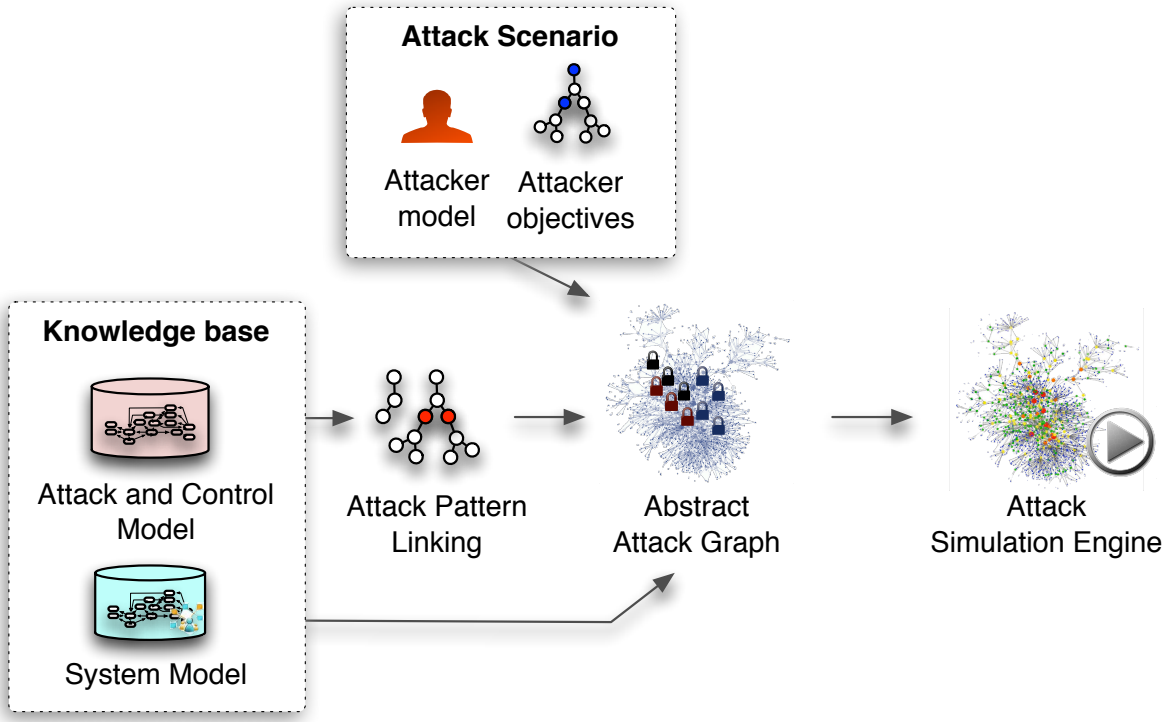
Framework
Overview



Framework
Overview



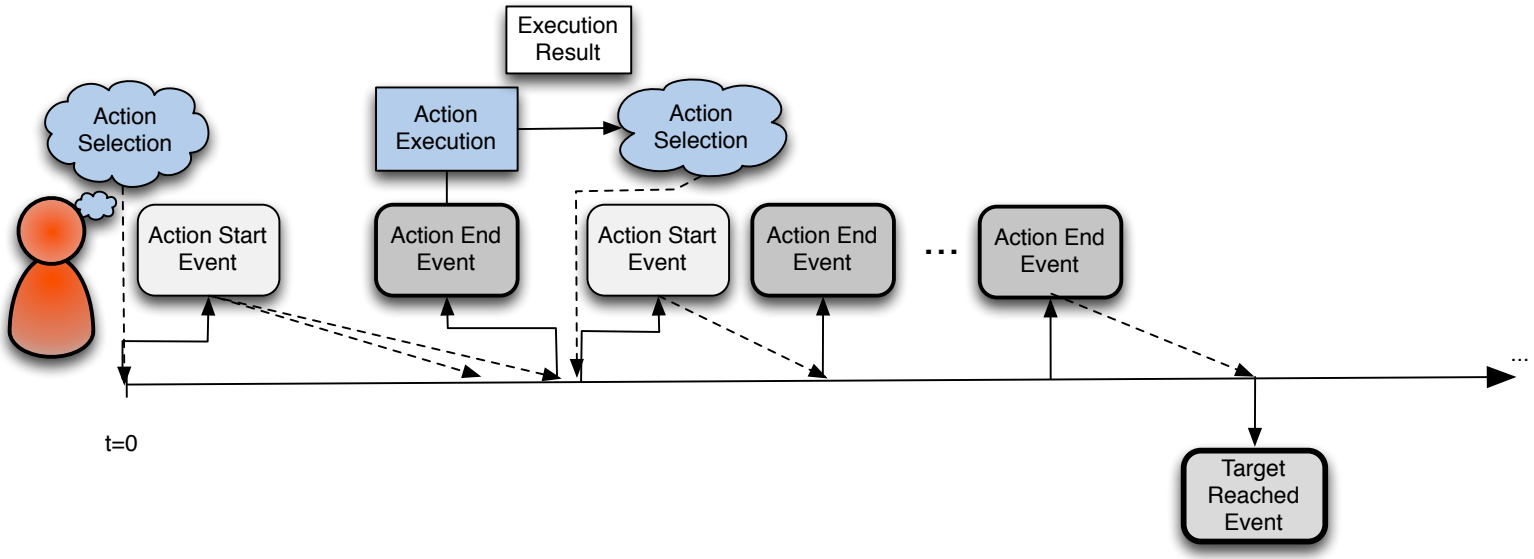
Framework
Overview



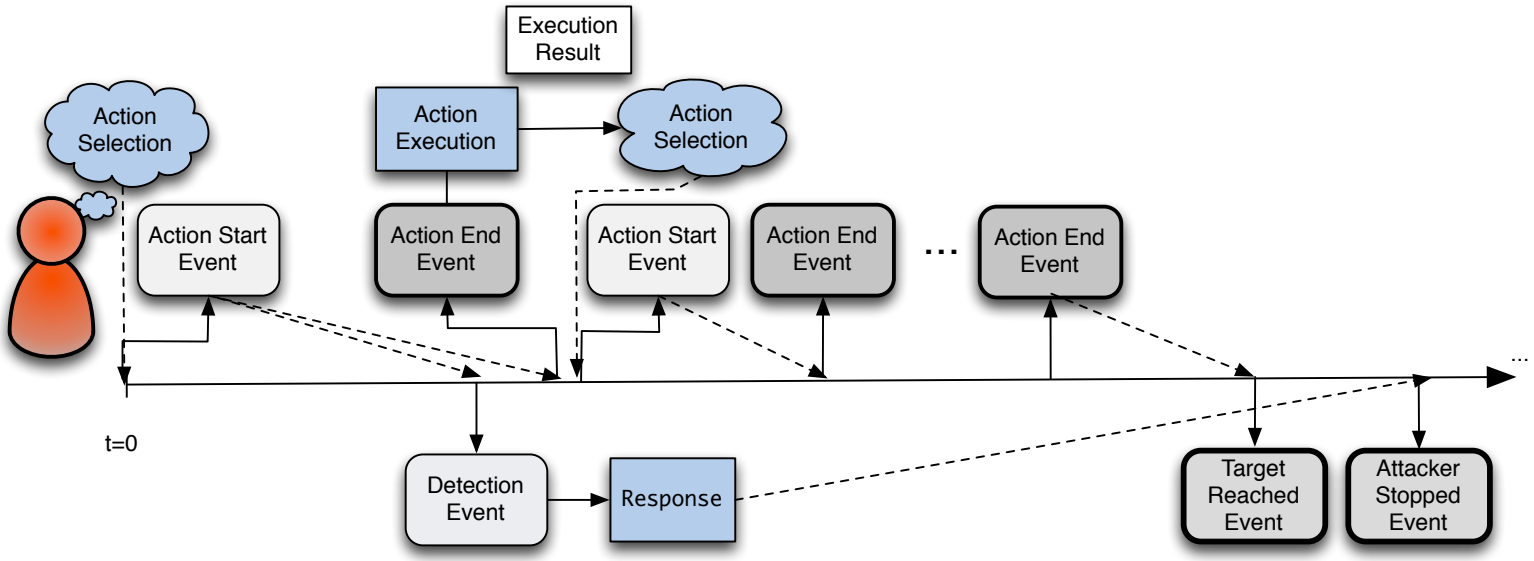
Simulation
Discrete Event Scheduling

Simulation
Discrete Event Scheduling

Simulation
