

Simulation-based optimization of information security controls: An adversary-centric approach

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



December 9, 2013; Washington, DC



Agenda

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Major security management challenges

- ▶ **Growing complexity** of information systems
 - ▶ **Malicious threats** and targeted attacks
 - ▶ **Increasingly sophisticated** attacks that exploit
 - ▶ software vulnerabilities
 - ▶ network vulnerabilities
 - ▶ social vulnerabilities
 - ▶ insider knowledge and access
 - ▶ etc.
 - ▶ **Heterogeneous adversaries**
hacktivists, script kiddies, insiders, advanced persistent threats ...
- **Best way to cope with such risks?**

3 Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Core ideas

Security is. . .

- ▶ not the result of any particular technical measure
- ▶ a system property that emerges from **interactions**
- ▶ not an absolute concept, but involves **tradeoffs**
- ▶ meaningless without a specific **threat model**

“Best” solution is highly context-dependent, e.g.,

- ▶ system characteristics
- ▶ threat landscape
- ▶ available resources
- ▶ decision-makers’ risk preferences

4 Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Problem definition

Objective: choose an “optimal” set of security controls

Approach:

1. Model
 - a) abstract causal interdependencies
 - b) the information system and its context
 - c) adversaries and their behavior
2. Apply sets of security controls and simulate attacks
3. Optimize control sets w.r.t. multiple objectives
4. Support decision-maker in the selection of a control set

5 Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

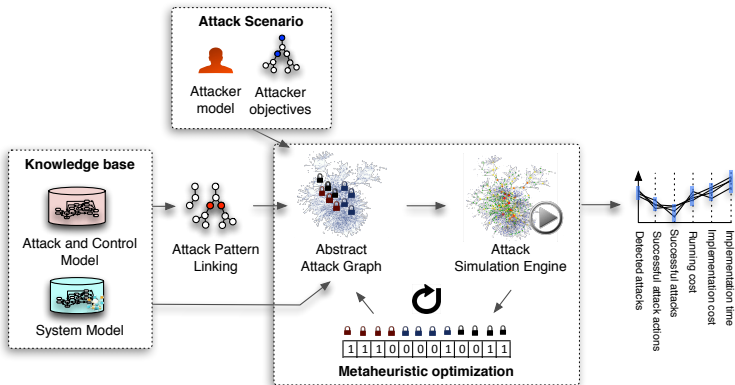
Experimental setup

Results

Conclusions

Appendix

Overview



Introduction

6

Framework

- Knowledge base
- Attack patterns
- Simulation
- Optimization
- Decision support

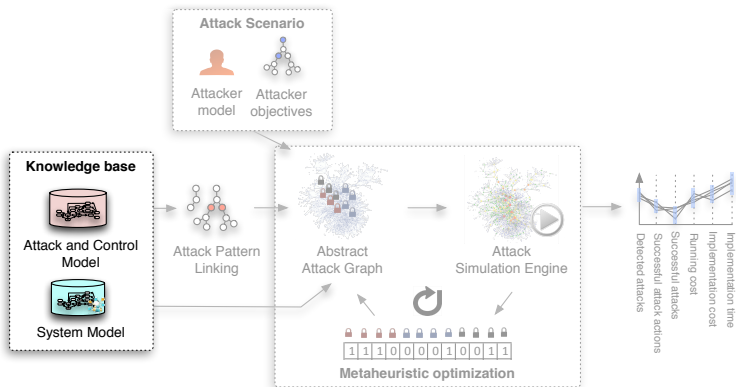
Example

- Experimental setup
- Results

Conclusions

Appendix

Knowledge base



Introduction

Framework

7

Knowledge base

- Attack patterns
- Simulation
- Optimization
- Decision support

Example

- Experimental setup
- Results

Conclusions

Appendix

Knowledge base



- ▶ Captures abstract attack knowledge
- ▶ Actions linked through pre- and post-conditions to form graph

Introduction

Framework

8

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

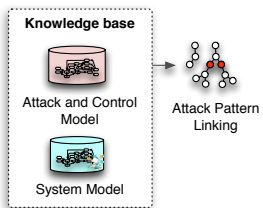
Experimental setup

Results

Conclusions

Appendix

Attack patterns



Introduction

Framework

Knowledge base

10 **Attack patterns**

Simulation

Optimization

Decision support

Example

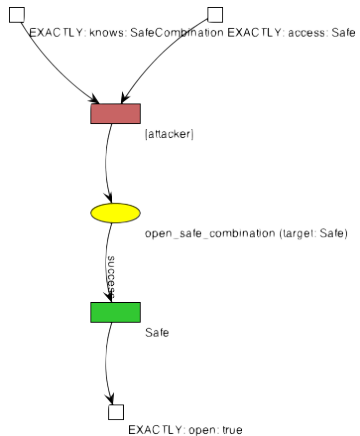
Experimental setup

Results

Conclusions

Appendix

Attack pattern linking



Introduction

Framework

Knowledge base

11 Attack patterns

Simulation

Optimization

Decision support

Example

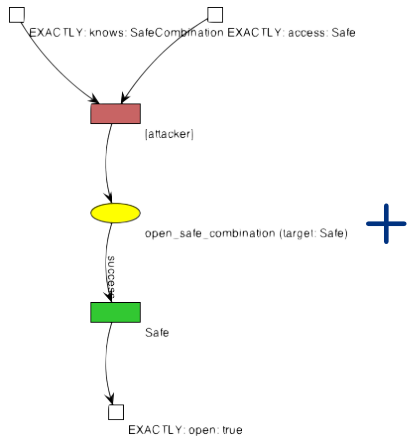
Experimental setup

Results

Conclusions

Appendix

Attack pattern linking



Introduction

Framework

Knowledge base

11 Attack patterns

Simulation

Optimization

Decision support

Example

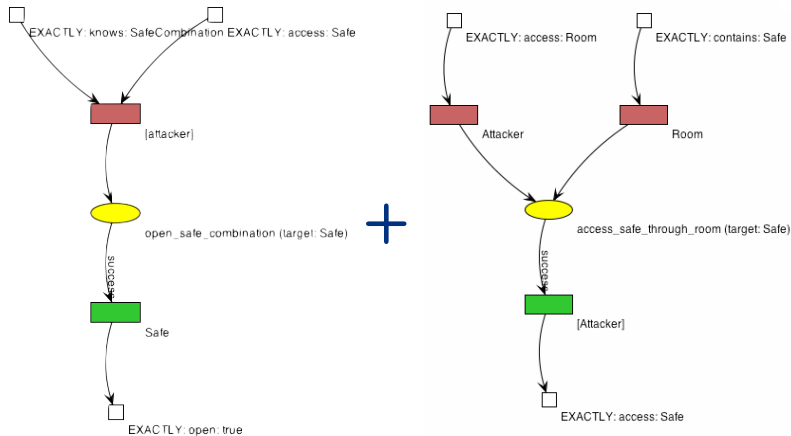
Experimental setup

Results

Conclusions

Appendix

Attack pattern linking



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

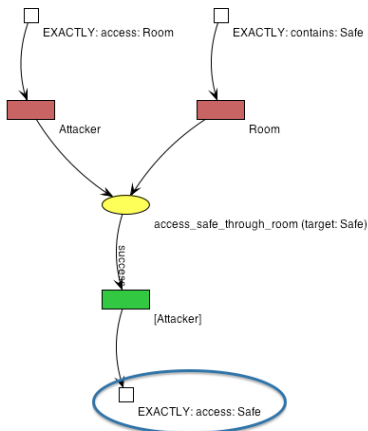
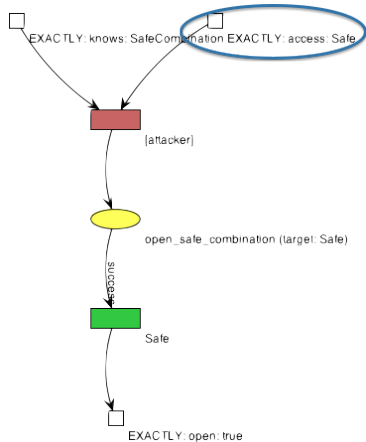
Conclusions

Appendix

11

46

Attack pattern linking



Introduction

Framework

- Knowledge base
- Attack patterns
- Simulation
- Optimization
- Decision support

Example

- Experimental setup
- Results

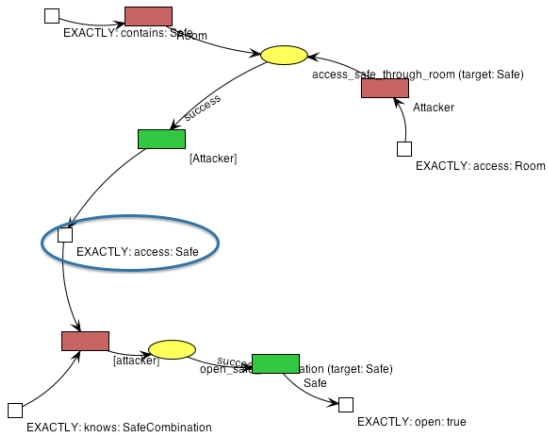
Conclusions

Appendix

11

46

Attack pattern linking



Introduction

Framework

Knowledge base

11

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

CAPEC [?]

- ▶ Publicly available list of common attack patterns
- ▶ 413 patterns described in varying levels of detail
- ▶ Not fully formalized (textual descriptions)

Transformation:

1. Generic CAPEC pattern → more specific actions
e.g., "134 Email Injection" → `emailKeylogger`, `emailBackdoor`
2. Single CAPEC pattern → sequential atomic actions
e.g., "49 Brute Forcing" → `bruteForce`, `accessHost`, `accessData`
3. Add additional actions
e.g., `accessData`, `accessHost`
4. Formalize
 - ▶ preconditions
 - ▶ postconditions
 - ▶ impact

Introduction

Framework

Knowledge base

12 Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

CAPEC example: Brute Force (1)

Brute Force 1		
Attack Pattern ID: 112 (Standard Attack Pattern Completeness: Complete)	Typical Severity: High	Status: Draft
Description		
Summary		
<p>In this attack, some asset (information, functionality, identity, etc.) is protected by a finite secret value. The attacker attempts to gain access to this asset by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset. Examples of secrets can include, but are not limited to, passwords, encryption keys, database lookup keys, and initial values to one-way functions.</p> <p>The key factor in this attack is the attacker's ability to explore the possible secret space rapidly. This, in turn, is a function of the size of the secret space and the computational power the attacker is able to bring to bear on the problem. If the attacker has modest resources and the secret space is large, the challenge facing the attacker is intractable. While the defender cannot control the resources available to an attacker, they can control the size of the secret space. Creating a large secret space involves selecting one's secret from as large a field of equally likely alternative secrets as possible and ensuring that an attacker is unable to reduce the size of this field using available clues or cryptoanalysis. Doing this is more difficult than it sounds since elimination of patterns (which, in turn, would provide an attacker clues that would help them reduce the space of potential secrets) is difficult to do using deterministic machines, such as computers. Assuming a finite secret space, a brute force attack will eventually succeed. The defender must rely on making sure that the time and resources necessary to do so will exceed the value of the information. For example, a secret space that will likely take hundreds of years to explore is likely safe from raw-brute force attacks.</p>		

Introduction

Framework

Knowledge base

13 Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

CAPEC example: Brute Force (2)

Attack Execution Flow

Explore

1. Determine secret testing procedure:

Determine how a potential guess of the secret may be tested. This may be accomplished by comparing some manipulation of the secret to a known value, use of the secret to manipulate some known set of data and determining if the result displays specific characteristics (for example, turning ciphertext into plaintext), or by submitting the secret to some external authority and having the external authority respond as to whether the value was the correct secret. Ideally, the attacker will want to determine the correctness of their guess independently since involvement of an external authority is usually slower and can provide an indication to the defender that a brute-force attack is being attempted.

