Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

An Optimal Metric-Aware Response Selection Strategy for Intrusion Response Systems

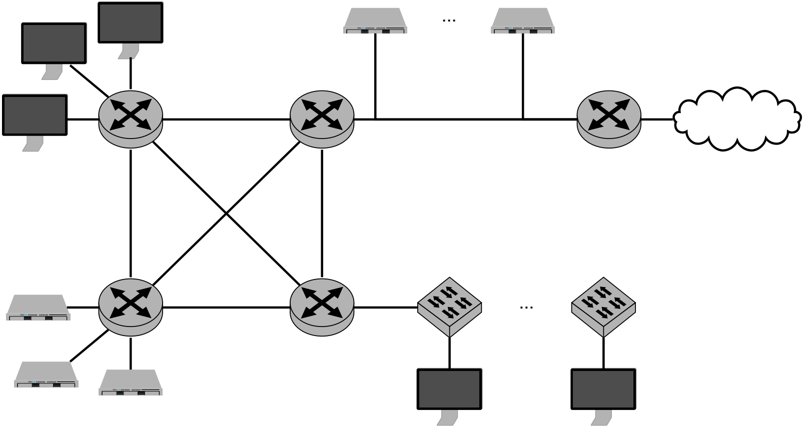
Nadine Herold, Matthias Wachs, Stephan-A. Posselt and Georg Carle