Discrete Event Scheduling

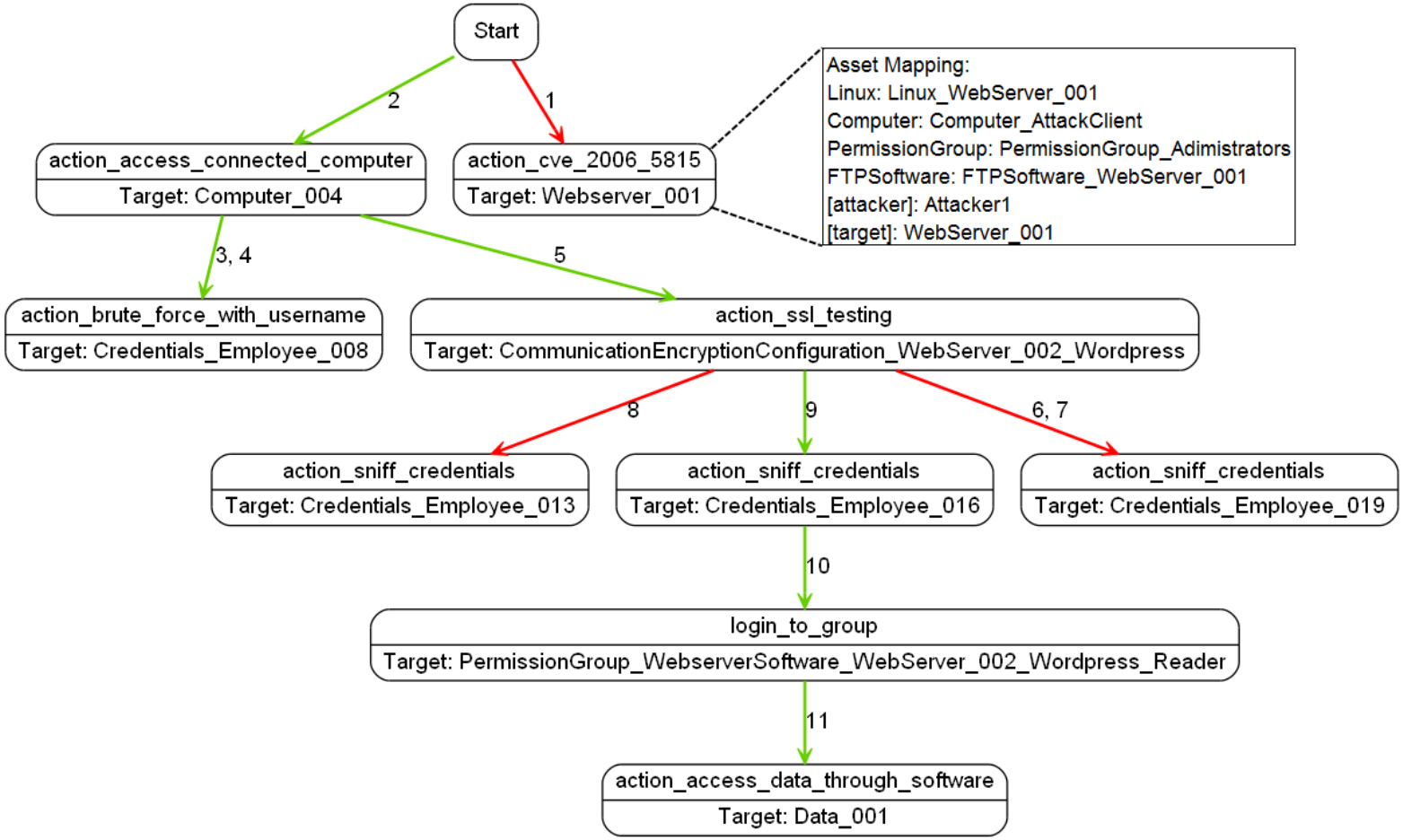


Simulation
Discrete Event Scheduling

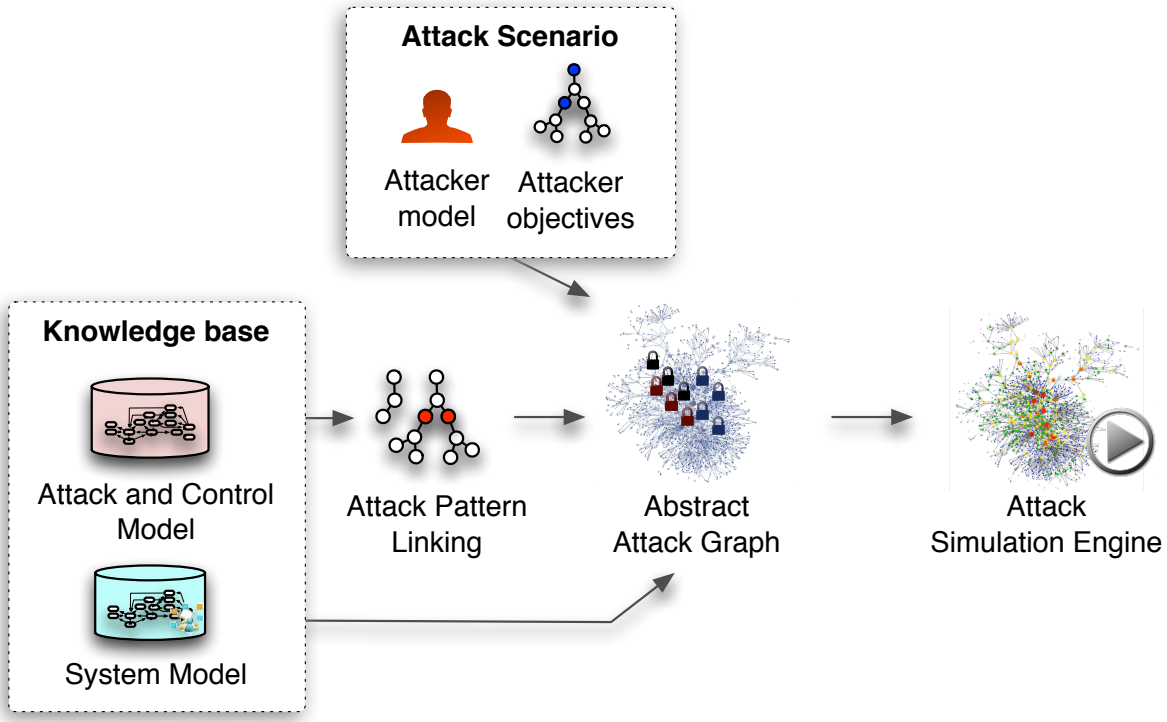


Simulation

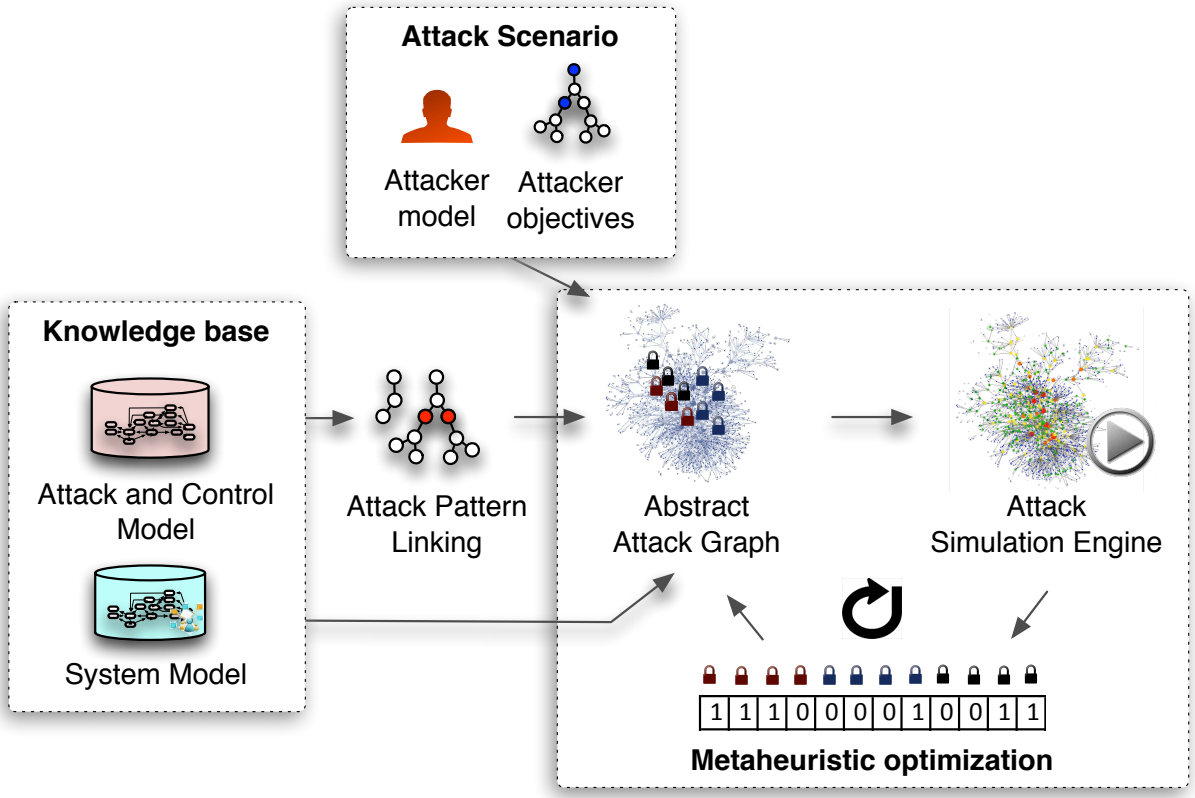
Example attack sequence



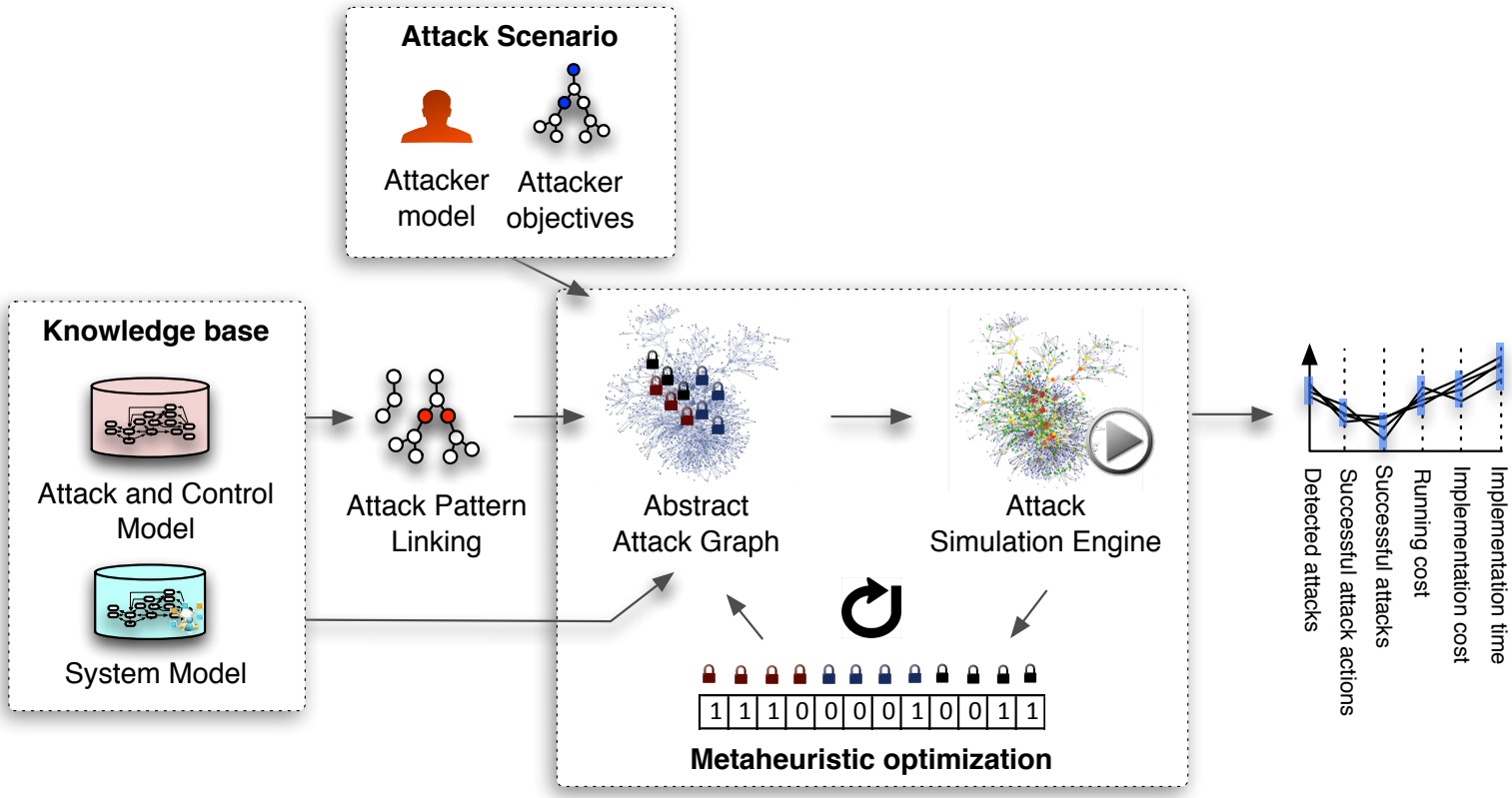
Framework
Overview