Attack Step Techniques

ID	Attack Step Technique Description	Environments
1	Determine if there is a way to parallelize the attack. Most brute force attacks can take advantage of parallel techniques by dividing the search space among available resources, thus dividing the average time to success by the number of resources available. If there is a single choke point, such as a need to check answers with an external authority, the attacker's position is significantly degraded.	env-All

2. Reduce search space:

Find ways to reduce the secret space. The smaller the attacker can make the space they need to search for the secret value, the greater their chances for success. There are a great many ways in which the search space may be reduced.

Attack Step Techniques

ID	Attack Step Technique Description	Environments
1	If possible, determine how the secret was selected. If the secret was determined algorithmically (such as by a random number generator) the algorithm may have patterns or dependencies that reduce the size of the secret space. If the secret was created by a human, behavioral factors may, if not completely reduce the space, make some types of secrets more likely than others. (For example, humans may use the same secrets in multiple places or use secrets that look or sound familiar for ease of recall.)	env-All
2	If the secret was chosen algorithmically, cryptanalysis can be applied to the algorithm to discover patterns in this algorithm. (This is true even if the secret is not used in cryptography.) Periodicity, the need for seed values, or weaknesses in the generator all can result in a significantly smaller secret space.	env-All
3	If the secret was chosen by a person, social engineering and simple espionage can indicate patterns in their secret selection. If old secrets can be learned (and a target may feel they have little need to protect a secret that has been replaced) hints as to their selection preferences can be gleaned. These can include character substitutions a target employs, patterns in sources (dates, famous phrases, music lyrics, family members, etc.). Once these patterns have been determined, the initial efforts of a brute-force attack can focus on these areas.	env-All
4	Some algorithmic techniques for secret selection may leave indicators that can be tested for relatively easily and which could then be used to eliminate large areas of the search space for consideration. For example, it may be possible to determine that a secret does or does not start with a given character after a relatively small number of tests. Alternatively, it might be possible to discover the length of the secret relatively easily. These discoveries would significantly reduce the search space, thus increasing speed with which the attacker discovers the secret.	env-All

3. Expand victory conditions:

It is sometimes possible to expand victory conditions. For example, the attacker might not need to know the exact secret but simply needs a value that produces the same result using a one-way function. While doing this does not reduce the size of the search space, the presence of multiple victory conditions does reduce the likely amount of time that the attacker will need to explore the space before finding a workable value.

Exploit

1. Gather information so attack can be performed independently.:

If possible, gather the necessary information so a successful search can be determined without consultation of an external authority. This can be accomplished by capturing ciphertext (if the goal is decoding the text) or the encrypted password dictionary (if the goal is learning passwords).

Introduction

Framework

Knowledge base

13 Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

CAPEC example: Brute Force (3)

▼ Attack Prerequisites

The attacker must be able to determine when they have successfully guessed the secret. As such, one-time pads are immune to this type of attack since there is no way to determine when a guess is correct.

▼ Methods of Attack

- Brute Force

▼ Attacker Skills or Knowledge Required

Skill or Knowledge Level: Low

The attack simply requires basic scripting ability to automate the exploration of the search space. More sophisticated attackers may be able to use more advanced methods to reduce the search space and increase the speed with which the secret is located.

▼ Resources Required

Ultimately, the speed with which an attacker discovers a secret is directly proportional to the computational resources the attacker has at their disposal. This attack method is resource expensive: having large amounts of computational power do not guarantee timely success, but having only minimal resources makes the problem intractable against all but the weakest secret selection procedures.

▼ Indicators-Warnings of Attack

Description

Repeated submissions of incorrect secret values may indicate a brute force attack. For example, repeated bad passwords when accessing user accounts or repeated queries to databases using non-existent keys.

Description

Attempts to download files protected by secrets (usually using encryption) may be a precursor to an offline attack to break the file's encryption and read its contents. This is especially significant if the file itself contains other secret values, such as password files.

Description

If the attacker is able to perform the checking offline then there will likely be no indication that an attack is ongoing.

▼ Obfuscation Techniques

Description

The attack is impossible to detect if the attacker can test for successful discovery of the secret value independently, without needing to consult an external authority.

Description

If an external authority must be consulted, the attacker can attempt to space out their guesses to avoid a large number of failed guesses in a short period of time, but doing so slows the attack to the point of making it unworkable against all but the most trivial secret spaces. As such, if an external authority must be consulted the attacked is unlikely to be able to keep the attack secret.

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

13

46

CAPEC example: Brute Force (4)

▼ Solutions and Mitigations

Select a provably large secret space for selection of the secret. Provably large means that the procedure by which the secret is selected does not have artifacts that significantly reduce the size of the total secret space.

Do not provide the means for an attacker to determine success independently. This forces the attacker to check their guesses against an external authority, which can slow the attack and warn the defender. This mitigation may not be possible if testing material must appear externally, such as with a transmitted cryptotext.

▼ Attack Motivation-Consequences

Scope	Technical Impact	Note
Confidentiality	Read application data	
Confidentiality	Gain privileges / assume identity	
Access_Control		
Authorization		

▼ Related Weaknesses

CWE-ID	Weakness Name	Weakness Relationship Type
330	Use of Insufficiently Random Values	Secondary
326	Inadequate Encryption Strength	Secondary
521	Weak Password Requirements	Secondary

▼ Related Attack Patterns

Nature	Type	ID	Name	Description	W
ChildOf		223	Probabilistic Techniques		1000
HasMember		344	WASC Threat Classification 2.0 - WASC-11 - Brute Force		333
ParentOf		20	Encryption Brute Forcing		1000
ParentOf		49	Password Brute Forcing		1000

▼ Relevant Security Requirements

Protect sensitive data, even when the data is encrypted. If an attacker can gain access to encrypted data, they can mount a brute-force attack independently. The defender will not be aware of this attack or be able to do anything about it and at that point it is purely a function of the attacker's available resources as to how long it takes them to learn the secret.

Monitor activity logs for suspicious activity. An attacker that must use an external authority to check their brute-force guesses is easy to detect, but only if that external authority is monitoring activity and detects the abnormally large number of failed guesses.

▼ Related Guidelines

- Do not assume secrets will protect sensitive data in the long-term
- Monitor systems for suspicious activity.

▼ Purposes

- Penetration

Introduction

Framework

Knowledge base

13 Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Brute force: Prolog rule formulation

Preconditions

```
action_bruteForce(Attacker, TargetHost, TargetGroup):-
    technicalSkillLevel(Attacker, TechnicalSkillLevel),
    TechnicalSkillLevel >= 1,
    owned(Attacker, AttackHost),
    connected(AttackHost, TargetHost, rdpProtocol, rdpPort),
    accessHost(TargetGroup, TargetHost, _),
    not(inGroup(Attacker, TargetGroup)).
```

Postcondition

```
exec_success_action_bruteForce(Attacker, TargetHost, TargetGroup):-
    assert(inGroup(Attacker, TargetGroup)).
```

Impact

```
action_impact(action_bruteForce, confidentiality).
impact_success_bruteForce(Attacker, TargetHost, TargetGroup, SecurityAttribute, Impact):-
    importance(TargetGroup, SecurityAttribute, Impact).
```

Simulation attributes

```
/** cost, time, base probability, maxTries, simultaneous */
action_properties(action_bruteForce, 0, 18000, 0.01, 0, true).
available_action(action_bruteForce).
```