October 23, 2016

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

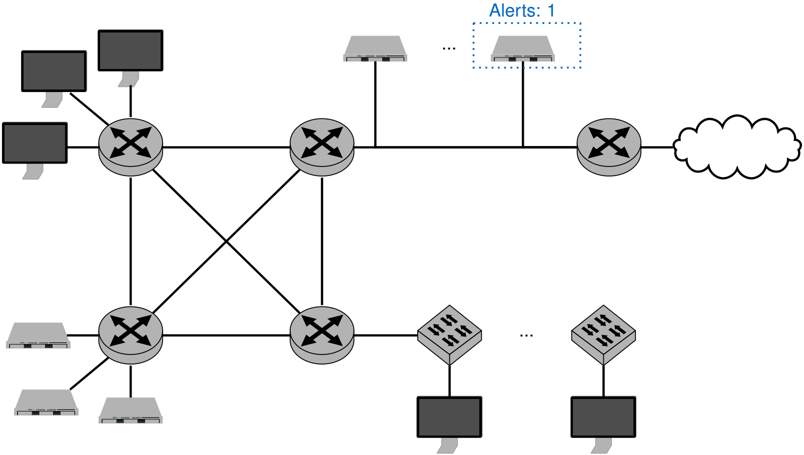
Introduction and Problem Statement

Motivation



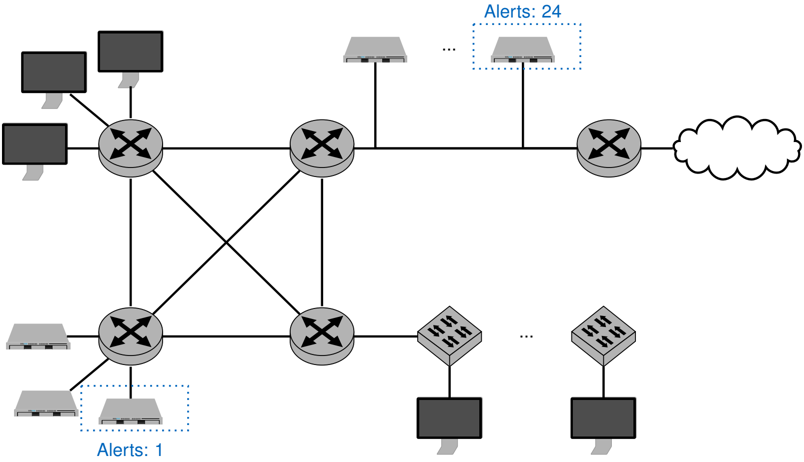
Introduction and Problem Statement

Motivation



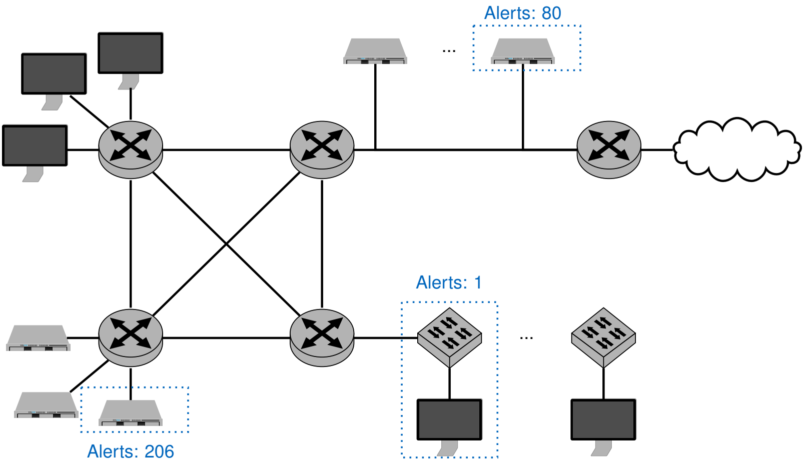
Introduction and Problem Statement

Motivation



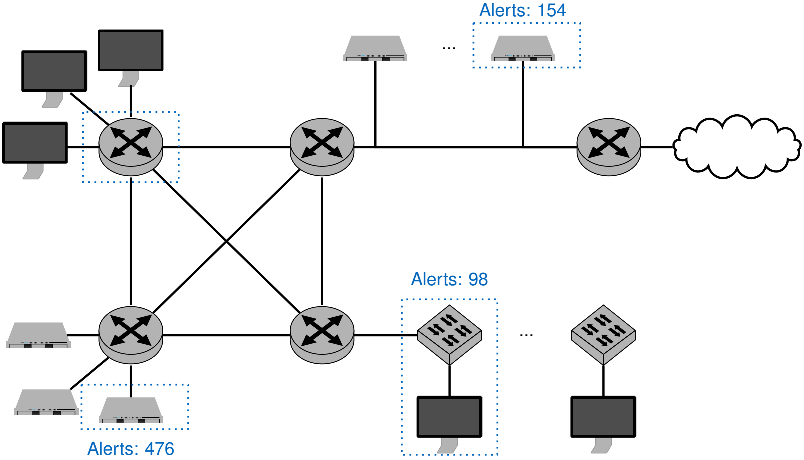
Introduction and Problem Statement

Motivation



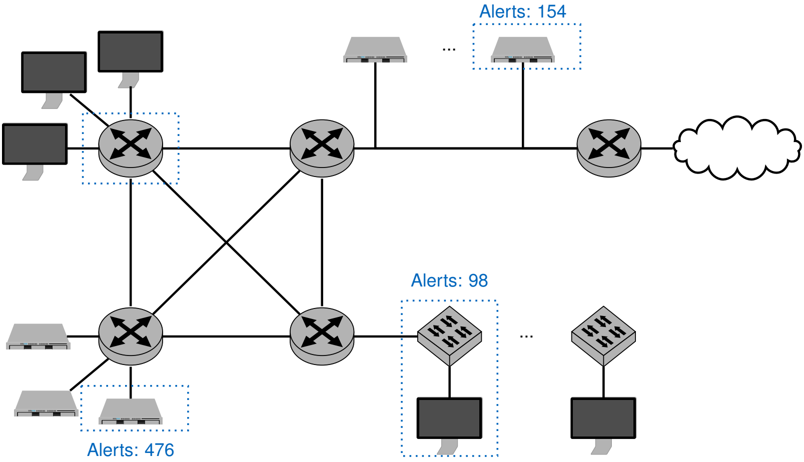
Introduction and Problem Statement

Motivation



Introduction and Problem Statement

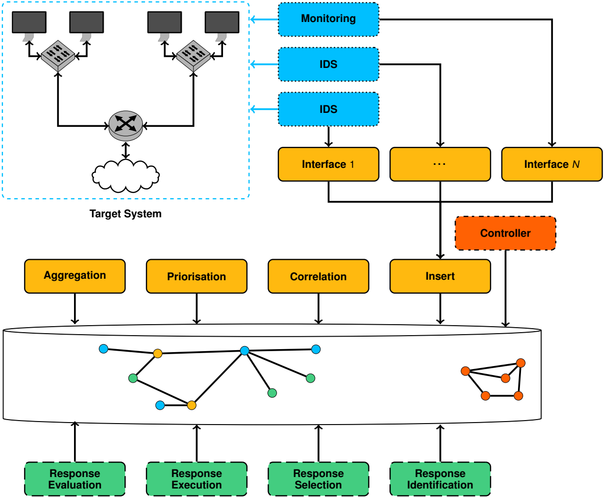
Motivation



What can we do now? What options do we have?

