Reaktionsauswahl mittels Lineare Optimierung

SURF – Systemic Security for Critical Infrastructures

Abschlussmeeting und Demoday für das Projekt SURF
08.12.2016, Infineon Technologies AG, Am Campeon 1-12, Neubiberg

Nachteile bisheriger Lösungen

Statische Zuweisungen **von vordefinierten Reaktionen auf Angriffe sind wenige flexibel und bedürfen einer zeitintensiven Wartung.**

Kosten-sensitive Ansätze **ermöglichen nur die Auswahl einer einzelnen Reaktion auf einen einzelnen Angriff. Relationen und Synergy-Effekte zwischen Reaktionen werden außen vorgelassen.**

Bisherige Ansätze basierend auf der Erstellung von *Reaktionsplänen* bedürfen einer aufwändigen Vor- oder Nachbearbeitung der erstellten Pläne.

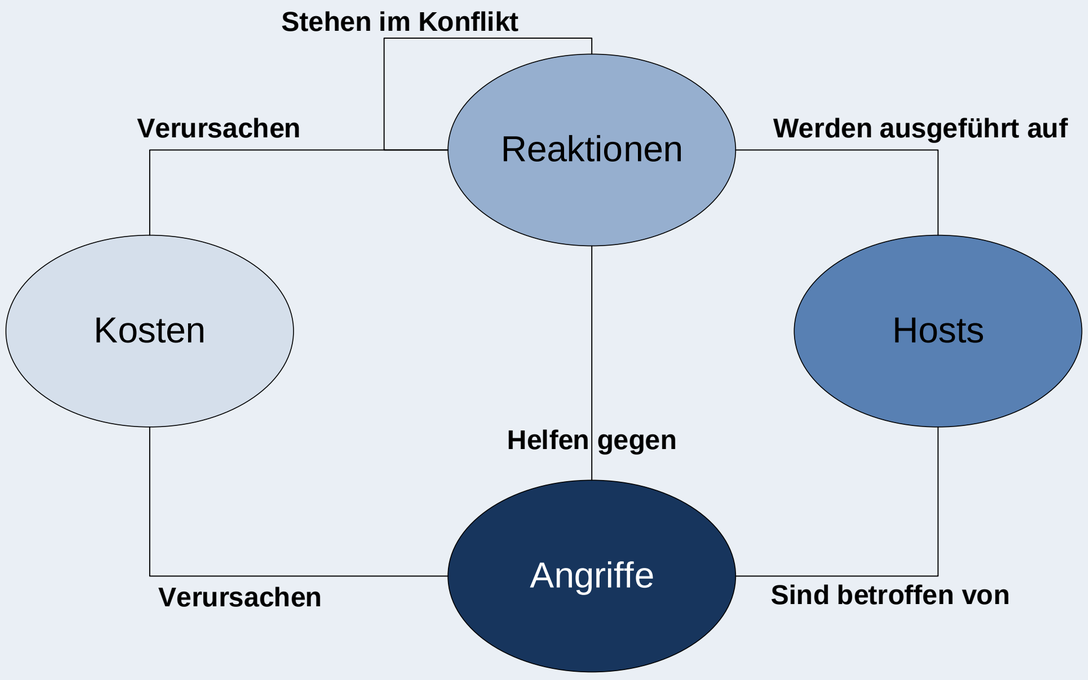
Mixed Integer Linear Programming

Für eine gegebene Modellinstanz sollen die folgenden Fragestellungen beantwortet werden: Welche zur Verfügung stehenden Reaktionen müssen ausgewählt werden, sodass

- **… alle vom Angriff betroffenen Entitäten befreit werden?**
- **… die minimal möglichen Kosten entstehen?**
- **… nicht mehr Kosten als Schaden entstehen?**
- **… Relationen zwischen den Reaktionen beachtet werden?**

Problemlösung: Erstellen eines Mengen-basierten Modells, Transformation in eine MILP-Instanz (Mixed Integer Linear Programming) und Lösung mithilfe verfügbarer Solver.