Introduction

Framework

Knowledge base

14 Attack patterns

Simulation

Optimization

Decision support

Example

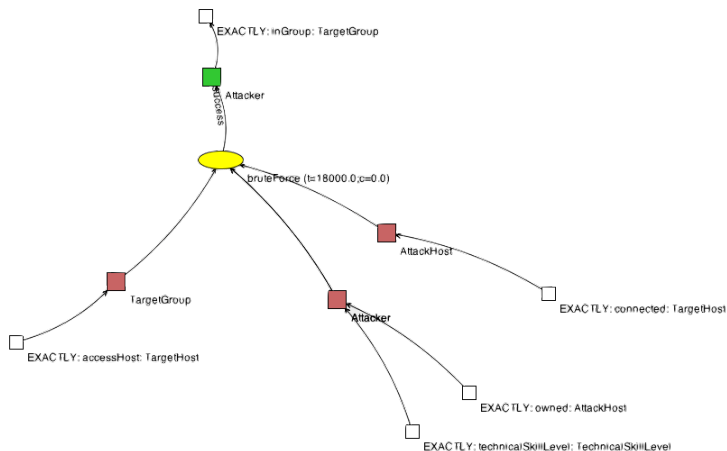
Experimental setup

Results

Conclusions

Appendix

Brute force: graph representation



Introduction

Framework

Knowledge base

15 **Attack patterns**

Simulation

Optimization

Decision support

Example

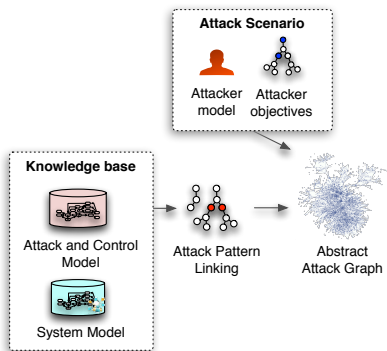
Experimental setup

Results

Conclusions

Appendix

Simulation



Introduction

Framework

Knowledge base
Attack patterns

16

Simulation

Optimization
Decision support

Example

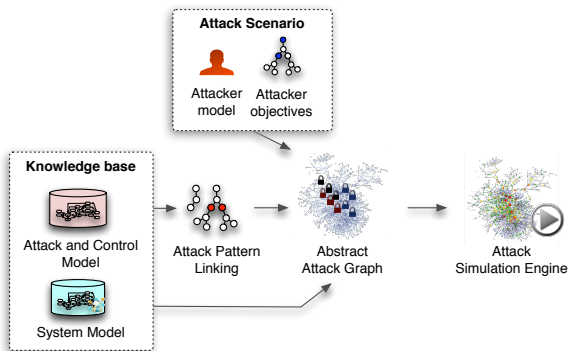
Experimental setup
Results

Conclusions

Appendix

46

Simulation



Introduction

Framework

Knowledge base
Attack patterns

16

Simulation

Optimization
Decision support

Example

Experimental setup
Results

Conclusions

Appendix

46

Discrete Event Scheduling



Introduction

Framework

Knowledge base

Attack patterns

17 **Simulation**

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

Appendix

Discrete Event Scheduling



Introduction

Framework

Knowledge base

Attack patterns

17

Simulation

Optimization

Decision support

Example

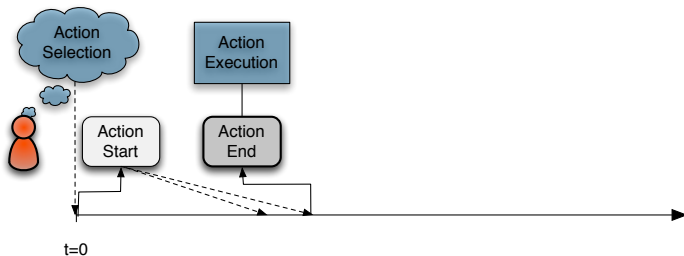
Experimental setup

Results

Conclusions

Appendix

Discrete Event Scheduling



Introduction

Framework

Knowledge base
Attack patterns

17

Simulation

Optimization
Decision support

Example

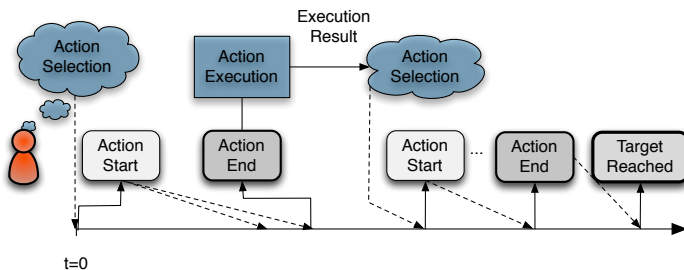
Experimental setup
Results

Conclusions

Appendix

46

Discrete Event Scheduling



Introduction

Framework

Knowledge base
Attack patterns

Simulation

Optimization
Decision support

Example

Experimental setup
Results

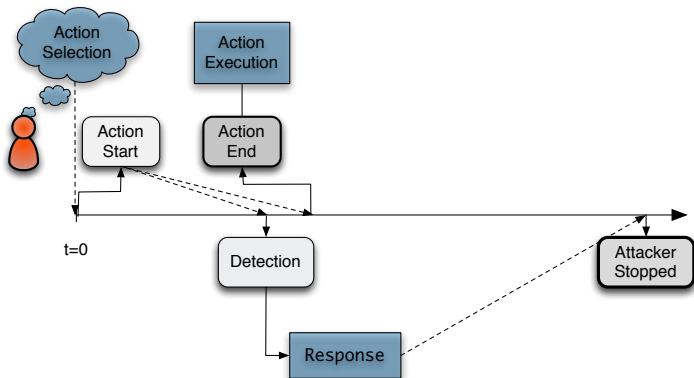
Conclusions

Appendix

17

46

Discrete Event Scheduling



Introduction

Framework

Knowledge base
Attack patterns

17

Simulation

Optimization
Decision support

Example

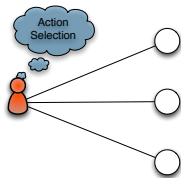
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

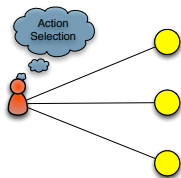
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

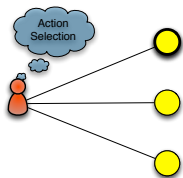
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base

Attack patterns

18

Simulation

Optimization

Decision support

Example

Experimental setup

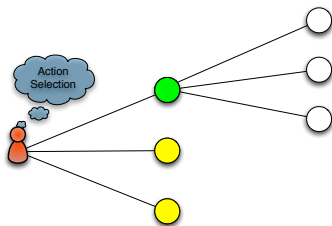
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

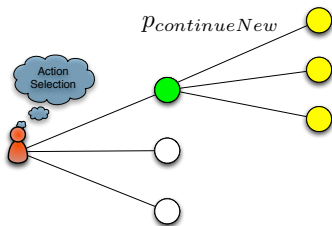
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

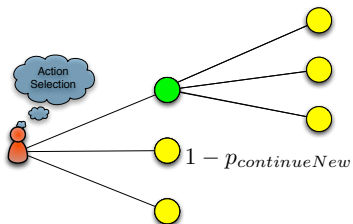
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

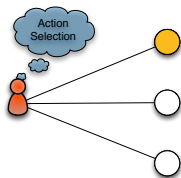
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

Example

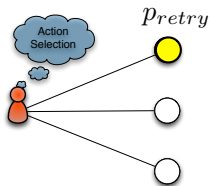
Experimental setup
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{rel} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{suc}(a)^{w_{suc}} \left(1 - p_{det}(a)\right)^{w_{det}} \left(1 - d_a^{rel}\right)^{w_{dist}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base

Attack patterns

18

Simulation

Optimization

Decision support

Example

Experimental setup

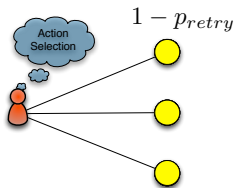
Results

Conclusions

Appendix

Behavioral model

Choice set:



Choice function: for all considered actions $a \in A$

1. Calculate distance in abstract graph:

$$d_a^{\text{rel}} \leftarrow \frac{d(a,t)}{\max(d(a,t))+1}$$

2. Calculate weight:

$$W_a \leftarrow p_{\text{suc}}(a)^{w_{\text{suc}}} \left(1 - p_{\text{det}}(a)\right)^{w_{\text{det}}} \left(1 - d_a^{\text{rel}}\right)^{w_{\text{dist}}}$$

3. **return** *weightedChoice*(A, W)

Introduction

Framework

Knowledge base
Attack patterns

18

Simulation

Optimization
Decision support

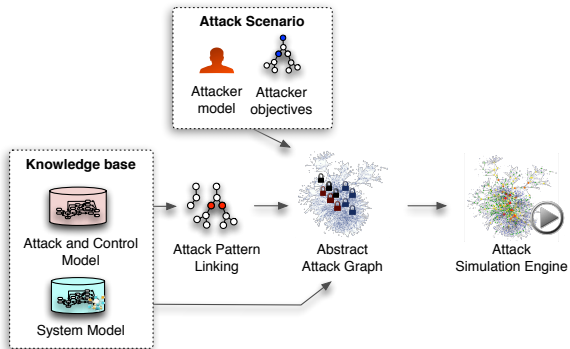
Example

Experimental setup
Results

Conclusions

Appendix

Optimization



Introduction

Framework

Knowledge base

Attack patterns

Simulation

19

Optimization

Decision support

Example

Experimental setup

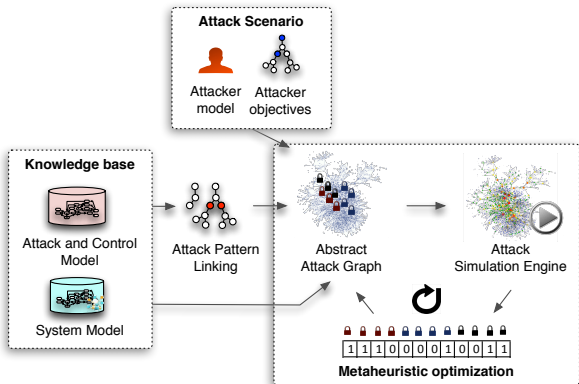
Results

Conclusions

Appendix

46

Optimization



Introduction

Framework

Knowledge base

Attack patterns

Simulation

19

Optimization

Decision support

Example

Experimental setup

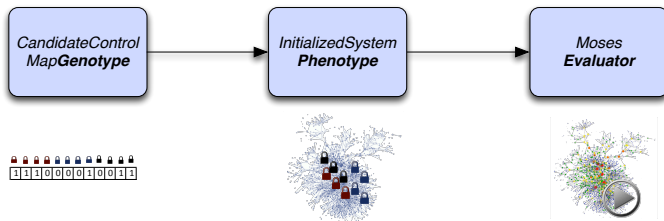
Results

Conclusions

Appendix

46

Evaluation of control portfolios



- ▶ Probabilistic → multiple replications per control set
- ▶ Currently reduced to a deterministic problem using expected/median/worst case values etc.