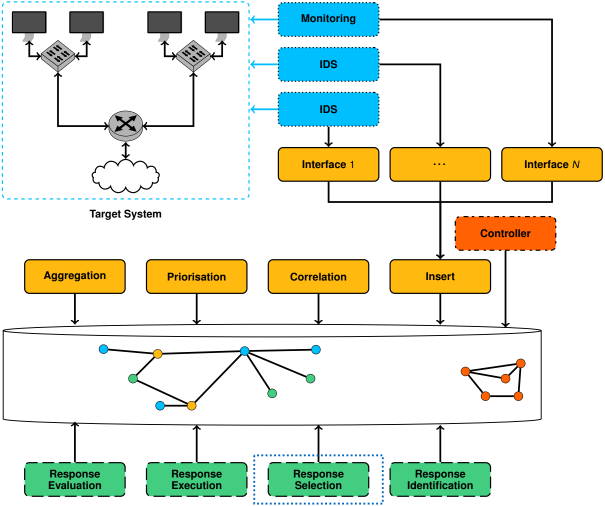
Introduction and Problem Statement

What do we want to achieve?



Introduction and Problem Statement

What do we want to achieve?



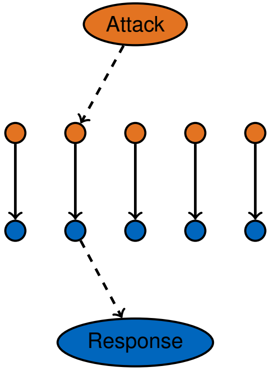
Related Work

Existing Approaches towards Response Selection

Related Work

Existing Approaches towards Response Selection

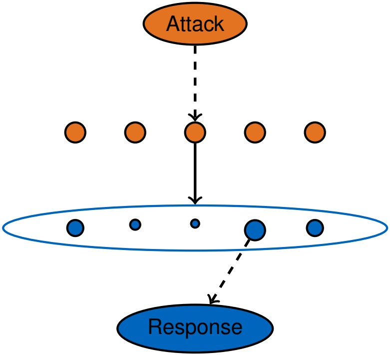
- Rule based approaches (static mappings or ECA rules) [4, 12, 21, 3, 17]



Related Work

Existing Approaches towards Response Selection

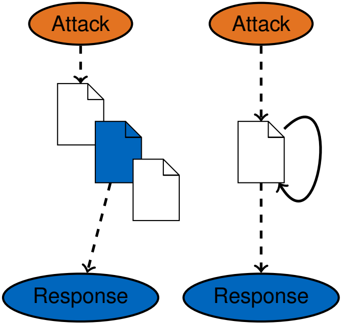
- Rule based approaches (static mappings or ECA rules) [4, 12, 21, 3, 17]
- Basic cost-sensitive approaches [6, 23, 26, 24, 25, 28, 1, 20, 16, 15, 14, 22]



Related Work

Existing Approaches towards Response Selection

- Rule based approaches (static mappings or ECA rules) [4, 12, 21, 3, 17]
- Basic cost-sensitive approaches [6, 23, 26, 24, 25, 28, 1, 20, 16, 15, 14, 22]
- Pre- or post-processing based approaches [8, 7, 27]



Related Work

Existing Approaches towards Response Selection

- Rule based approaches (static mappings or ECA rules) [4, 12, 21, 3, 17]
- Basic cost-sensitive approaches [6, 23, 26, 24, 25, 28, 1, 20, 16, 15, 14, 22]
- Pre- or post-processing based approaches [8, 7, 27]
- Decide whether or not to respond automated [2, 30]

System Design

Central Question and Approach

Formulating a Mixed Integer Linear Programming problem such that we can answer the following question:

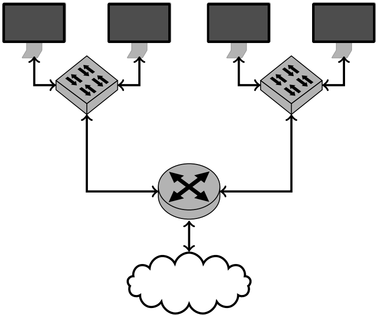
In a given model instance, which subset from the set of responses available

- *frees all affected entities from an incident,*
- *has minimal cost within the given set of metrics, and*
- *has lower cost than the incident being unmitigated?*

First, we define a set-based description that models the response selection problem. We transform this set-based description into a Linear Programming Problem. For each response selection process the instance is created and solved.