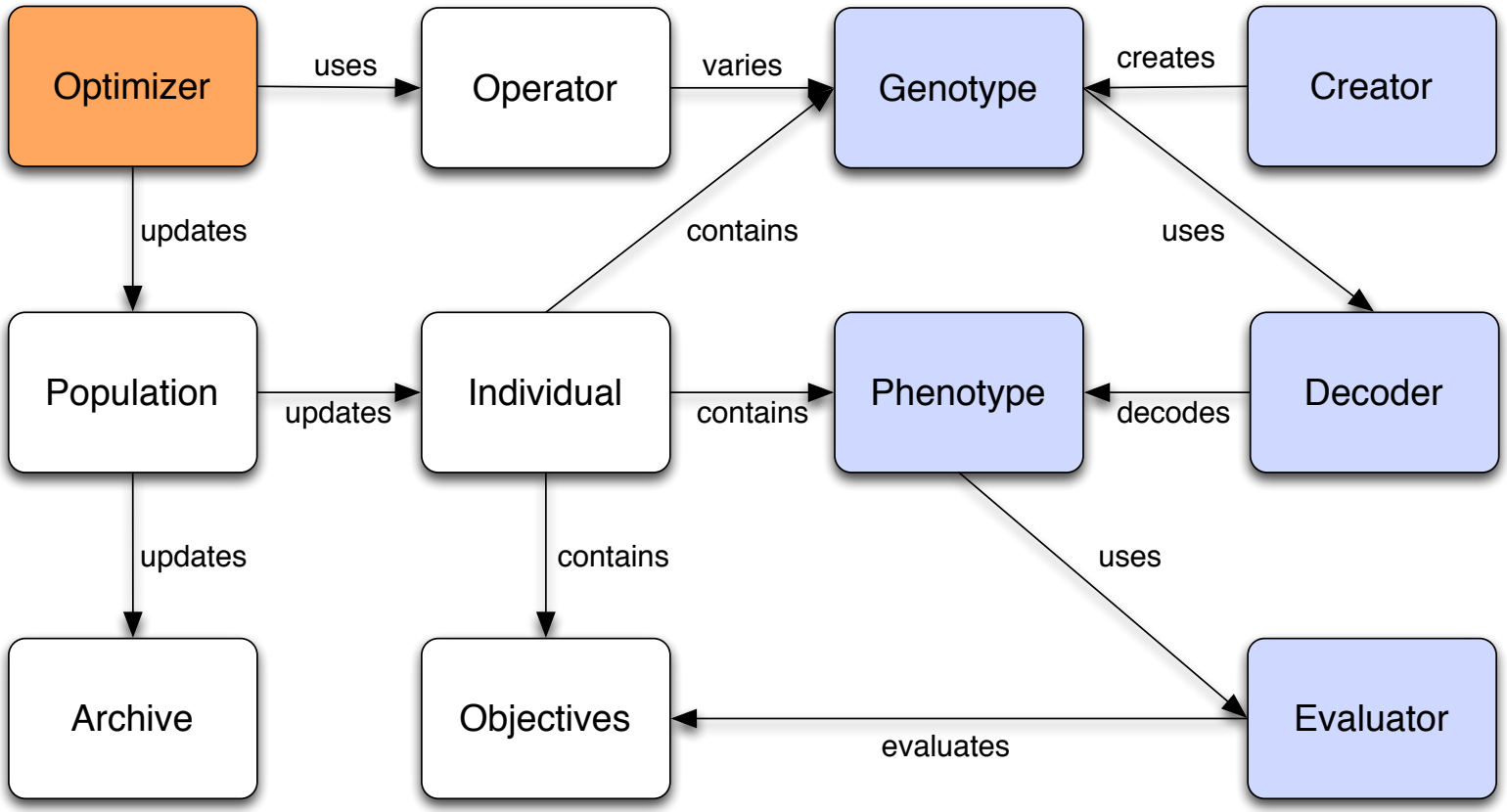
Framework
Overview



Framework
Overview

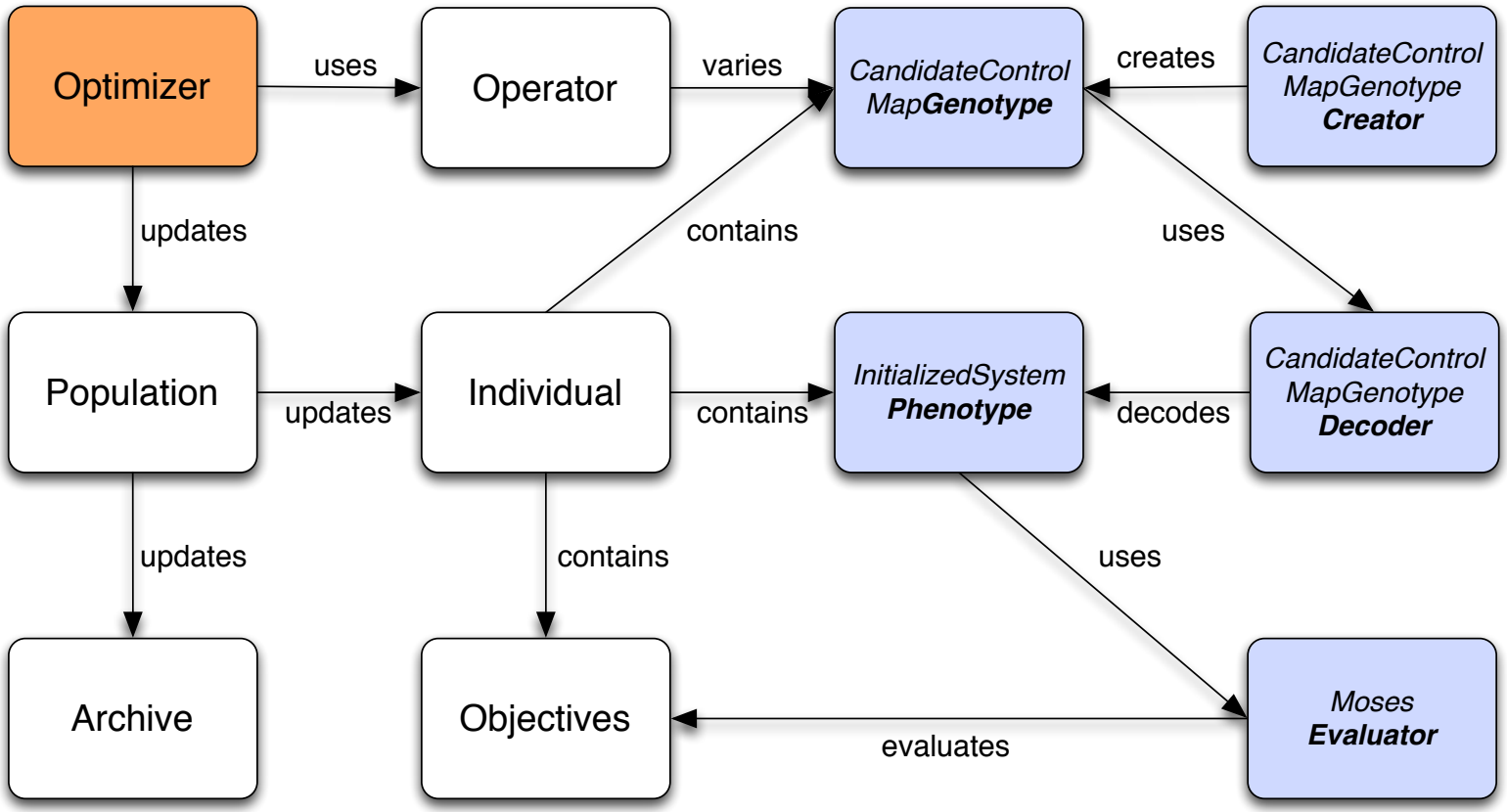


Optimization
Opt4j-based implementation



Source: adapted from **?**

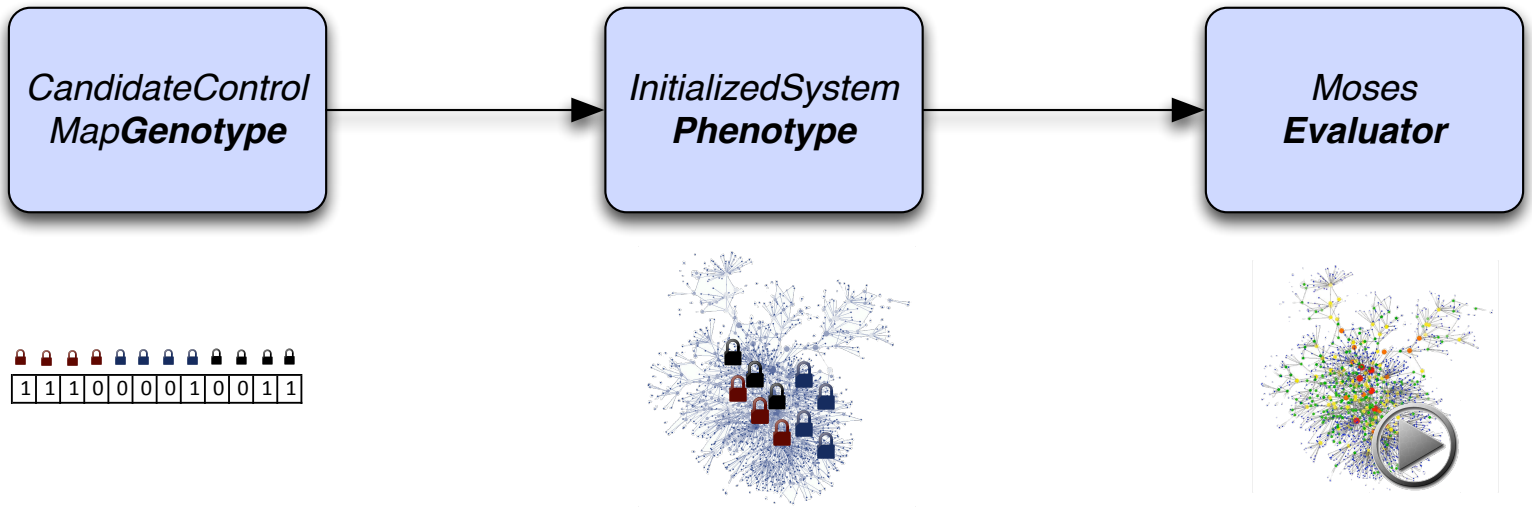
Optimization
Opt4j-based implementation