Introduction

Framework

Knowledge base

Attack patterns

Simulation

20

Optimization

Decision support

Example

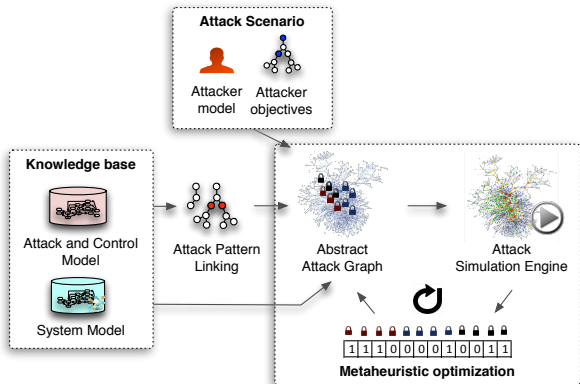
Experimental setup

Results

Conclusions

Appendix

Decision support



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

21 Decision support

Example

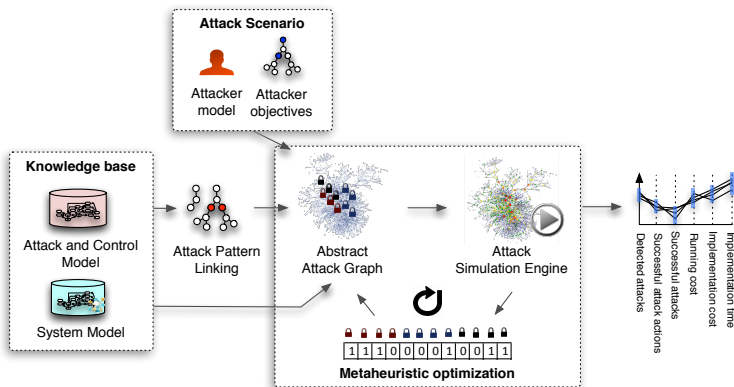
Experimental setup

Results

Conclusions

Appendix

Decision support



Introduction

Framework

Knowledge base
Attack patterns
Simulation
Optimization

21 Decision support

Example

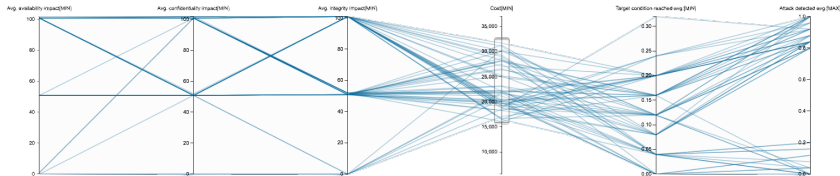
Experimental setup
Results

Conclusions

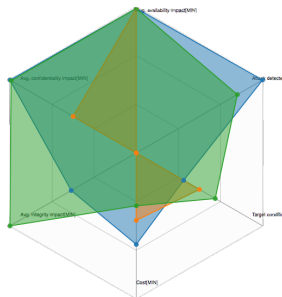
Appendix

Decision support

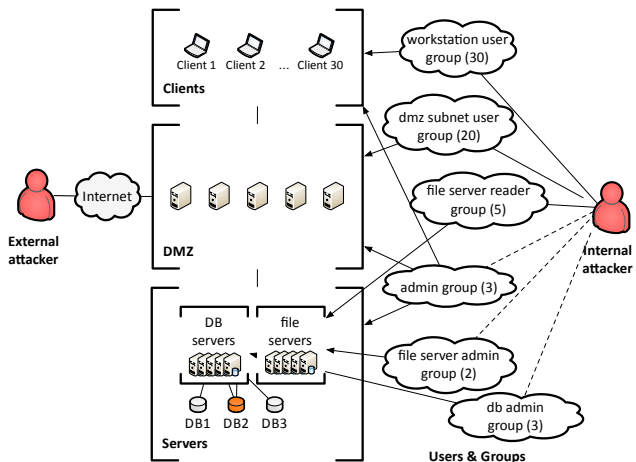
Iteration Number **90**



Iteration	evaluations	runtime(s)	Genotype	Avg. availab...	Avg. confide...	Avg. integ...	Cost(MN)	Target condi...	Attack detec...	id	<input type="checkbox"/>
90	2250	6648.466	0001001001...	101	51	0	17100.0	0.16	0.0	3	<input type="checkbox"/>
90	2250	6648.466	0001000000...	101	102	52	23200.0	0.12	1.0	5	<input type="checkbox"/>
90	2250	6648.466	0101000100...	101	101	101	31100.0	0.04	0.2	8	<input checked="" type="checkbox"/>
90	2250	6648.466	0101000000...	101	101	51	18300.0	0.08	0.8	12	<input checked="" type="checkbox"/>
90	2250	6648.466	0101000100...	101	51	101	27100.0	0.2	0.88	13	<input type="checkbox"/>
90	2250	6648.466	1000100000...	101	101	52	16100.0	0.2	0.84	14	<input checked="" type="checkbox"/>
90	2250	6648.466	0101000000...	51	51	51	19100.0	0.12	0.8	16	<input type="checkbox"/>
90	2250	6648.466	1010100000...	101	101	101	18800.0	0.32	0.92	18	<input type="checkbox"/>
90	2250	6648.466	0101000000...	51	51	51	28100.0	0.0	0.54	20	<input type="checkbox"/>
90	2250	6648.466	0101000100...	102	102	101	16500.0	0.04	0.16	21	<input type="checkbox"/>
90	2250	6648.466	1000001101...	101	101	52	21200.0	0.04	0.86	22	<input type="checkbox"/>



Scenario domain



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

23

Example

Experimental setup

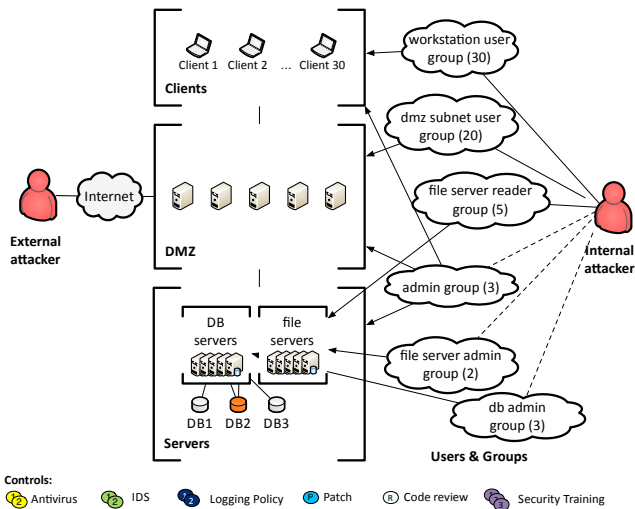
Results

Conclusions

Appendix

46

Scenario domain



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

23 Example

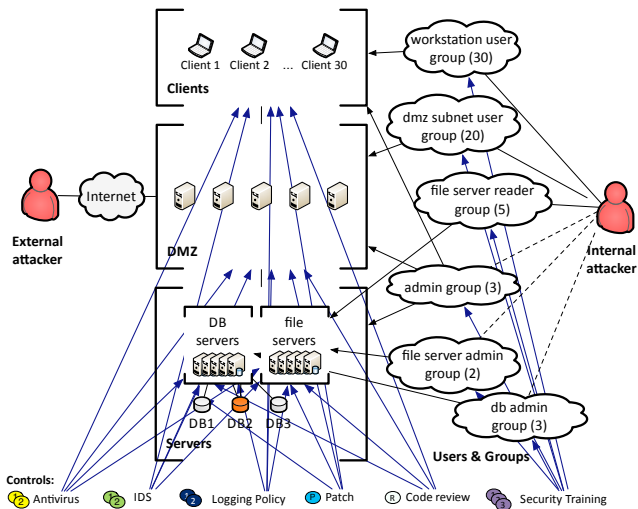
Experimental setup

Results

Conclusions

Appendix

Scenario domain



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

23

Example

Experimental setup

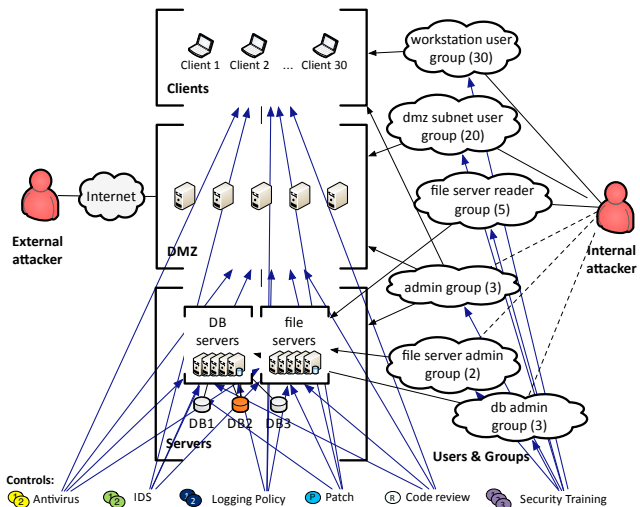
Results

Conclusions

Appendix

46

Scenario domain



58 binary decision variables (control-asset assignments)

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

23 Example

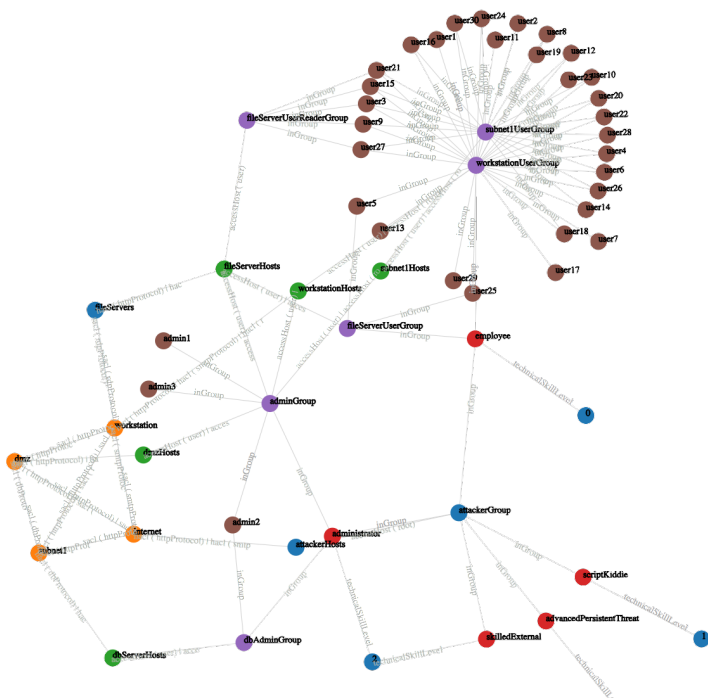
Experimental setup

Results

Conclusions

Appendix

46



Adversary types

Characteristics

	time (mins)	w_{det}	w_{suc}	w_{dist}	access
Employee	2500	0.45	0.25	0.30	workstations
Administrator	5000	0.50	0.20	0.30	all hosts
Skilled External	3333	0.30	0.40	0.30	-
Unskilled External	1667	0.30	0.40	0.30	-
APT	∞	0.50	0.20	0.30	-

Available actions (based on skill level, access)

Employee (skill: 0)	shoulderSurfing
Unskilled external (skill: 1)	spearfish
	sqlInjection
	socialAttack
	bruteForce
	emailKeylogger
	emailBackdoor
Skilled external (skill: 2)	+ bufferOverflow
	+ directoryTraversal
Admin (skill: 2)	(all above)
Advanced persistent threat (skill: 3)	+ zeroDay

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

25

Experimental setup

Results

Conclusions

Appendix

Optimization objectives

1. Minimize cost of controls
2. Minimize target condition achievement
3. Maximize detection of attacks
4. Minimize confidentiality impact (L/M/H)
5. Minimize integrity impact (L/M/H)
6. Minimize availability impact (L/M/H)

L/M/H: low, medium, high in lexicographic order

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

26 Experimental setup

Results

Conclusions

Appendix

Parameter settings

Simulation: 50 replications per control set

Optimization: 500 generations

▶ **Population**

- ▶ $\alpha = 100$ (population size)
- ▶ $\mu = 25$ (number of parents per generation)
- ▶ $\lambda = 25$ (number of offsprings per generation)
- ▶ Initialization: $\vec{1}, \vec{0}$, remaining random
(i.e., each control included with $p = 0.5$)

▶ **Selection:** NSGA2, 2 tournaments

▶ **Crossover:** 2-point crossover @ rate 0.95

▶ **Mutation:** mixed permutation (insert, revert, swap)
rate $1/n$

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

27 Experimental setup

Results

Conclusions

Appendix

Results

Runtime (3GHz Xeon, currently only single core used)
~ 90 mins (admin) – ~ 50 hrs (APT)

Proposed efficient solutions

- ▶ administrator: 2
- ▶ employee: 58
- ▶ unskilled external: 104
- ▶ skilled external: 306
- ▶ advanced persistent threat: 251

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

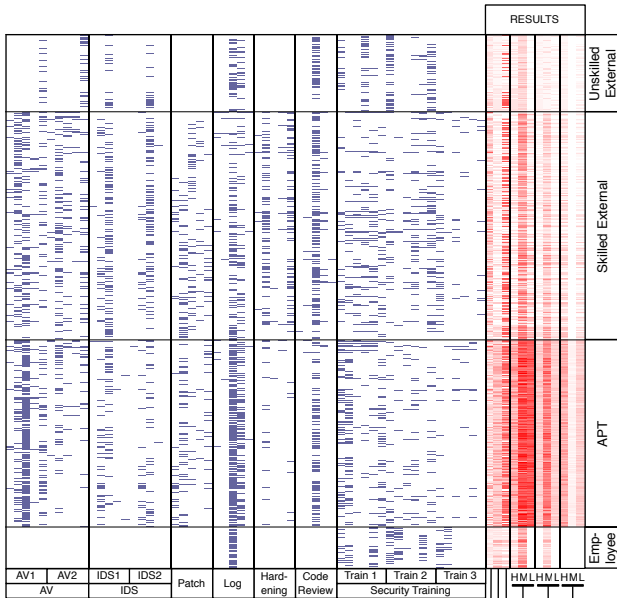
28

Results

Conclusions

Appendix

Results: Overview



Cost

Target condition reached

Detected attacks

Confidentiality impact

Integrity impact

Availability impact

HMLHMLHML

Administrator example attack trace



action_accessData

Target:
null

Asset mapping:
TargetHost: dbServerHosts
Data: db2

Results: Administrator

av1 on subnet1Hosts
av1 on empHosts
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on dbServerHosts
av2 on empHosts
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on empHosts
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on empHosts
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on workstationHosts
patchCVE_2013_04_22 on empHosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on empHosts
logPolicy1 on dbServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on empHosts
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on empHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on dbAdminGroup
securityTraining1 on subnet1UserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserGroup
securityTraining2 on adminGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on workstationUserGroup
securityTraining3 on fileServerUserReaderGroup
securityTraining3 on workstationUserGroup