System Design

Illustrative Example

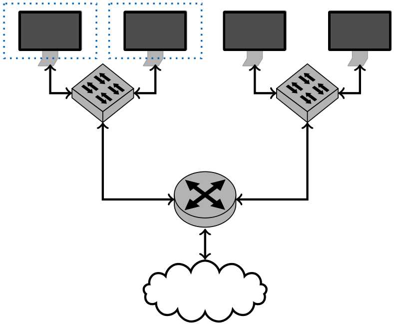


Target system with

- 4 hosts,
- 2 switches, and
- 1 router

System Design

Illustrative Example

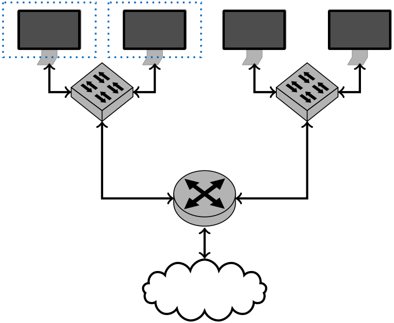


Attack on services running on

- host 1 (h_1) and
- host 2 (h_2)

System Design

Illustrative Example



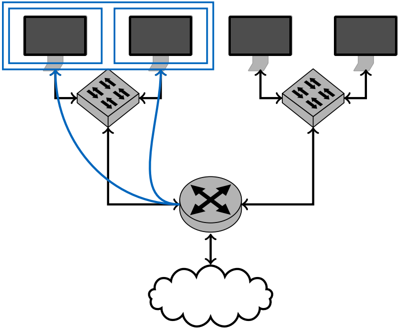
What can we do?

- What can we execute?
- Who can execute?
- Who is (positive) effected?
- What restrictions to consider?

Response	Executing	Effected			Conflicts

System Design

Illustrative Example



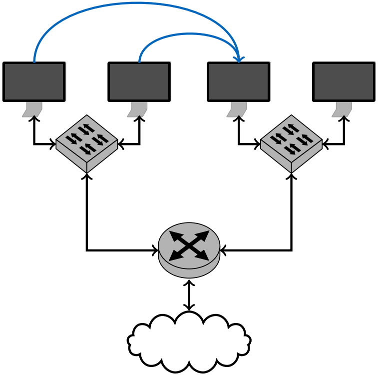
Router can block traffic to

- host 1 (h_1)
- host 2 (h_1)
- (h_1) and (h_2)

Response	Executing	Effected			Conflicts
$r_{block}(h_1)$	*router*	h_1			-
$r_{block}(h_2)$	*router*	h_2			-
$r_{block}(n)$	*router*	h_2, h_1			-

System Design

Illustrative Example



Services can be migrated to

- host 3 (h_3)

Capacity for one service!

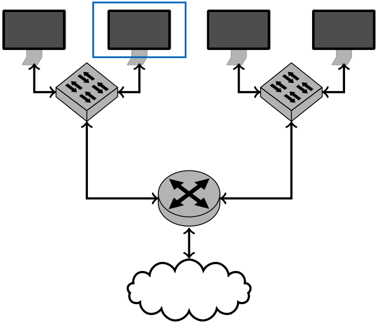
Response	Executing	Effected			Conflicts
$r_{block}(h_1)$	*router*	h_1			-
$r_{block}(h_2)$	*router*	h_2			-
$r_{block}(n)$	*router*	h_2, h_1			-
$r_{migrate}(h_1)$	h_3	h_1			$r_{migrate}(h_2)$
$r_{migrate}(h_2)$	h_3	h_2			$r_{migrate}(h_1)$

System Design

Illustrative Example

Reconfigure service running on

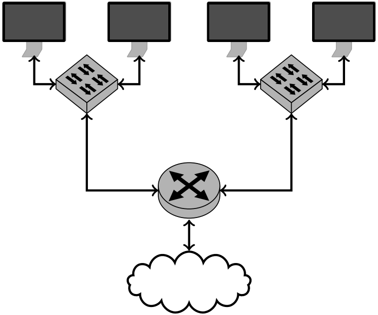
- host 2 (h_2)



Response	Executing	Effected			Conflicts
$r_{block}(h_1)$	*router*	h_1			-
$r_{block}(h_2)$	*router*	h_2			-
$r_{block}(n)$	*router*	h_2, h_1			-
$r_{migrate}(h_1)$	h_3	h_1			$r_{migrate}(h_2)$
$r_{migrate}(h_2)$	h_3	h_2			$r_{migrate}(h_1)$
$r_{reconf}(h_2)$	h_2	h_2			-

System Design

Illustrative Example



Use metrics to assess responses, e.g.

- duration
- cost

Huge variety available in literature ([15, 16, 6, 31, 29, 18, 25, 24, 30, 14, 13, 5, 11, 23, 19, 22, 20, 9, 10]).