Source: adapted from **?**

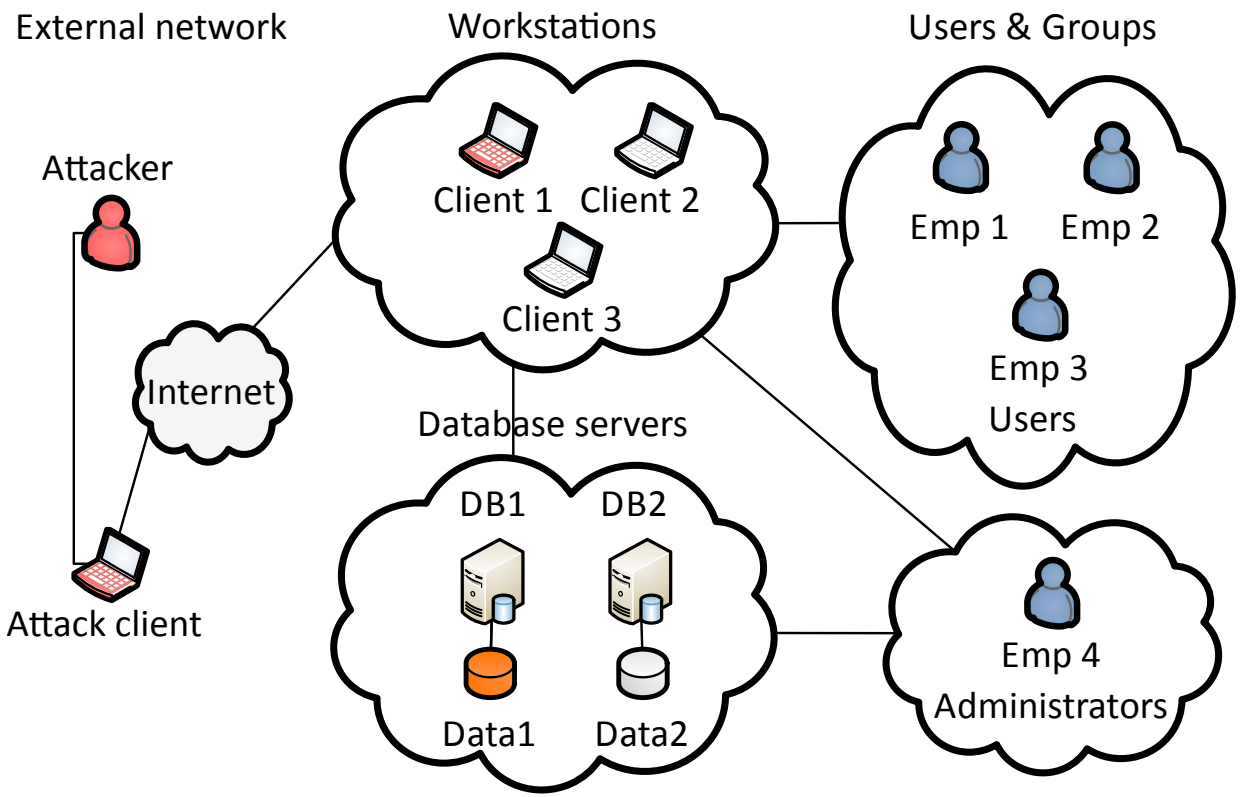
Optimization

Evaluation of candidate control portfolios

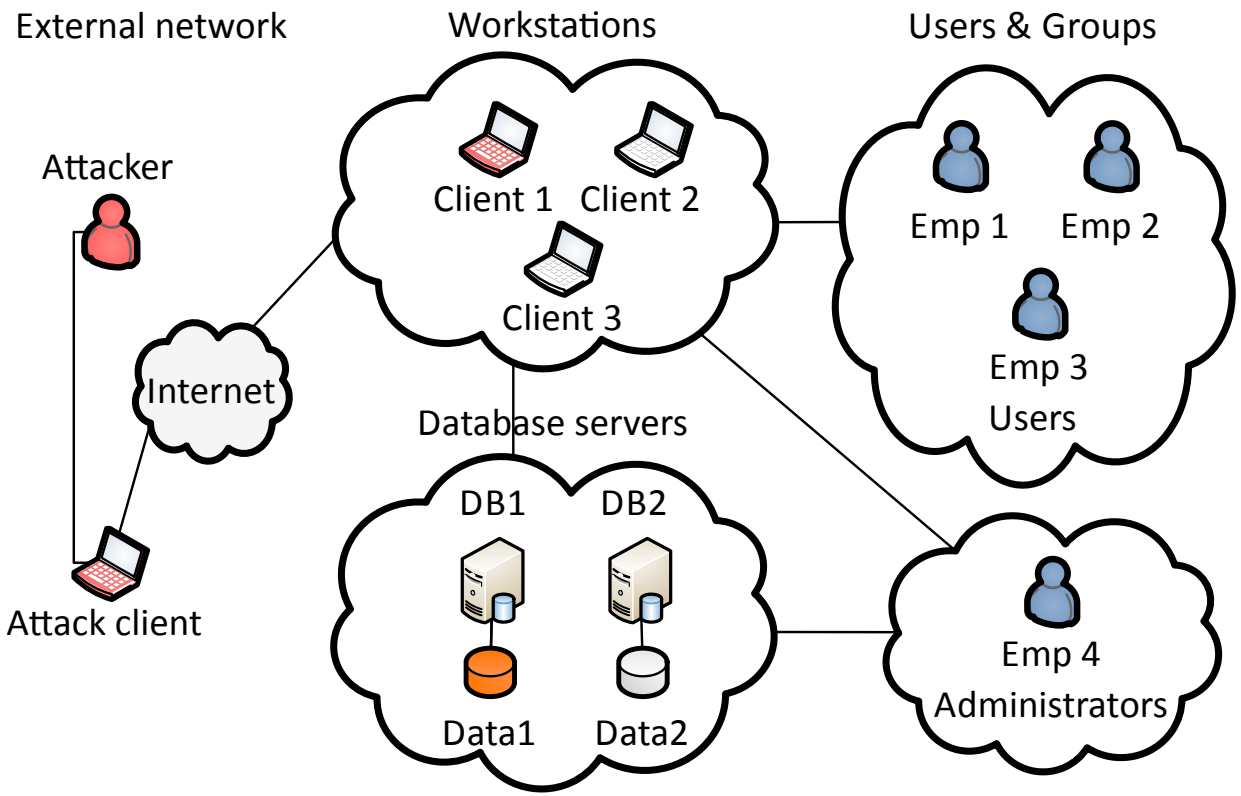


- Probabilistic, requires many replications per candidate control set