Cost
Target condition not used
Deleted status
Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Results: Administrator

av1 on subnet1Hosts
av1 on empHots
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on empHots
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on empHots
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on empHots
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on workstationHosts
patchCVE_2013_04_22 on empHots
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on empHots
logPolicy1 on dbServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on empHots
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on empHots
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on dbAdminGroup
securityTraining1 on subnet1UserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserReaderGroup
securityTraining2 on adminGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on fileServerUserReaderGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on fileServerUserReaderGroup
securityTraining3 on workstationUserGroup

Target condition reached
Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Target condition always reached

Results: Administrator

Single high confidentiality impact

av1 on subnet1Hosts
av1 on empHosts
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on empHosts
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on empHosts
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on empHosts
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on empHosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on empHosts
logPolicy1 on dbServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on empHosts
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on empHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on dbAdminGroup
securityTraining1 on subnet1UserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserReaderGroup
securityTraining2 on adminGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on fileServerUserReaderGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on fileServerUserReaderGroup
securityTraining3 on workstationUserGroup
Cost

Target condition reached

Confidentiality high

Confidentiality low

Integrity high

Integrity medium

Integrity low

Availability high

Availability medium

Availability low

Results: Administrator

av1 on subnet1Hosts
av1 on empHosts
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on empHosts
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on empHosts
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on empHosts
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on empHosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on subnet1Hosts
logPolicy1 on dbServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on empHosts
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on empHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on dbAdminGroup
securityTraining1 on subnet1UserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserGroup
securityTraining2 on adminGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on workstationUserGroup
securityTrainings on workstationUserGroup

Cost

Detected attacks

Confidentiality medium
Integrity medium
Availability low
Confidentiality low
Integrity medium
Availability high
Confidentiality low
Integrity low
Availability high
Confidentiality medium
Integrity medium
Availability low

Log policy improves detection

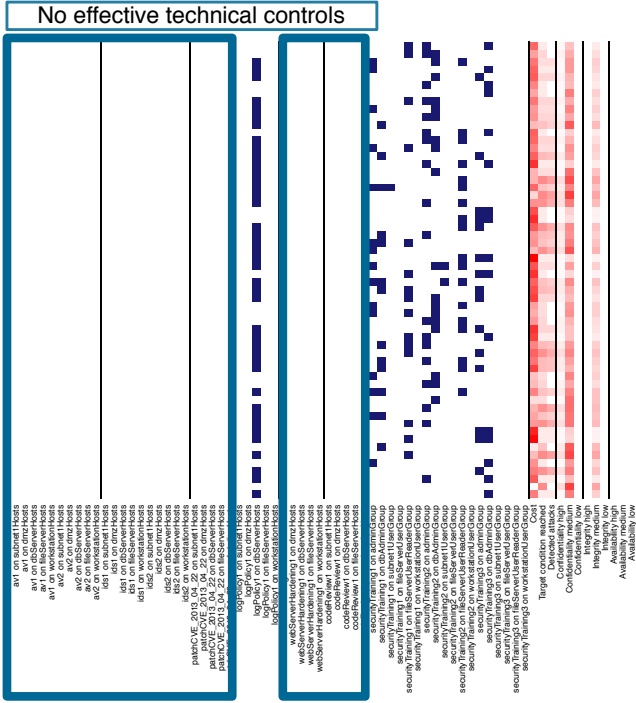
Employee example attack trace



Results: Employee

av1 on subnet11Hosts	
av1 on dsServerHosts	
av1 on dsServerHosts	
av1 on fileServerHosts	
av1 on workstationHosts	
av2 on subnet11Hosts	
av2 on dsServerHosts	
av2 on dsServerHosts	
av2 on fileServerHosts	
av2 on workstationHosts	
ids1 on subnet11Hosts	
ids1 on dsServerHosts	
ids1 on dsServerHosts	
ids1 on fileServerHosts	
ids1 on workstationHosts	
ids2 on subnet11Hosts	
ids2 on dsServerHosts	
ids2 on dsServerHosts	
ids2 on fileServerHosts	
ids2 on workstationHosts	
patchCVE_2013_04_22 on subnet11Hosts	
patchCVE_2013_04_22 on dsServerHosts	
patchCVE_2013_04_22 on dsServerHosts	
patchCVE_2013_04_22 on fileServerHosts	
patchCVE_2013_04_22 on workstationHosts	
logPolicy1 on dsServerHosts	
logPolicy1 on dsServerHosts	
logPolicy1 on dsServerHosts	
logPolicy1 on fileServerHosts	
logPolicy1 on workstationHosts	
webServerHardening1 on dsServerHosts	
webServerHardening1 on dsServerHosts	
webServerHardening1 on dsServerHosts	
webServerHardening1 on fileServerHosts	
webServerHardening1 on workstationHosts	
codeReview1 on dsServerHosts	
codeReview1 on dsServerHosts	
codeReview1 on dsServerHosts	
codeReview1 on fileServerHosts	
codeReview1 on workstationHosts	
securityTraining1 on adminGroup	
securityTraining1 on adminGroup	
securityTraining1 on adminGroup	
securityTraining1 on subnet1UserGroup	
securityTraining1 on fileServerUserGroup	
securityTraining1 on fileServerUserGroup	
securityTraining2 on adminGroup	
securityTraining2 on adminGroup	
securityTraining2 on adminGroup	
securityTraining2 on subnet1UserGroup	
securityTraining2 on fileServerUserGroup	
securityTraining2 on fileServerUserGroup	
securityTraining3 on adminGroup	
securityTraining3 on adminGroup	
securityTraining3 on adminGroup	
securityTraining3 on subnet1UserGroup	
securityTraining3 on fileServerUserGroup	
securityTraining3 on fileServerUserGroup	
securityTraining3 on workstationUserGroup	
securityTraining3 on workstationUserGroup	
Target condition was detected	
Detected attacks	
Confidentiality high	
Confidentiality medium	
Confidentiality low	
Integrity high	
Integrity medium	
Integrity low	
Availability high	
Availability medium	
Availability low	

Results: Employee



Results: Employee

Security trainings are effective

av1 on subnet11Hosts	
av1 on dsServerHosts	
av1 on fileServerHosts	
av1 on workstationHosts	
av2 on subnet11Hosts	
av2 on dsServerHosts	
av2 on fileServerHosts	
av2 on workstationHosts	
ids1 on subnet11Hosts	
ids1 on dsServerHosts	
ids1 on fileServerHosts	
ids1 on workstationHosts	
ids2 on subnet11Hosts	
ids2 on dsServerHosts	
ids2 on fileServerHosts	
ids2 on workstationHosts	
patchCVE_2013_04_22 on subnet11Hosts	
patchCVE_2013_04_22 on dsServerHosts	
patchCVE_2013_04_22 on fileServerHosts	
patchCVE_2013_04_22 on workstationHosts	
logPolicy1 on dirzHosts	
logPolicy1 on dsServerHosts	
logPolicy1 on fileServerHosts	
logPolicy1 on workstationHosts	
webServerHardening1 on dirzHosts	
webServerHardening1 on dsServerHosts	
webServerHardening1 on fileServerHosts	
webServerHardening1 on workstationHosts	
codeReview1 on dirzHosts	
codeReview1 on dsServerHosts	
codeReview1 on fileServerHosts	
codeReview1 on workstationHosts	
securityTraining1 on adminGroup	
securityTraining1 on subnet1UserGroup	
securityTraining1 on fileServerUserGroup	
securityTraining1 on dsServerUserGroup	
securityTraining2 on adminGroup	
securityTraining2 on adminGroup	
securityTraining2 on subnet1UserGroup	
securityTraining2 on fileServerUserGroup	
securityTraining2 on dsServerUserGroup	
securityTraining3 on adminGroup	
securityTraining3 on adminGroup	
securityTraining3 on subnet1UserGroup	
securityTraining3 on fileServerUserGroup	
securityTraining3 on dsServerUserGroup	
Cost	
Target condition was	
Detected attacks	
Confidentiality high	
Confidentiality medium	
Confidentiality low	
Integrity high	
Integrity medium	
Integrity low	
Availability high	
Availability medium	
Availability low	

Results: Employee

Success rate can be reduced from 46% to 6%

av1 on subnet11Hosts
av1 on dsServerHosts
av1 on dsServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on subnet11Hosts
av2 on dsServerHosts
av2 on dsServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on subnet11Hosts
ids1 on dsServerHosts
ids1 on dsServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on subnet11Hosts
ids2 on dsServerHosts
ids2 on dsServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on subnet11Hosts
patchCVE_2013_04_22 on dsServerHosts
patchCVE_2013_04_22 on dsServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on dsServerHosts
logPolicy1 on dsServerHosts
logPolicy1 on dsServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on dsServerHosts
webServerHardening1 on dsServerHosts
webServerHardening1 on dsServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on dsServerHosts
codeReview1 on dsServerHosts
codeReview1 on dsServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on adminGroup
securityTraining1 on adminGroup
securityTraining1 on subnet1UserGroup
securityTraining1 on fileServerReaderGroup
securityTraining1 on fileServerReaderGroup
securityTraining2 on adminGroup
securityTraining2 on adminGroup
securityTraining2 on adminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerReaderGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on adminGroup
securityTraining3 on fileServerReaderGroup
securityTraining3 on fileServerReaderGroup
securityTraining3 on workstationUserGroup
securityTraining3 on workstationUserGroup

Target condition reached

Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Results: Employee

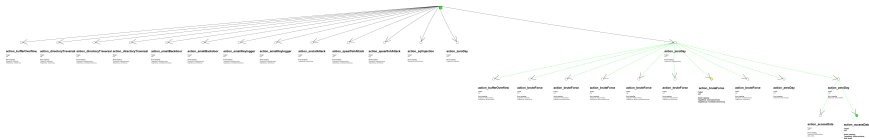
Log policy can increase detection rate to ~ 1/3

```
av1 on subnet11Hosts
av1 on subnet11Hosts
av1 on dbServerHosts
av1 on fileServerHosts
av2 on workstationHosts
av2 on subnet11Hosts
av2 on dbServerHosts
av2 on fileServerHosts
id1 on workstationHosts
id1 on subnet11Hosts
id1 on dbServerHosts
id1 on fileServerHosts
id2 on workstationHosts
id2 on subnet11Hosts
id2 on dbServerHosts
id2 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
patchCVE_2013_04_22 on subnet11Hosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
logPolicy1 on subnet11Hosts
logPolicy1 on dbServerHosts
logPolicy1 on workstationHosts
logPolicy1 on fileServerHosts
webServerHardening1 on dirzHosts
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on dirzHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on adminGroup
securityTraining1 on subset1UserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerReaderGroup
securityTraining2 on adminGroup
securityTraining2 on subset1UserGroup
securityTraining2 on subset2UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on fileServerReaderGroup
securityTraining3 on adminGroup
securityTraining3 on subset1UserGroup
securityTraining3 on subset2UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on fileServerReaderGroup
Cost
```