Response	Executing	Effected	Duration	Costs	Conflicts
$r_{block}(h_1)$	*router*	h_1	1.2	70	-
$r_{block}(h_2)$	*router*	h_2	1.2	50	-
$r_{block}(n)$	*router*	h_2, h_1	1.5	90	-
$r_{migrate}(h_1)$	h_3	h_1	10	20	$r_{migrate}(h_2)$
$r_{migrate}(h_2)$	h_3	h_2	10	20	$r_{migrate}(h_1)$
$r_{reconf}(h_2)$	h_2	h_2	5	10	-

System Design

Set-based Description

Description	Set	Example
Set of entities in the network	$S = \{s_1, s_2, ...\}$	$\{h_1, h_2, h_3, h_4, r\}$
Set of entities affected by the incident	$A = \{a_1, a_2, ...\} \subseteq S$	$\{h_1, h_2\}$
Set of responses to counter the incident	$R = \{r_1, r_2, ...\}$	$\{r_{b_1}, r_{b_2}, r_{b_3}, r_{m_1}, r_{m_2}, r_r\}$
Set of metrics to assess responses	$M = \{m_1, m_2, ...\}$	$\{d, c\}$
Response costs with respect to metrics	$c\colon R \times M \to \mathbb{R}_{\geq 0}$	$\{(r_r, d) = 4, (r_r, c) = 10, \cdots\}$
Potential damage of the incident	$d\colon M \to \mathbb{R}_{\geq 0}$	$\{(d) = 60, (c) = 20\}$
Information on conflicting responses	$c\colon R \times R \to \mathbb{B}$	$\{(r_{m_1}, r_{m_2}) = 1, \cdots\}$
Executor of a response	$e\colon S \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, \cdots\}$
Hosts a response effects	$f\colon A \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, (h_1, r_r) = 0, \cdots\}$

System Design

Set-based Description

Description	Set	Example
Set of entities in the network •	$S = \{s_1, s_2, ...\}$	$\{h_1, h_2, h_3, h_4, r\}$
Set of entities affected by the incident	$A = \{a_1, a_2, ...\} \subseteq S$	$\{h_1, h_2\}$
Set of responses to counter the incident •	$R = \{r_1, r_2, ...\}$	$\{r_{b_1}, r_{b_2}, r_{b_3}, r_{m_1}, r_{m_2}, r_r\}$
Set of metrics to assess responses •	$M = \{m_1, m_2, ...\}$	$\{d, c\}$
Response costs with respect to metrics	$c: R \times M \rightarrow \mathbb{R}_{\geq 0}$	$\{(r_r, d) = 4, (r_r, c) = 10, \cdots\}$
Potential damage of the incident	$d: M \rightarrow \mathbb{R}_{\geq 0}$	$\{(d) = 60, (c) = 20\}$
Information on conflicting responses •	$c: R \times R \rightarrow \mathbb{B}$	$\{(r_{m_1}, r_{m_2}) = 1, \cdots\}$
Executor of a response •	$e: S \times R \rightarrow \mathbb{B}$	$\{(h_2, r_r) = 1, \cdots\}$
Hosts a response effects •	$f: A \times R \rightarrow \mathbb{B}$	$\{(h_2, r_r) = 1, (h_1, r_r) = 0, \cdots\}$

Infrastructure information and policy given as input in advance •

System Design

Set-based Description

Description	**Set**	**Example**
Set of entities in the network •	$S = \{s_1, s_2, ...\}$	$\{h_1, h_2, h_3, h_4, r\}$
Set of entities affected by the incident $*$	$A = \{a_1, a_2, ...\} \subseteq S$	$\{h_1, h_2\}$
Set of responses to counter the incident •	$R = \{r_1, r_2, ...\}$	$\{r_{b_1}, r_{b_2}, r_{b_3}, r_{m_1}, r_{m_2}, r_r\}$
Set of metrics to assess responses •	$M = \{m_1, m_2, ...\}$	$\{d, c\}$
Response costs with respect to metrics	$c\colon R \times M \to \mathbb{R}_{\geq 0}$	$\{(r_r, d) = 4, (r_r, c) = 10, \cdots\}$
Potential damage of the incident $*$	$d\colon M \to \mathbb{R}_{\geq 0}$	$\{(d) = 60, (c) = 20\}$
Information on conflicting responses •	$c\colon R \times R \to \mathbb{B}$	$\{(r_{m_1}, r_{m_2}) = 1, \cdots\}$
Executor of a response •	$e\colon S \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, \cdots\}$
Hosts a response effects •	$f\colon A \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, (h_1, r_r) = 0, \cdots\}$