Mengendarstellung



Mathematische Darstellung

Zielfunktion:	$\min(\sum_{i=1}^{\lvert R\rvert}\sum_{j=1}^{\lvert M\rvert} n_i c_{i,j})$	**Minimale Kosten**
Effektivität:	$\forall a \in A : \sum_{j=1}^{\lvert R\rvert} n_j f_{a,j} \geq 1$	**Befreiung aller Entitäten**
Eindeutigkeit:	$\forall r_i \in R : 0 \leq n_i \leq 1$	**Reaktion wählen oder nicht**
Schaden:	$\forall m \in M : \sum_{i=1}^{\lvert R\rvert} n_i c_{i,m} \leq d_m$	**Kosten unter Schaden**
Konflikte:	$\sum_{j=1}^{\lvert R\rvert}\sum_{i}^{\lvert R\rvert} n_i n_j o_{i,j} = 0$	**Reaktionen sind Konfliktfrei**

Implementierung

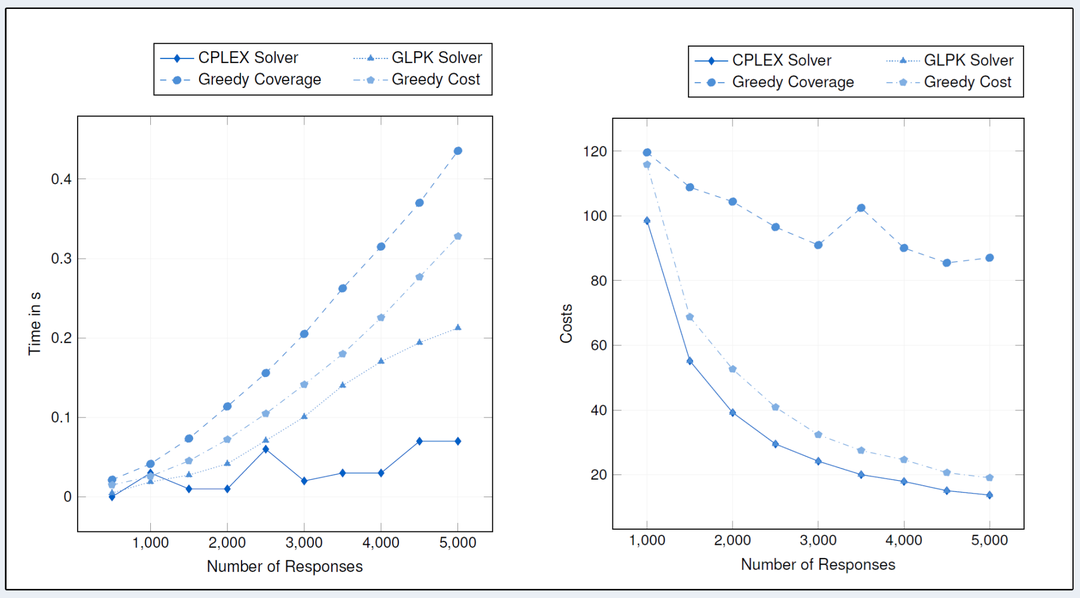
Umsetzung des mathematischen Modells mit Hilfe der Solver *CPLEX* und *GLPK*.

Implementierung von Heuristiken zur verbesserten Evaluation des Ansatzes: *Cheapest-First* und *Coverage-First*.

Testframework zur Generierung von Szenarien, zum Vergleichen von Implementierungen und zur Erhebung von Statistiken.

Implementierung einer generischen Solver-API zur Einbindung der einzelnen Solver in weitere Systeme.

Evaluation



Projekteckdaten

Gefördert vom BmBF

Bundesministerium für Bildung und Forschung

Laufzeit 09/2014 – 08/2016 (12/2016)

Bereich IT-Sicherheit – Kritische Infrastrukturen

Ziel Entwicklung einer Ganzheitlichen Lösung zur Verbesserung der Schutzsysteme für KRITIS

Weitere Informationen

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

Veröffentlichung:
Nadine Herold, Matthias Wachs, Stephan-A. Posselt, Goerg Carle: *An Optimal Metric-Aware Response Selection Strategy for Intrusion Response Systems*. In 9th International Symposium on Foundations & Practice of Security, Quebec, Kanada.

Kontaktinformationen – TUM

Webseite https://www.net.in.tum.de/html/surf/

Verbundkoordination Infineon Technologies AG

Kontaktadressen – TUM

Prof. Dr.-Ing. Georg Carle
+49 89 289 18030
carle@Net.in.tum.de

Dr. Holger Kinkelin
+49 89 289 18006
kinkelin@net.in.tum.de