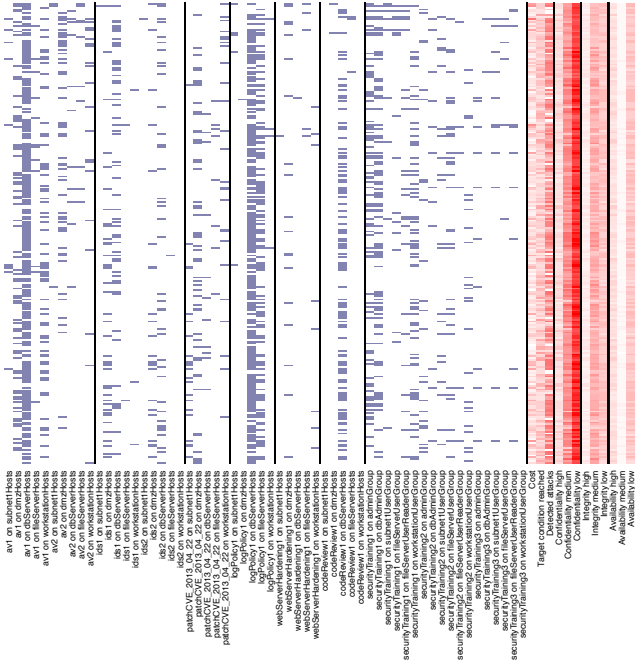
Detected attacks

Confidentiality	medium
Comidentiality	low
Integrity	medium
Integrity	low
Availability	high
Availability	medium
Availability	low

APT example attack trace



Results: Advanced persistent threat



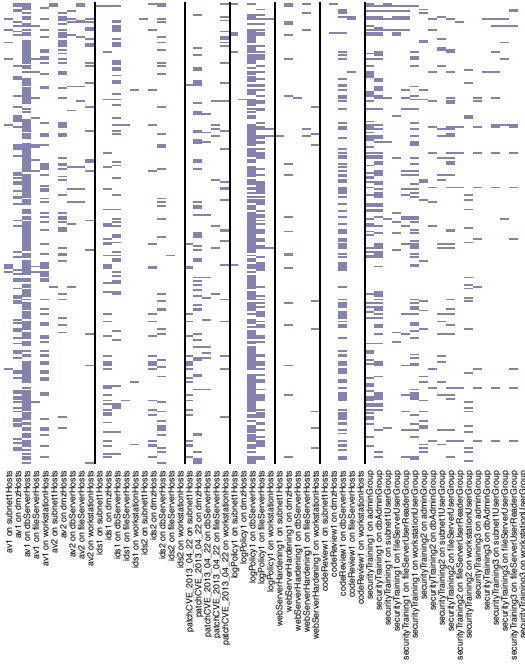
Results: Advanced persistent threat

Wide range of effective controls

av1 on subnet1-hoists
av1 on dmz-hoists
av1 on db-Serverhoists
av1 on subnets-hoists
av1 on workstation-hoists
av2 on subnet1-hoists
av2 on dmz-hoists
av2 on db-Serverhoists
av2 on subnets-hoists
av2 c workstation-hoists
ids1 on subnet1-hoists
ids1 on dmz-hoists
ids1 on db-Serverhoists
ids1 on subnets-hoists
ids1 on workstation-hoists
ids2 on subnet1-hoists
ids2 on dmz-hoists
ids2 on db-Serverhoists
ids2 on subnets-hoists
ids2 c workstation-hoists
patchCVE_2013_04_22 on subnet1-hoists
patchCVE_2013_04_22 on dmz-hoists
patchCVE_2013_04_22 on db-Serverhoists
patchCVE_2013_04_22 on subnets-hoists
patchCVE_2013_04_22 on workstation-hoists
logPolicy1 on subnet1-hoists
logPolicy1 on dmz-hoists
logPolicy1 on db-Serverhoists
logPolicy1 on subnets-hoists
logPolicy1 c workstation-hoists
webServerHardening1 on subnet1-hoists
webServerHardening1 on dmz-hoists
webServerHardening1 on db-Serverhoists
webServerHardening1 on subnets-hoists
webServerHardening1 c workstation-hoists
codeReview1 on subnet1-hoists
codeReview1 on dmz-hoists
codeReview1 on db-Serverhoists
codeReview1 on subnets-hoists
codeReview1 c workstation-hoists
securityTraining1 on adminGroup
securityTraining1 on dbAdminGroup
securityTraining1 on subnetUserGroup
securityTraining1 on dbServerReaderGroup
securityTraining1 on workstationUserGroup
securityTraining1 on fileServerUserGroup
securityTraining2 on adminGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnetUserGroup
securityTraining2 on dbServerReaderGroup
securityTraining2 on workstationUserGroup
securityTraining2 on fileServerUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnetUserGroup
securityTraining3 on fileServerReaderGroup

Target condition reached
Derecord attach
Confidentiality high
Confidentiality medium
Confidentiality low
Integrity low
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Results: Advanced persistent threat



Target condition reached

Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

High success rate (> 2/3)

Results: Advanced persistent threat

IDS and log policies can raise detection rates to ~ 2/3

```
av1 on subnet1-ho5ts
av1 on omzho5ts
av1 on dsServerho5ts
av1 on dsServerho5ts
av1 on workstationho5ts
av2 on subnet1-ho5ts
av2 on omzho5ts
av2 on dsServerho5ts
av2 on dsServerho5ts
av2 on workstationho5ts
ias1 on omzho5ts
ias1 on dsServerho5ts
ias1 on dsServerho5ts
ias1 on workstationho5ts
ias2 on omzho5ts
ias2 on dsServerho5ts
ias2 on dsServerho5ts
ias2 on workstationho5ts

patchCVE_2013_04_22 on omzho5ts
patchCVE_2013_04_22 on dsServerho5ts
patchCVE_2013_04_22 on dsServerho5ts
patchCVE_2013_04_22 on fileServerho5ts

logpolicy1 on subnet1-ho5ts
logpolicy1 on omzho5ts
logpolicy1 on dsServerho5ts
logpolicy1 on dsServerho5ts
logpolicy1 on workstationho5ts

webServerHardening1 on omzho5ts
webServerHardening1 on dsServerho5ts
webServerHardening1 on dsServerho5ts
webServerHardening1 on workstationho5ts

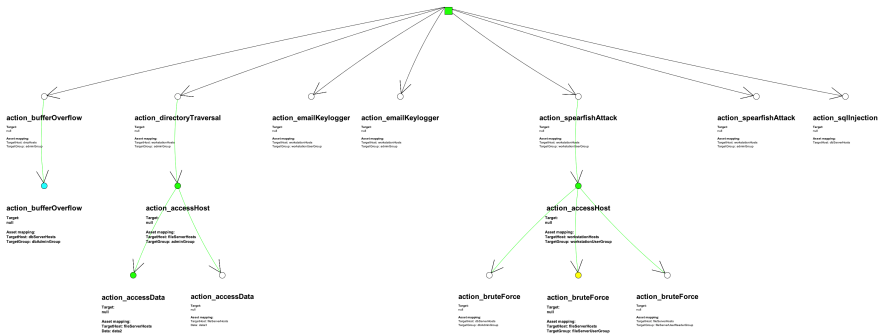
codeReview1 on subnet1-ho5ts
codeReview1 on omzho5ts
codeReview1 on dsServerho5ts
codeReview1 on dsServerho5ts
codeReview1 on workstationho5ts

securityTraining1 on adminGroup
securityTraining1 on adminGroup
securityTraining1 on subnetUserGroup
securityTraining1 on subnetUserGroup
securityTraining1 on fileServerReaderUserGroup
securityTraining1 on fileServerReaderUserGroup
securityTraining1 on workstationUserGroup
securityTraining1 on workstationUserGroup
securityTraining2 on adminGroup
securityTraining2 on adminGroup
securityTraining2 on fileServerReaderUserGroup
securityTraining2 on fileServerReaderUserGroup
securityTraining2 on workstationUserGroup
securityTraining2 on workstationUserGroup
securityTraining3 on subnetUserGroup
securityTraining3 on subnetUserGroup
securityTraining3 on fileServerReaderUserGroup
securityTraining3 on fileServerReaderUserGroup
securityTraining3 on workstationUserGroup
securityTraining3 on workstationUserGroup
Cost
```

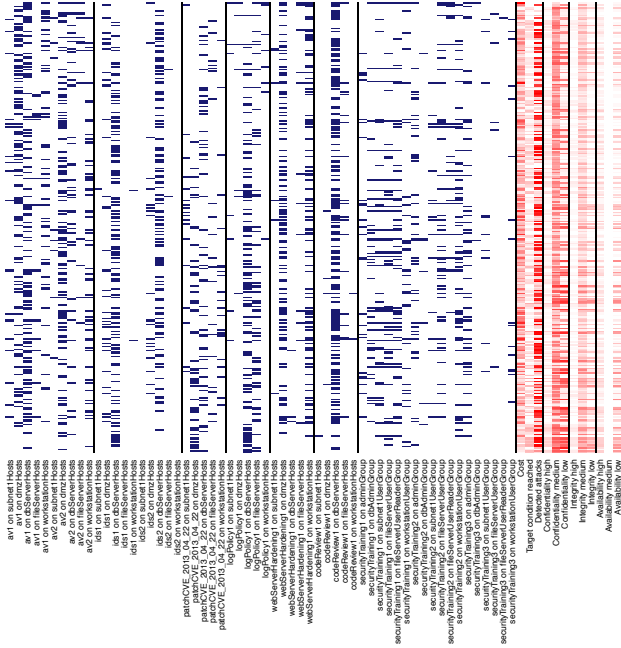
Target condition reached

Confidentiality	high
Confidentiality	low
Integrity	high
Integrity	medium
Integrity	low
Availability	high
Availability	medium
Availability	low

Skilled external example attack trace



Results: Skilled external

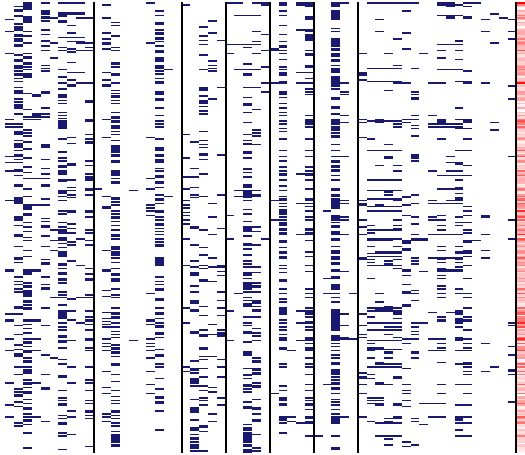


Results: Skilled external

av1 on subnet1Hosts
av1 on dmzHosts
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on dmzHosts
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on subnet1Hosts
ids1 on dmzHosts
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on subnet1Hosts
ids2 on dmzHosts
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on subnet1Hosts
patchCVE_2013_04_22 on dmzHosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on subnet1Hosts
logPolicy1 on dmzHosts
logPolicy1 on dbServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on dmzHosts
webServerHardening1 on subnet1Hosts
webServerHardening1 on dbServerHosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on subnet1Hosts
codeReview1 on dmzHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on adminGroup
securityTraining1 on dbAdminGroup
securityTraining1 on userGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserHeaderGroup
securityTraining1 on workstationUserGroup
securityTraining2 on dbAdminGroup
securityTraining2 on adminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on fileServerUserHeaderGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserHeaderGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on workstationUserGroup
Cost