Infrastructure information and policy given as input in advance •

Information to extract from the incident $*$

System Design

Set-based Description

Description	Set	Example
Set of entities in the network •	$S = \{s_1, s_2, ...\}$	$\{h_1, h_2, h_3, h_4, r\}$
Set of entities affected by the incident ∗	$A = \{a_1, a_2, ...\} \subseteq S$	$\{h_1, h_2\}$
Set of responses to counter the incident •	$R = \{r_1, r_2, ...\}$	$\{r_{b_1}, r_{b_2}, r_{b_3}, r_{m_1}, r_{m_2}, r_r\}$
Set of metrics to assess responses •	$M = \{m_1, m_2, ...\}$	$\{d, c\}$
Response costs with respect to metrics †	$c: R \times M \to \mathbb{R}_{\geq 0}$	$\{(r_r, d) = 4, (r_r, c) = 10, \cdots\}$
Potential damage of the incident ∗	$d: M \to \mathbb{R}_{\geq 0}$	$\{(d) = 60, (c) = 20\}$
Information on conflicting responses •	$c: R \times R \to \mathbb{B}$	$\{(r_{m_1}, r_{m_2}) = 1, \cdots\}$
Executor of a response •	$e: S \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, \cdots\}$
Hosts a response effects •	$f: A \times R \to \mathbb{B}$	$\{(h_2, r_r) = 1, (h_1, r_r) = 0, \cdots\}$

Infrastructure information and policy given as input in advance •

Information to extract from the incident ∗

Information to collect during response execution †

System Design

MILP Definition

Objective Function

$$\min(\sum_{i=1}^{|R|} \sum_{j=1}^{|M|} n_i c_{i,j}) = \min(n_1 c_{1,1} + \cdots + n_{|R|} c_{|R|,|M|})$$

Freed Constraint

$$\forall a \in A: \sum_{j=1}^{|R|} n_j f_{a,j} \geq 1$$

Uniqueness Constraint

$$\forall r_i \in R: 0 \leq n_i \leq 1$$

Damage Constraint

$$\forall m \in M: \sum_{i=1}^{|R|} n_i c_{i,m} \leq d_m$$

Conflicting Constraint

$$\sum_{i=1}^{|R|} \sum_{j=1}^{|R|} o_{i,j} n_i n_j = 0$$

Implementation and Evaluation

Implementation

- Mixed Integer Linear Programming (MILP) formulation for GLPK and CPLEX
- Heuristics for comparison (Cheapest-First and Coverage-First)
- Test-framework to generate scenarios, compare implementations, and gain statistics
- Generic solver API for embedding the solvers into other applications

Code available on GitHub using GPLv3 license:

`https://github.com/Egomania/ResponseSelection`

Evaluation Methodology

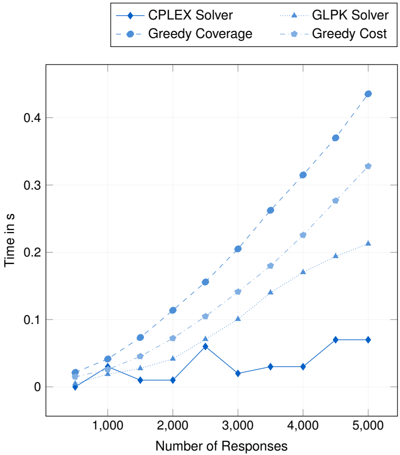
We analyze the behavior of the presented MILP approach and both heuristics in different incident scenarios by increasing problem complexity. We raise the problem complexity by increasing (one at a time) the

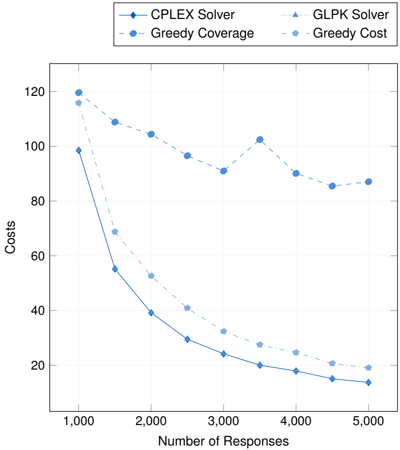
a. Number of responses
b. Number of entities
c. Number of conflicts
d. Number of entities a response is applicable to (coverage factor)

in the problem while keeping the number of remaining problem parameters fixed.