- Currently reduced to a deterministic problem using expected/median/worst case values etc.

Simple Scenario
Domain

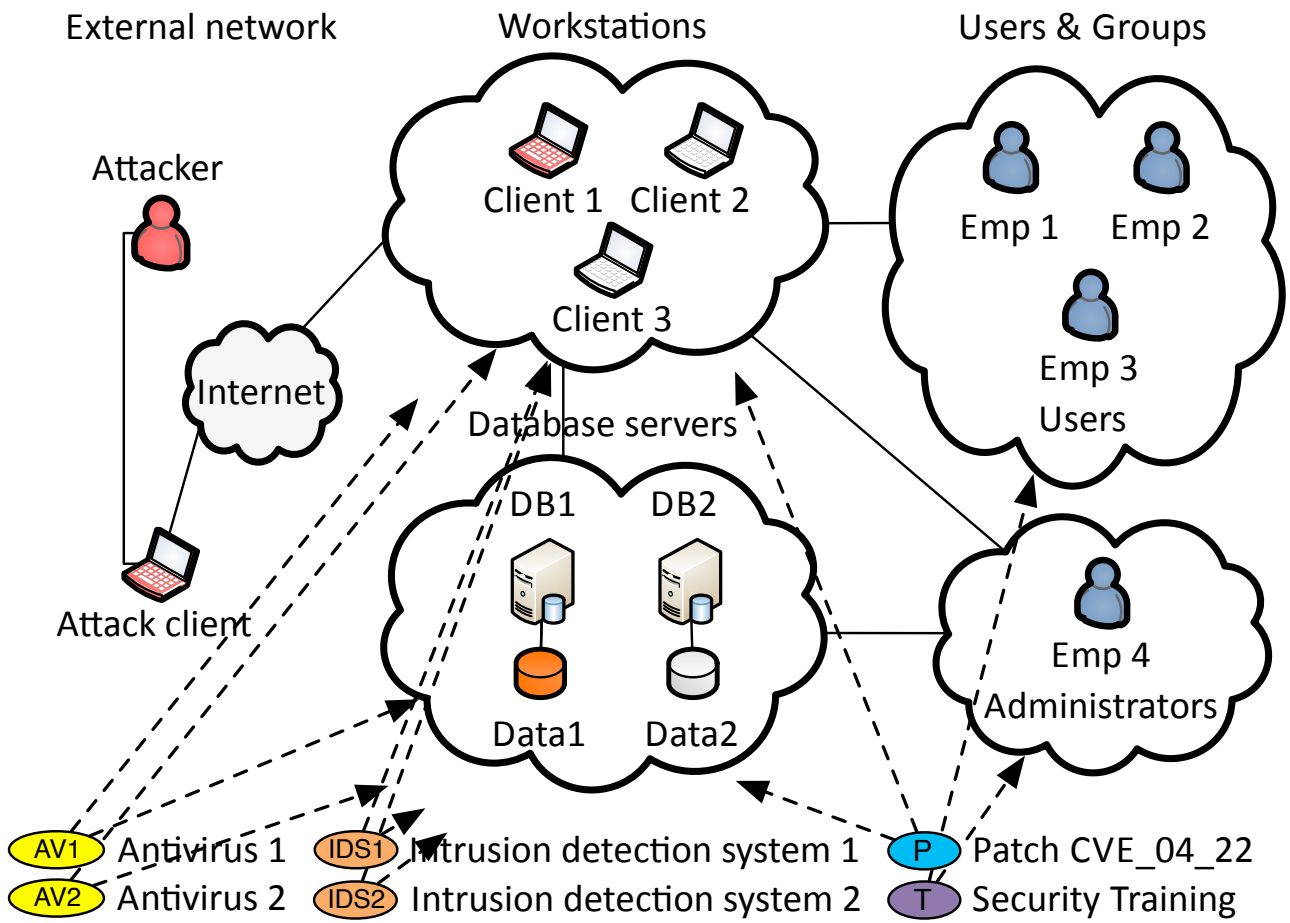


Simple Scenario
Domain



AV1 Antivirus 1 IDS1 Intrusion detection system 1 P Patch CVE_04_22
AV2 Antivirus 2 IDS2 Intrusion detection system 2 T Security Training