Target condition reached
Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Lower impact



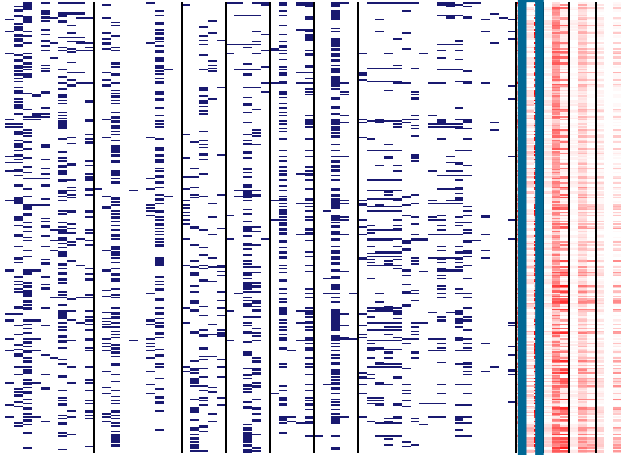
Results: Skilled external

av1 on subnet1Hosts
av1 on dmzHosts
av1 on dbServerHosts
av1 on fileServerHosts
av1 on workstationHosts
av2 on dmzHosts
av2 on dbServerHosts
av2 on fileServerHosts
av2 on workstationHosts
ids1 on dmzHosts
ids1 on dbServerHosts
ids1 on fileServerHosts
ids1 on workstationHosts
ids2 on dmzHosts
ids2 on dbServerHosts
ids2 on fileServerHosts
ids2 on workstationHosts
patchCVE_2013_04_22 on subnet1Hosts
patchCVE_2013_04_22 on dmzHosts
patchCVE_2013_04_22 on dbServerHosts
patchCVE_2013_04_22 on fileServerHosts
patchCVE_2013_04_22 on workstationHosts
logPolicy1 on subnet1Hosts
logPolicy1 on dmzHosts
logPolicy1 on dbServerHosts
logPolicy1 on fileServerHosts
logPolicy1 on workstationHosts
webServerHardening1 on dmzHosts
webServerHardening1 on subnet1Hosts
webServerHardening1 on fileServerHosts
webServerHardening1 on workstationHosts
codeReview1 on subnet1Hosts
codeReview1 on dmzHosts
codeReview1 on dbServerHosts
codeReview1 on fileServerHosts
codeReview1 on workstationHosts
securityTraining1 on adminGroup
securityTraining1 on dbAdminGroup
securityTraining1 on dbUserGroup
securityTraining1 on fileServerUserGroup
securityTraining1 on fileServerUserHeaderGroup
securityTraining1 on workstationUserGroup
securityTraining2 on dbAdminGroup
securityTraining2 on subnet1UserGroup
securityTraining2 on fileServerUserGroup
securityTraining2 on fileServerUserHeaderGroup
securityTraining2 on workstationUserGroup
securityTraining3 on adminGroup
securityTraining3 on dbAdminGroup
securityTraining3 on subnet1UserGroup
securityTraining3 on fileServerUserGroup
securityTraining3 on fileServerUserHeaderGroup
securityTraining3 on workstationUserGroup
securityTraining3 on workstationUserHeaderGroup

target condition reached

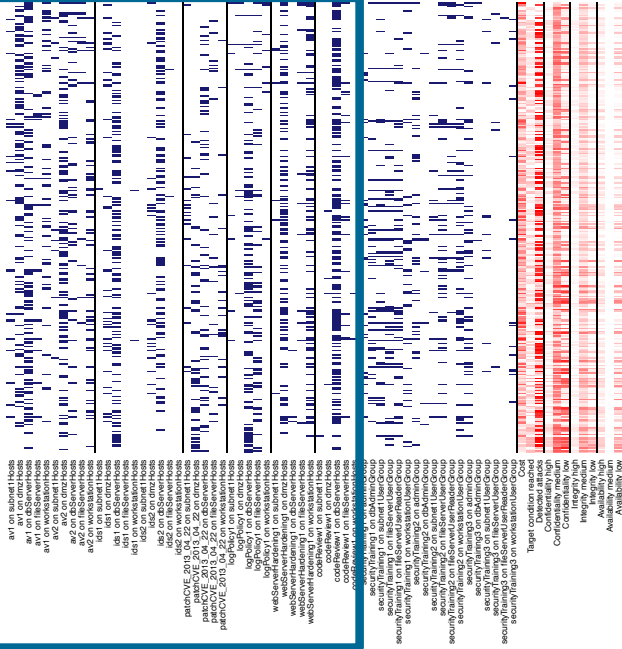
Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Lower success probability

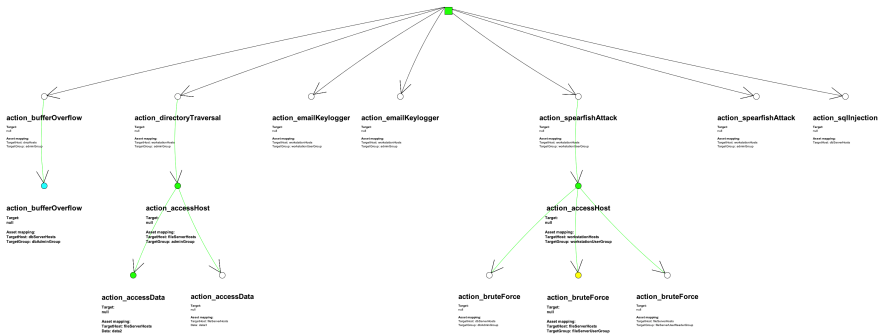


Results: Skilled external

More effective technical controls



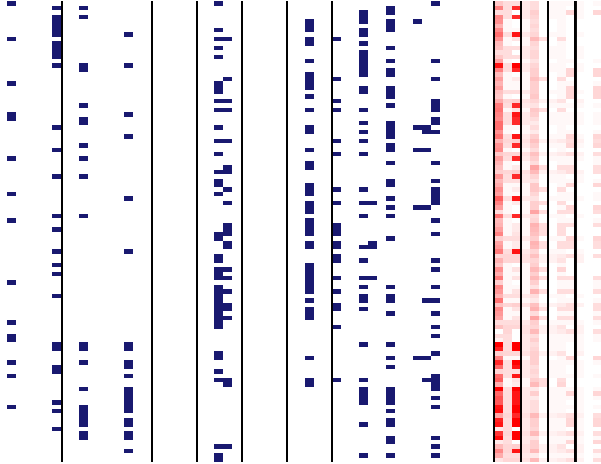
Unskilled external example attack trace



Results: Unskilled external

av1 on subnet1/Hosts
av1 on crmz/Hosts
av1 on dbServer/Hosts
av1 on dbServer/Hosts
av1 on workstation/Hosts
av2 on subnet1/Hosts
av2 on crmz/Hosts
av2 on dbServer/Hosts
av2 on dbServer/Hosts
av2 on workstation/Hosts
ids1 on subnet1/Hosts
ids1 on crmz/Hosts
ids1 on dbServer/Hosts
ids1 on dbServer/Hosts
ids1 on workstation/Hosts
ids2 on subnet1/Hosts
ids2 on crmz/Hosts
ids2 on dbServer/Hosts
ids2 on dbServer/Hosts
ids2 on workstation/Hosts
patchCVE_2013_04_22 on subnet1/Hosts
patchCVE_2013_04_22 on crmz/Hosts
patchCVE_2013_04_22 on dbServer/Hosts
patchCVE_2013_04_22 on dbServer/Hosts
patchCVE_2013_04_22 on workstation/Hosts
logPolicy1 on subnet1/Hosts
logPolicy1 on crmz/Hosts
logPolicy1 on dbServer/Hosts
logPolicy1 on dbServer/Hosts
logPolicy1 on workstation/Hosts
webServerHardening1 on subnet1/Hosts
webServerHardening1 on crmz/Hosts
webServerHardening1 on dbServer/Hosts
webServerHardening1 on dbServer/Hosts
webServerHardening1 on workstation/Hosts
codeReview1 on subnet1/Hosts
codeReview1 on crmz/Hosts
codeReview1 on dbServer/Hosts
codeReview1 on dbServer/Hosts
codeReview1 on workstation/Hosts
securityTraining1 on admin/Group
securityTraining1 on subnet1/User/Group
securityTraining1 on subnet1/User/Group
securityTraining1 on workstation/User/Group
securityTraining1 on workstation/User/Group
securityTraining2 on admin/Group
securityTraining2 on dbAdmin/Group
securityTraining2 on subnet1/User/Group
securityTraining2 on fileServer/User/Group
securityTraining2 on workstation/User/Group
securityTraining3 on admin/Group
securityTraining3 on subnet1/User/Group
securityTraining3 on fileServer/User/Group
securityTraining3 on workstation/User/Group

Target condition success
Detected attacks
Confidentiality high
Confidentiality medium
Confidentiality low
Confidentiality very low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low



Results: Unskilled external

Fewer technical controls

av1 on subnet1/Hosts
av1 on crmz/Hosts
av1 on dbServer/Hosts
av1 on erp/Hosts
av1 on workstation/Hosts
av2 on subnet1/Hosts
av2 on crmz/Hosts
av2 on dbServer/Hosts
av2 on erp/Hosts
av2 on workstation/Hosts
ids1 on subnet1/Hosts
ids1 on crmz/Hosts
ids1 on dbServer/Hosts
ids1 on erp/Hosts
ids1 on workstation/Hosts
ids2 on subnet1/Hosts
ids2 on crmz/Hosts
ids2 on dbServer/Hosts
ids2 on erp/Hosts
ids2 on workstation/Hosts
logPolicy1 on crmz/Hosts
logPolicy1 on dbServer/Hosts
logPolicy1 on erp/Hosts
logPolicy1 on workstation/Hosts
webServerHardening1 on subnet1/Hosts
webServerHardening1 on dbServer/Hosts
webServerHardening1 on erp/Hosts
webServerHardening1 on workstation/Hosts
codeReview1 on subnet1/Hosts
codeReview1 on crmz/Hosts
codeReview1 on dbServer/Hosts
codeReview1 on erp/Hosts
codeReview1 on workstation/Hosts
securityTraining1 on admin/Group
securityTraining1 on subnet1/UserGroup
securityTraining1 on workstation/UserGroup
securityTraining1 on fileServer/UserGroup
securityTraining1 on fileServerAdmin/Group
securityTraining2 on admin/Group
securityTraining2 on crmz/Group
securityTraining2 on dbServer/Group
securityTraining2 on fileServer/UserGroup
securityTraining2 on fileServerAdmin/Group
securityTraining2 on workstation/UserGroup
securityTraining3 on admin/Group
securityTraining3 on crmz/Group
securityTraining3 on dbServer/UserGroup
securityTraining3 on fileServer/UserGroup
securityTraining3 on fileServerAdmin/Group
securityTraining3 on workstation/UserGroup