Implementation and Evaluation

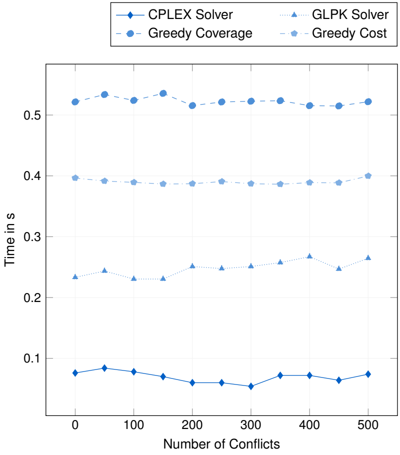
Results - Increasing Number of Responses

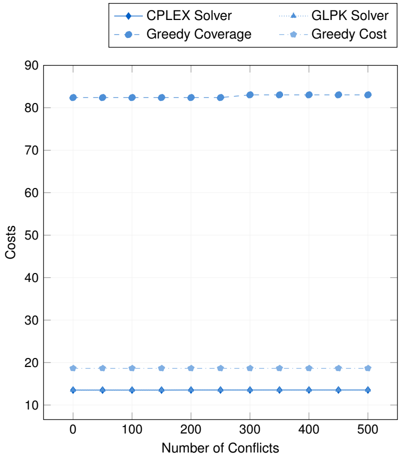




Implementation and Evaluation

Results - Increasing Number of Conflicts





Wrap Up

Conclusion and Future Work

Contributions

- Formulation of response selection as MILP Problem.
- Implementation with different solvers.
- Applicability is shown in all dimensions of the problem complexity.
- Cost and performance comparison with two different heuristics.

Improvements for the Future

- Include pre- and postconditions.
- Integrate existing assessment approaches as cost functions.
- Provide partial solutions.

Wrap Up

Contact

Thank you for the audience!

Nadine Herold, Matthias Wachs, Stephan-A. Posselt and Georg Carle

Technische Universität München
Department of Informatics
Chair of Network Architectures and Services
Boltzmann Straße 3
85748 Garching bei München
Germany

`{lastname}@net.in.tum.de`
`https://github.com/Egomania/ResponseSelection`

Bibliography

[1] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt.
Using specification-based intrusion detection for automated response.
In G. Vigna, C. Kruegel, and E. Jonsson, editors, *Recent Advances in Intrusion Detection*, volume 2820 of *Lecture Notes in Computer Science*, pages 136–154. Springer Berlin Heidelberg, 2003.

[2] M. Bloem, T. Alpcan, and T. Basar.
Intrusion response as a resource allocation problem.
In *45th IEEE Conference on Decision and Control*, December 2006.

[3] E. Costante, D. Fauri, S. Etalle, J. den Hartog, and N. Zannone.
A hybrid framework for data loss prevention and detection.
In *Proceedings of the Workshop on Research for Insider Threats (WRIT)*, 2016.

[4] N. Cuppens-Boulahia, F. Cuppens, J. de Vergara, E. Vazquez, J. Guerra, and H. Debar.
An ontology-based approach to react to network attacks.
In *3rd International Conference on Risks and Security of Internet and Systems (CRiSIS '08)*, pages 27–35, October 2008.

[5] A. Fawaz, R. Berthier, and W. Sanders.
Cost modeling of response actions for automated response and recovery in ami.
In *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pages 348–353, November 2012.

[6] G. Gonzalez Granadillo, H. Débar, G. Jacob, C. Gaber, and M. Achemlal.
Individual countermeasure selection based on the return on response investment index.
In I. Kotenko and V. Skormin, editors, *Computer Network Security*, volume 7531 of *Lecture Notes in Computer Science*, pages 156–170. Springer Berlin Heidelberg, 2012.

[7] G. G. Granadillo, E. Alvarez, A. Motzek, M. Merialdo, J. Garcia-Alfaro, and H. Debar.
Towards an automated and dynamic risk management response system.
In *21st Nordic Conference on Secure IT Systems (NordSec)*, 2016.

Bibliography

[8] G. G. Granadillo, A. Motzek, J. Garcia-Alfaro, and H. Debar.
Selection of mitigation actions based on financial and operational impact assessments.
In *11th International Conference on Availability, Reliability and Security (ARES)*, 2016.

[9] M. Jahnke, C. Thul, and P. Martini.
Graph based metrics for intrusion response measures in computer networks.
In *32nd IEEE Conference on Local Computer Networks (LCN)*, pages 1035–1042, October 2007.

[10] M. Jahnke, C. Thul, and P. Martini.
Comparison and improvement of metrics for selecting intrusion response measures against dos attacks.
In *Sicherheit*, pages 381–393. Citeseer, 2008.