Simple Scenario
Domain



Simple Scenario
Decision variables and objectives

Decision space: 12 binary variables

Objectives:

1. Cost (MIN)
2. Successful attack actions ratio (MIN)
3. Target condition reached average (MIN)
4. Share of undetected detectable attack actions (MIN)

Attacker objective: access Data1 on DB1

Simple scenario
Algorithms and parameter settings

Simulation parameters

- 50 replications per candidate set
- Random "drill-down" decision model

Optimization parameters (NSGA2 and SPEA2)

- Generations: 100
- Population size (α): 100
- Number of parents per generation (μ): 25
- Number of offsprings per generation (λ): 25
- Crossover:
  - Rate: 0.95
  - Single crossover point
- Mutation: constant rate 0.05

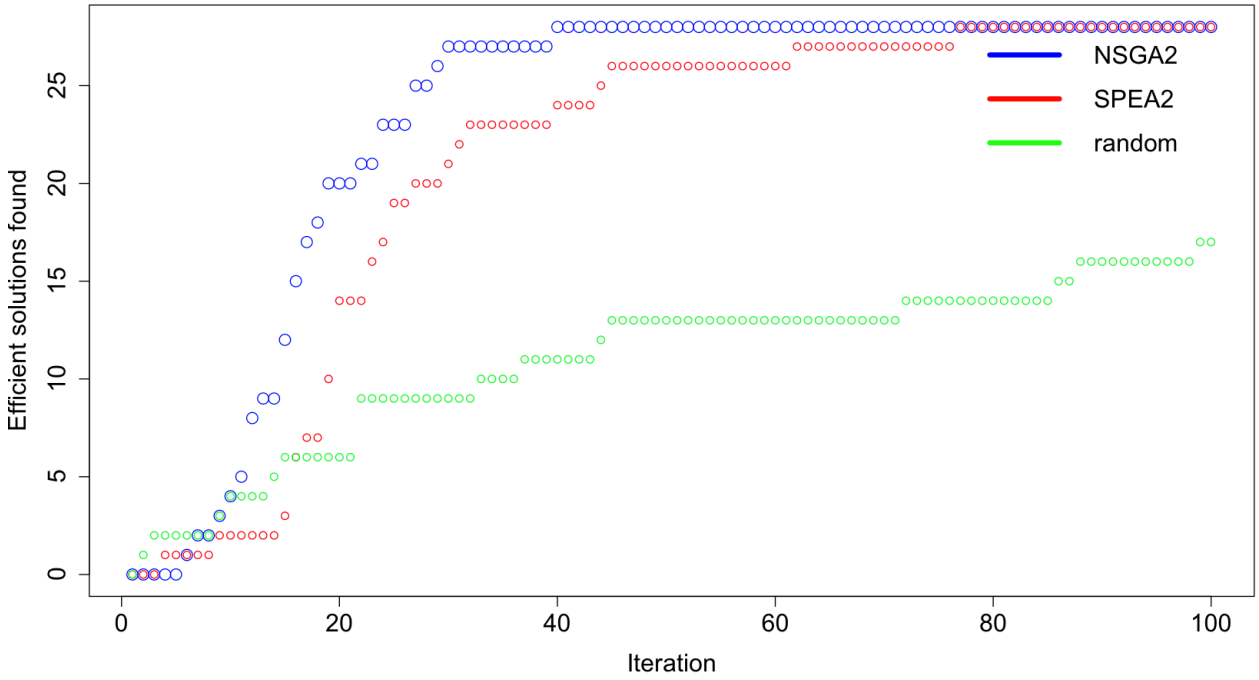
Initial Results

Simple scenario

Runtime (search space: 2^{12})

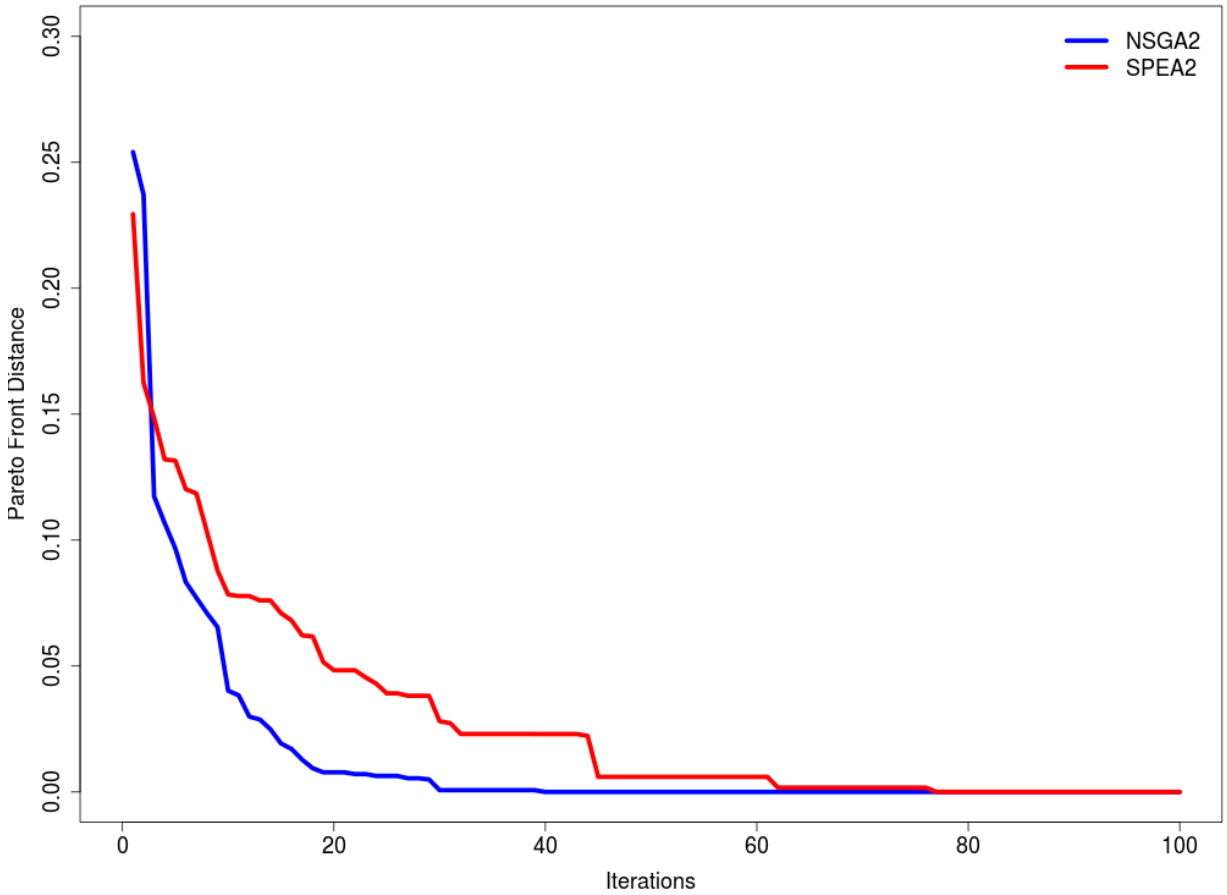
- per replication: $\sim 25ms$ (3GHz DualCore Xeon)
- per evaluation: $\sim 1,250ms$ (50 replications)
- total: CE: 183min, NSGA2: 61min, SPEA2: 70min

Efficient solutions:



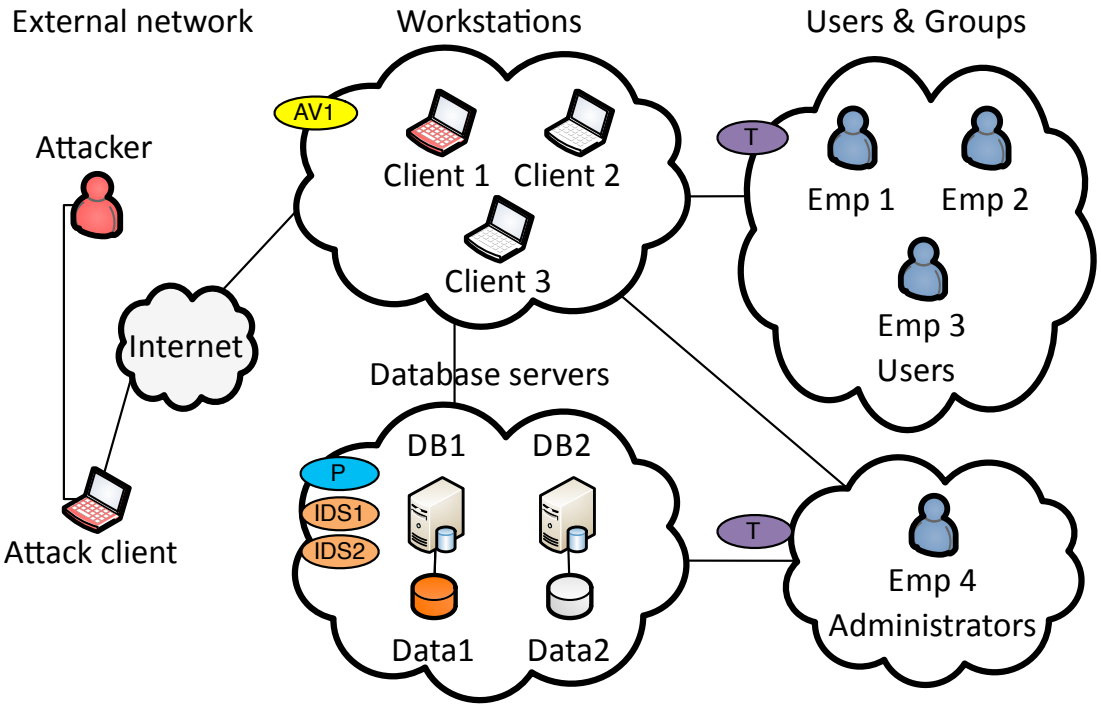
Initial Results

Simple scenario



$$Q_4(A) = \frac{1}{|CE|} \sum_{r \in CE} \min_{z \in A} D(z,r)$$

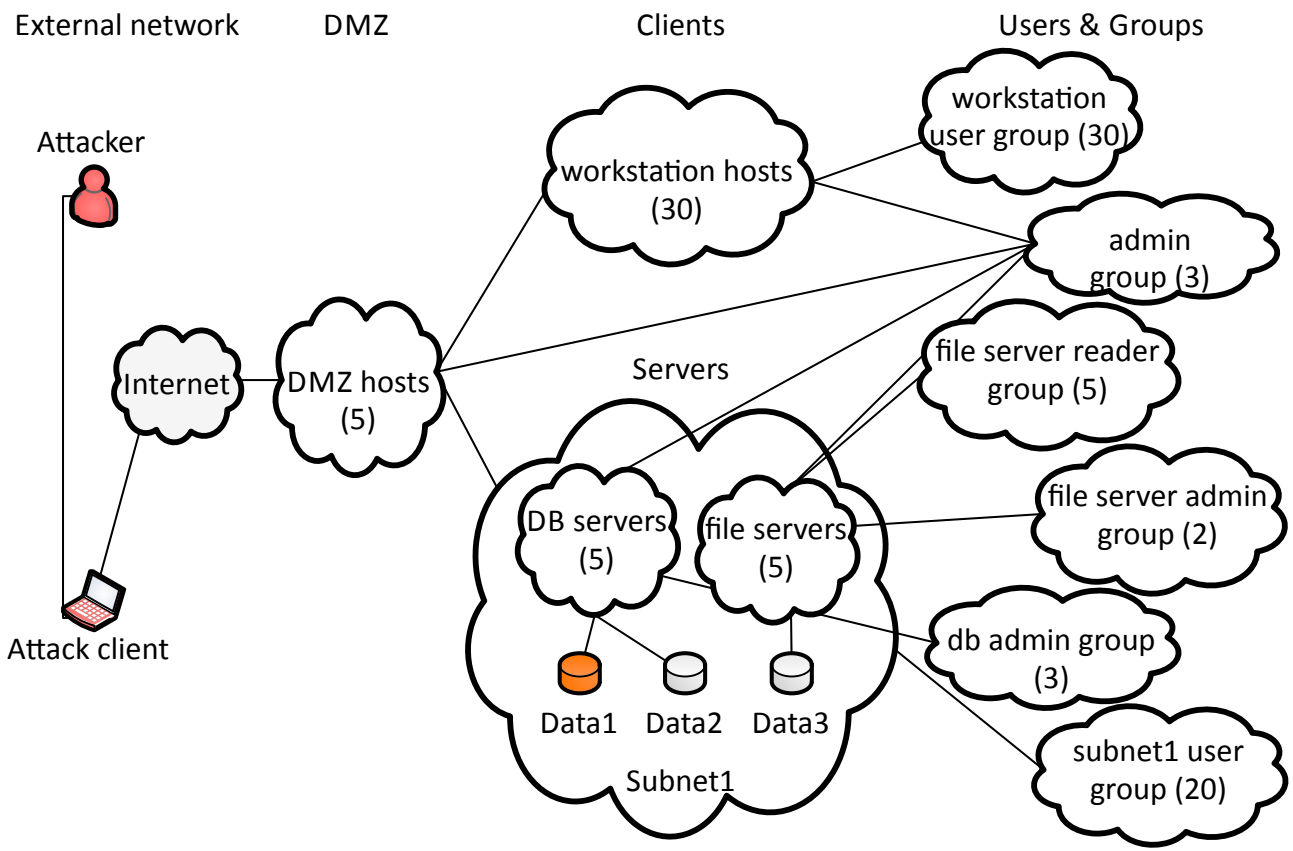
Simple scenario
Example efficient solution



AV1 Antivirus 1 — IDS1 Intrusion detection system 1 — P Patch CVE_04_22
AV2 Antivirus 2 — IDS2 Intrusion detection system 2 — T Security Training

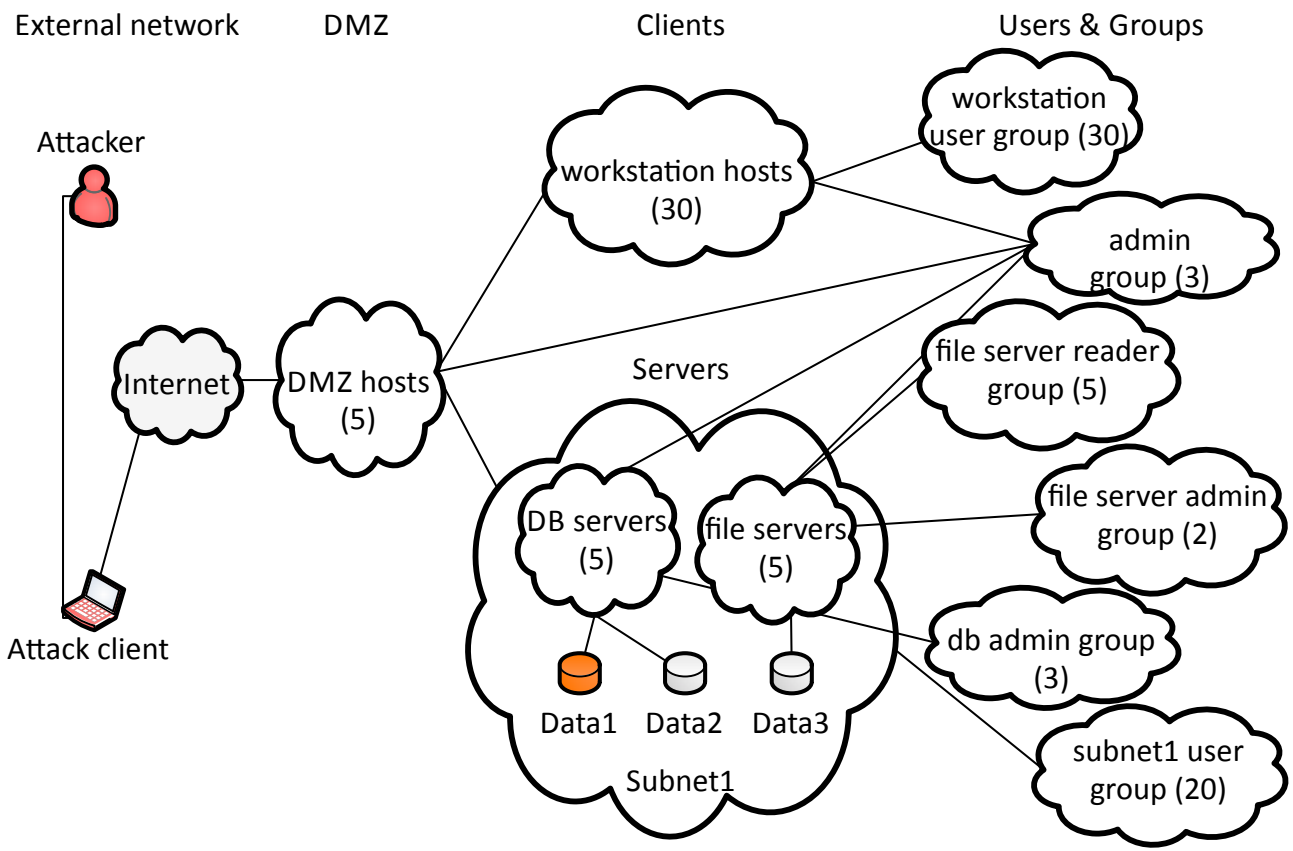
Cost	22.400
Successful attack actions ratio	0.000558
Target condition reached average	0.018519
Share of undetected detectable attack actions	0.083333