Target condition reached

Detected attacks

Confidentiality high

Confidentiality medium

Confidentiality low

Integrity high

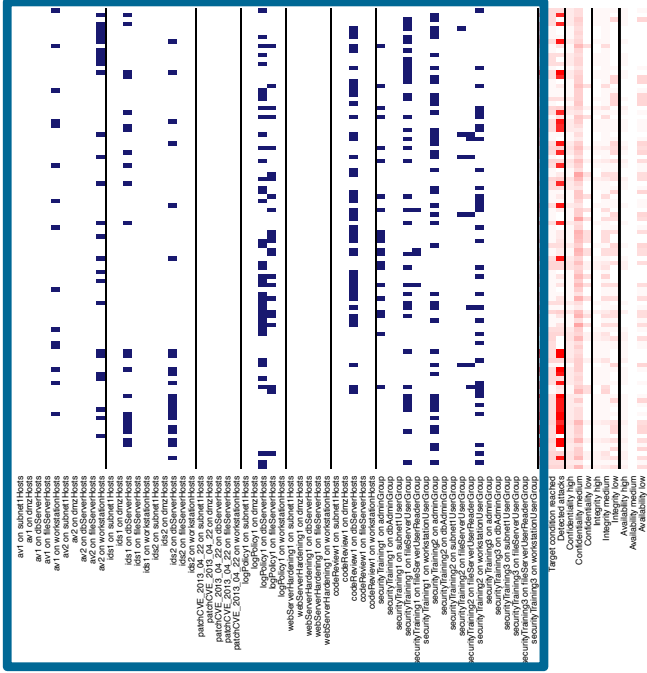
Integrity medium

Integrity low

Availability high

Availability medium

Availability low



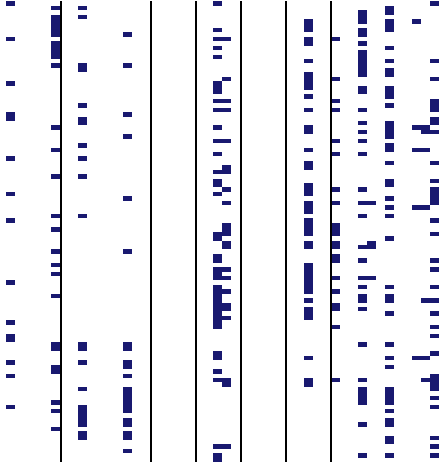
Results: Unskilled external

av1 on subnet1/Hosts
av1 on ctmz/Hosts
av1 on dbServer/Hosts
av1 on workstation/Hosts
av1 on workstation/Hosts
av2 on subnet1/Hosts
av2 on ctmz/Hosts
av2 on dbServer/Hosts
av2 on workstation/Hosts
av2 on workstation/Hosts
ids1 on subnet1/Hosts
ids1 on ctmz/Hosts
ids1 on dbServer/Hosts
ids1 on workstation/Hosts
ids1 on workstation/Hosts
ids2 on subnet1/Hosts
ids2 on ctmz/Hosts
ids2 on dbServer/Hosts
ids2 on workstation/Hosts
ids2 on workstation/Hosts
patchCVE_2013_04_22 on subnet1/Hosts
patchCVE_2013_04_22 on ctmz/Hosts
patchCVE_2013_04_22 on dbServer/Hosts
patchCVE_2013_04_22 on workstation/Hosts
patchCVE_2013_04_22 on workstation/Hosts
logPolicy1 on ctmz/Hosts
logPolicy1 on dbServer/Hosts
logPolicy1 on workstation/Hosts
logPolicy1 on workstation/Hosts
logPolicy1 on workstation/Hosts
webServerHardening1 on subnet1/Hosts
webServerHardening1 on ctmz/Hosts
webServerHardening1 on dbServer/Hosts
webServerHardening1 on workstation/Hosts
webServerHardening1 on workstation/Hosts
codeReview1 on subnet1/Hosts
codeReview1 on ctmz/Hosts
codeReview1 on dbServer/Hosts
codeReview1 on workstation/Hosts
codeReview1 on workstation/Hosts
securityTraining1 on admin/Group
securityTraining1 on subnet1/UserGroup
securityTraining1 on ctmz/UserGroup
securityTraining1 on fileServer/UserGroup
securityTraining1 on workstation/UserGroup
securityTraining1 on workstation/UserGroup
securityTraining2 on admin/Group
securityTraining2 on ctmz/UserGroup
securityTraining2 on fileServer/UserGroup
securityTraining2 on workstation/UserGroup
securityTraining2 on workstation/UserGroup
securityTraining3 on admin/Group
securityTraining3 on ctmz/UserGroup
securityTraining3 on fileServer/UserGroup
securityTraining3 on workstation/UserGroup
securityTraining3 on workstation/UserGroup

Target condition reached

Confidentiality high
Confidentiality medium
Confidentiality low
Integrity high
Integrity medium
Integrity low
Availability high
Availability medium
Availability low

Success probability can be lowered to ~ 3%



Conclusions

Summary

- ▶ Simulation-Optimization framework for IT security
- ▶ Attacker-centric approach

Current research challenges

- ▶ Knowledge base: attack pattern formalization
- ▶ Simulation: cognitive and behavioral model
- ▶ Optimization:
 - ▶ cost of portfolio evaluations
 - ▶ cost of permutations

Future work

- ▶ Control selection → system design
(very large design space + constraints)
- ▶ Problem-specific genotype structure

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

40

Conclusions

Appendix

46



Q & A

Contact:
ekiesling@sba-research.org

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

41 Conclusions

Appendix

Implementation

Knowledge base

- ▶ Initial experiments with OWL ontologies
- ▶ SWI-Prolog:¹ current rule-based implementation
- ▶ JPL:² Java access

Simulation

- ▶ Java 1.6
- ▶ Mason 14:³ discrete-event core
- ▶ Colt 1.2:⁴ random distributions
- ▶ Jung 2.0.1:⁵ graph structures and visualization
- ▶ Log4j, XStream, JUnit, Commons, ...

Optimization

- ▶ Opt4j 2.7⁶: evolutionary computation framework

¹ <http://www.swi-prolog.org>

² <http://www.swi-prolog.org/packages/jpl>

³ <http://cs.gmu.edu/~eclab/projects/mason/>

⁴ <http://acs.lbl.gov/software/colt/>

⁵ <http://jung.sourceforge.net/>

⁶ <http://opt4j.sourceforge.net/>

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

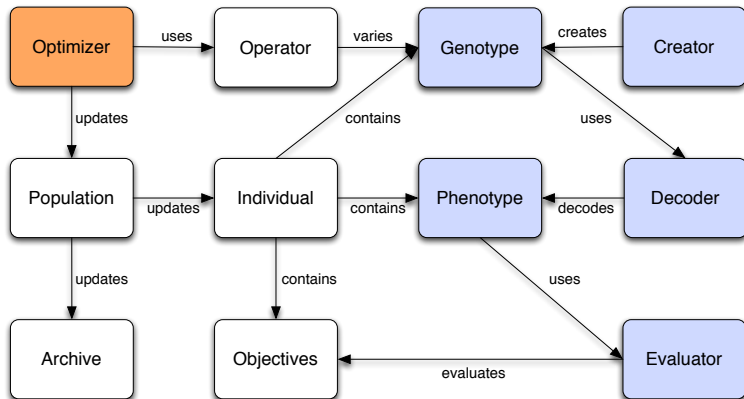
Experimental setup

Results

Conclusions

42 Appendix

Implementation: Optimization



Source: adapted from [?]

Introduction

Framework

- Knowledge base
- Attack patterns
- Simulation
- Optimization
- Decision support

Example

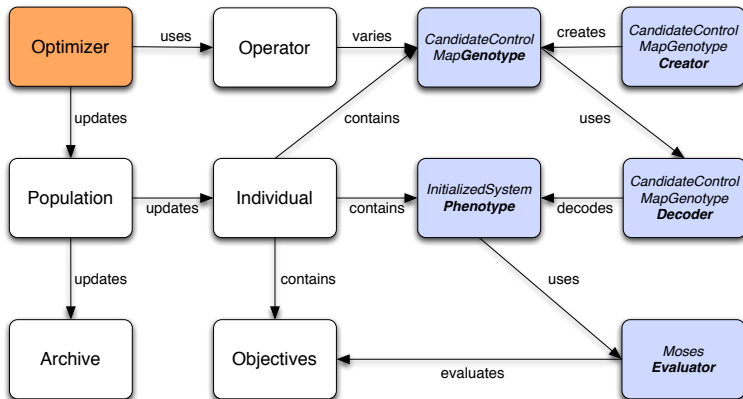
- Experimental setup
- Results

Conclusions

43 Appendix

46

Implementation: Optimization



Source: adapted from [?]

Introduction

Framework

- Knowledge base
- Attack patterns
- Simulation
- Optimization
- Decision support

Example

- Experimental setup
- Results

Conclusions

43 Appendix

46

Simulation approach - Motivation

1. Model dynamic attacks

- ▶ Strategic behavior: Attackers adapt to the system architecture
- ▶ Attacks consist of multiple sequential steps
- ▶ Each step potentially changes the system state
- ▶ Steps chosen depend on results of previous actions
- ▶ Controls influence attacker strategy
- ▶ Not all attackers behave the same way

2. Tackle complexity

- ▶ Constructing and analysing full attack graphs infeasible for large systems
- ▶ Security problems inherently stochastic

3. Capture inherent variability

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

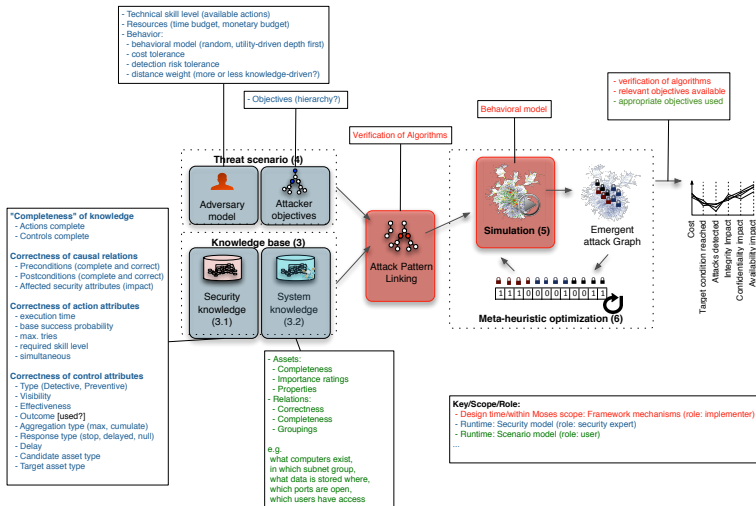
Results

Conclusions

44 Appendix

46

Validation



Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

45

Appendix

46

References I

Introduction

Framework

Knowledge base

Attack patterns

Simulation

Optimization

Decision support

Example

Experimental setup

Results

Conclusions

46 Appendix