[11] B. R. Jalal Baayer.
New cost-sensitive model for intrusion response systems minimizing false positive.
IJMER - International Journal of Modern Engineering Research, 2(5):3473–3478, October 2012.

[12] A. Kamra and E. Bertino.
Design and implementation of an intrusion response system for relational databases.
IEEE Transactions on Knowledge and Data Engineering, 23(6):875–888, 2011.

[13] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, and A. Martin.
Success likelihood of ongoing attacks for intrusion detection and response systems.
In *International Conference on Computational Science and Engineering (CSE '09)*, volume 3, pages 83–91, August 2009.

[14] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, and A. Martin.
Intelligent response system to mitigate the success likelihood of ongoing attacks.
In *6th International Conference on Information Assurance and Security (IAS)*, pages 99–105, Aug 2010.

[15] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar.
A service dependency model for cost-sensitive intrusion response.
In D. Gritzalis, B. Preneel, and M. Theoharidou, editors, *Computer Security – ESORICS 2010*, volume 6345 of *Lecture Notes in Computer Science*, pages 626–642. Springer Berlin Heidelberg, 2010.

[16] N. Kheir, H. Debar, N. Cuppens-Boulahia, F. Cuppens, and J. Viinikka.
Cost evaluation for intrusion response using dependency graphs.
In *International Conference on Network and Service Security (N2S '09)*, pages 1–6, June 2009.

[17] H. K. Kim, K. H. Im, and S. C. Park.
{DSS} for computer security incident response applying {CBR} and collaborative response.
Expert Systems with Applications, 37(1):852 – 870, 2010.

[18] W. Lee, M. Miller, S. J. Stolfo, W. Fan, and E. Zadok.
Toward cost-sensitive modeling for intrusion detection and response.
Journal of Computer Security, 10:2002, 2002.

[19] V. Mateos, V. A. Villagrá, F. Romero, and J. Berrocal.
Definition of response metrics for an ontology-based automated intrusion response systems.
Computers & Electrical Engineering, 38(5):1102 – 1114, 2012.

[20] S. Ossenbühl, J. Steinberger, and H. Baier.
Towards automated incident handling: How to select an appropriate response against a network-based attack?
In *9th International Conference on IT Security Incident Management IT Forensics (IMF)*, pages 51–67, May 2015.

[21] D. Schnackengerg, H. Holliday, R. Smith, K. Djahandari, and D. Sterne.
Cooperative intrusion traceback and response architecture (citra).
In *Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX '01)*, volume 1, pages 56–68, 2001.

Bibliography

[22] A. Shameli-Sendi and M. Dagenais.
Orcef: online response cost evaluation framework for intrusion response system.
Journal of Network and Computer Applications, 55:89–107, 2015.

[23] N. Stakhanova, S. Basu, and J. Wong.
A cost-sensitive model for preemptive intrusion response systems.
In *21st International Conference on Advanced Information Networking and Applications (AINA '07)*, pages 428–435, May 2007.

[24] C. Strasburg, N. Stakhanova, S. Basu, and J. Wong.
A framework for cost sensitive assessment of intrusion response selection.
In *33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC '09)*, volume 1, pages 355–360, 2009.

[25] C. Strasburg, N. Stakhanova, S. Basu, and J. S. Wong.
Intrusion response cost assessment methodology.
In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09)*, pages 388–391, New York, NY, USA, 2009. ACM.

[26] C. R. Strasburg, N. Stakhanova, S. Basu, and J. S. Wong.
The methodology for evaluating response cost for intrusion response systems.
Technical Report TR08-12, Iowa State University, 2008.

[27] S. Sultana, D. Midi, and E. Bertino.
Kinesis: A security incident response and prevention system for wireless sensor networks.
In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems (SenSys '14)*, pages 148–162, New York, NY, USA, 2014. ACM.

[28] T. Toth and C. Kruegel.
Evaluating the impact of automated intrusion response mechanisms.
In *Proceedings of the 18th Annual Computer Security Applications Conference*, pages 301–310, 2002.

Bibliography

[29] Y. Wu and S. Liu.
A cost-sensitive method for distributed intrusion response.
In *12th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 760–764, 2008.

[30] W. T. Yue and M. Çakanyıldırım.
A cost-based analysis of intrusion detection system configuration under active or passive response.
Decision Support Systems, 50(1):21 – 31, 2010.

[31] Z. Zhang, P.-H. Ho, and L. He.
Measuring ids-estimated attack impacts for rational incident response: A decision theoretic approach.
Computers & Security, 28(7):605 – 614, 2009.