Advanced Scenario
Domain



Advanced Scenario

Domain



Applied controls:

1 Antivirus 1
2 Antivirus 2
1 Intrusion detection system 1
2 Intrusion detection system 2
P Patch CVE_2013_04_22
1 2 Logging Policy
1 2 3 Security Training

Advanced Scenario
Algorithms and parameter settings

Simulation parameters

- 50 replications per candidate set
- Random "drill-down" decision model

Optimization parameters (NSGA2 and SPEA2)

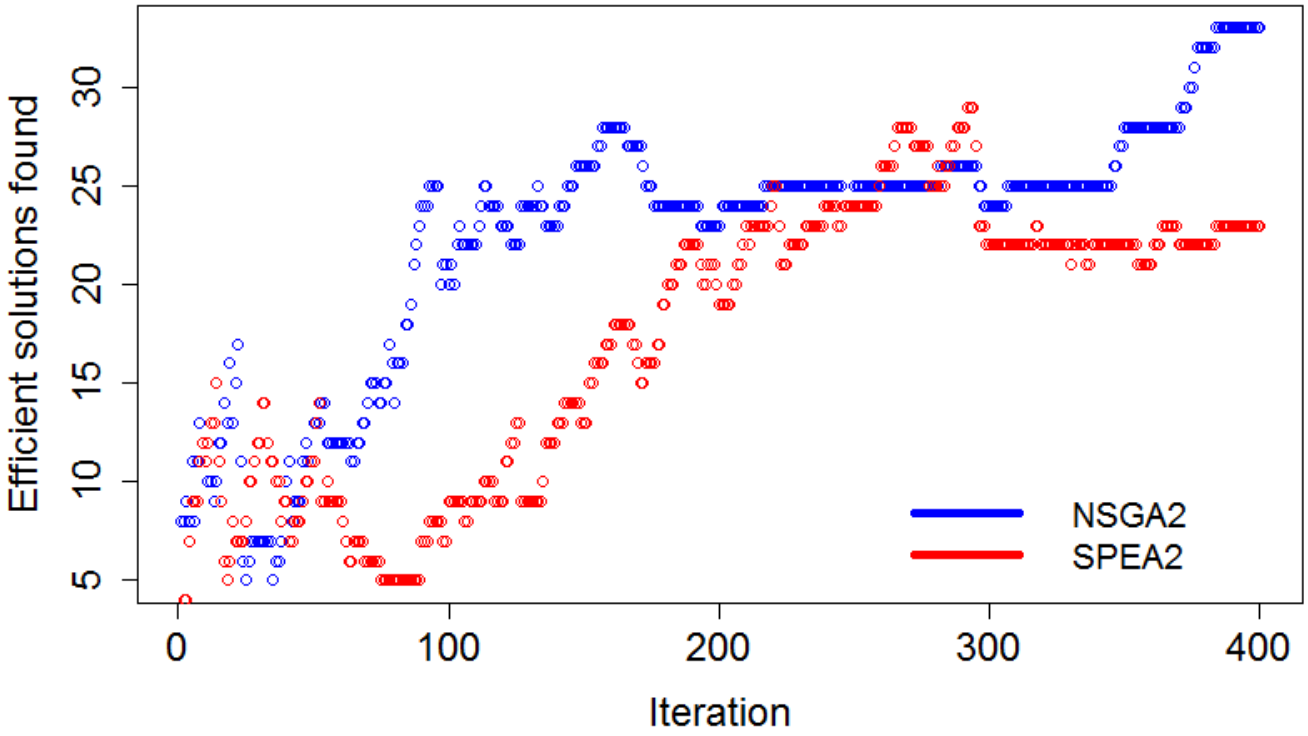
- Generations: 400
- Population size (α): 100
- Number of parents per generation (μ): 25
- Number of offsprings per generation (λ): 25
- Crossover:
  - Rate: 0.95
  - Single crossover point
- Mutation: constant rate 0.05

Initial Results
Advanced scenario

Runtime

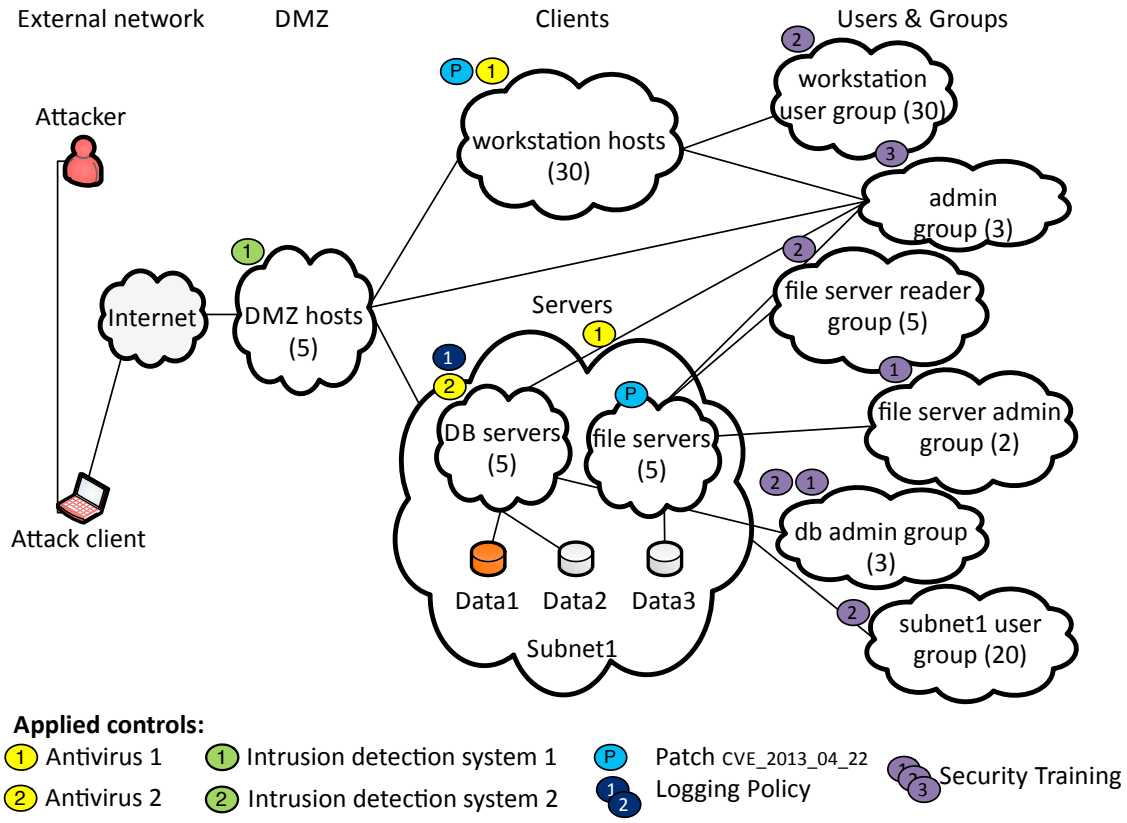
- per replication $\sim 30ms$ (3GHz DualCore Xeon)
- total: $\sim 4:30h$

Proposed efficient solutions



Advanced Scenario

Domain



Cost	15.330
Successful attack actions ratio	0.0185
Target condition reached average	0.0
Share of undetected detectable attack actions	0.0093

Conclusions
Outlook

Current research challenges

- Simulation:
  - Cognitive and behavioral model
- Optimization:
  - Computational cost for individual portfolio evaluations
  - Uncertainty of simulation
  - Thorough testing of optimization algorithms (more alogrithms, performance measures across multiple runs, multiple problem instances etc.)

Ideas for future work

- Probabilistic dominance concepts?
- Assign replications non-uniformly?
- Control selection $\rightarrow$ system design (very large design space + constraints)

Q & A

Contact:
ekiesling@sba-research.org