NETWORK DEFENCE STRATEGY EVALUATION: SIMULATION VS. LIVE NETWORK

Tuesday 9th May, 2017

Jana Medková
Martin Husák, Martin Drašar

CSIRT-MU

Introduction

- optimal strategy to defend network infrastructure
- no standard for benchmarking

Introduction

- optimal strategy to defend network infrastructure
- no standard for benchmarking
- current state of strategy evaluation:
  - verification of the strategy's decision logic
  - evaluation in a simulated environment
    - simulated attacks
    - replayed attacks
  - evaluation in a real environment, in-house attacks

Research Questions

1. What are the differences between defence strategy evaluation in simulated and real environments?
2. Does the attacker change his behaviour based on the defender's actions?

Experiment Setup I

Semi-real Run

- during the experiment, the strategy was set to defend a network of honeypots in Masaryk University network

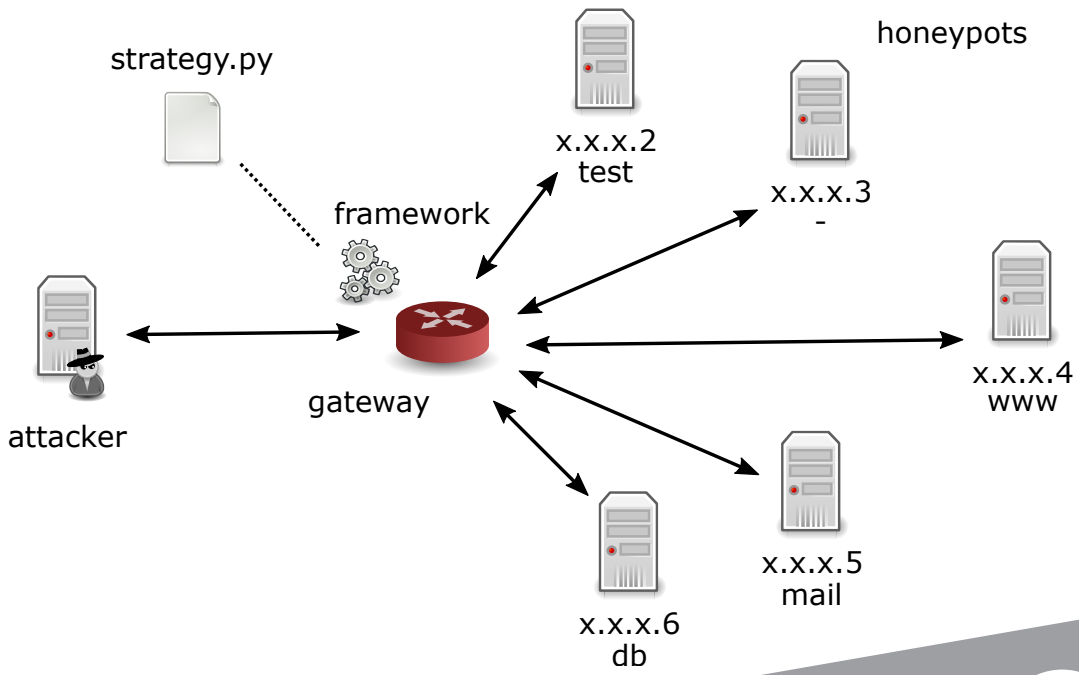
Simulation Run

- attacks observed on the network of honeypots before the experiment were replayed against the strategy

Experiment Setup II

Honeynet Topology

- central logging mechanisms and a database of authentication attempts
- gate that had the capability to manipulate the traffic
- experiment setup described in demo session



CSIRT-MU

Experiment Setup III

Defence Requirements

- the service should not be compromised (attack success penalty),
- the service should be available (unavailability penalty),
- the firewall should not be reconfigured frequently (reconfiguration penalty).

Tested Strategies I

Game Theory Based Strategy

- both the attacker's and defender's goals
- Nash equilibria to find the optimal defender's strategy
- finite, non-zero, two player game in an extensive form

Cost Sensitive Strategy

- considers the immediate defender's cost associated with action
- action cost consists of
  - negative impacts: cost of reconfiguration, cost of unavailability
  - positive impacts: potential damage that was mitigated by the defensive action

Collected Data

- experiment:
  - 644 attacks,
  - July and August 2016
- historical data:
  - 15,214 attacks,
  - December 2011 till June 2016

Strategy	Game theory	Cost sensitive
# attacks	207	437
# reconfigurations	2,374	1,029
# minutes blocked	5,294	22,467
# successful attacks	55	62

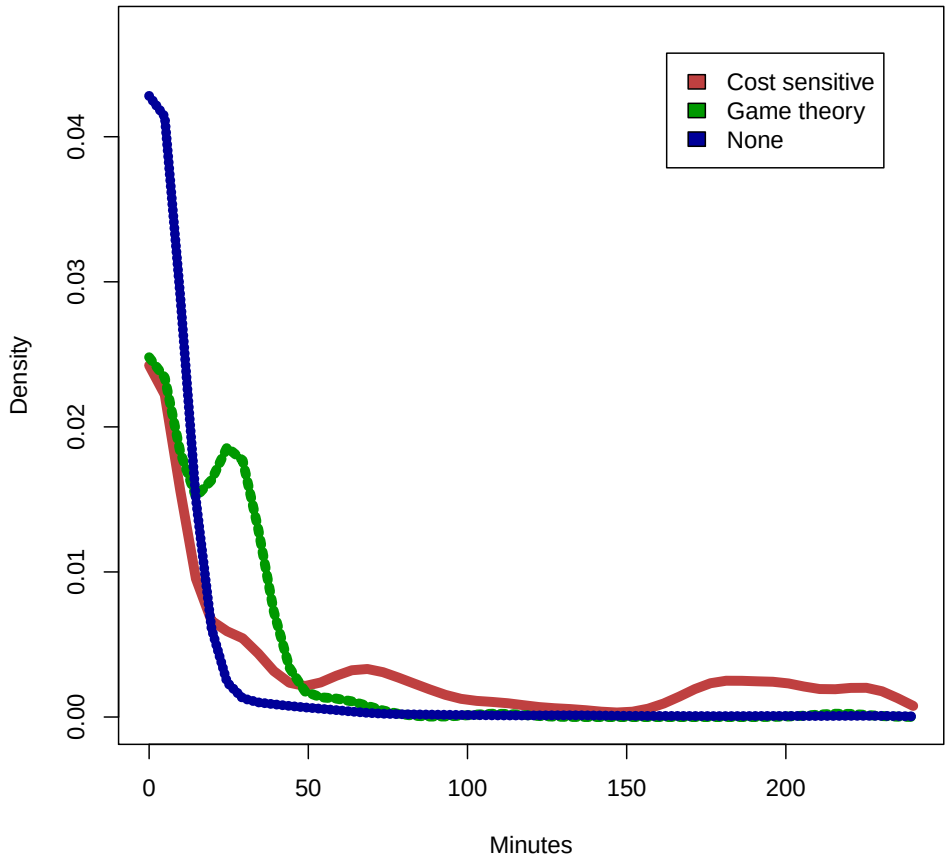
Simulated and Semi-real Execution

There is a statistically significant difference between the evaluation results in a simulated environment and a semi-real environment.

Environment	Strategy	Mean strategy score	Stdev
Semi-real	Game-theory	803	1,279
	Cost sensitive	489	938
Simulated	Game-theory	1,006	2,371
	Cost sensitive	1,109	2,343

Attacker's Behaviour

Attack Length



CSIRT-MU

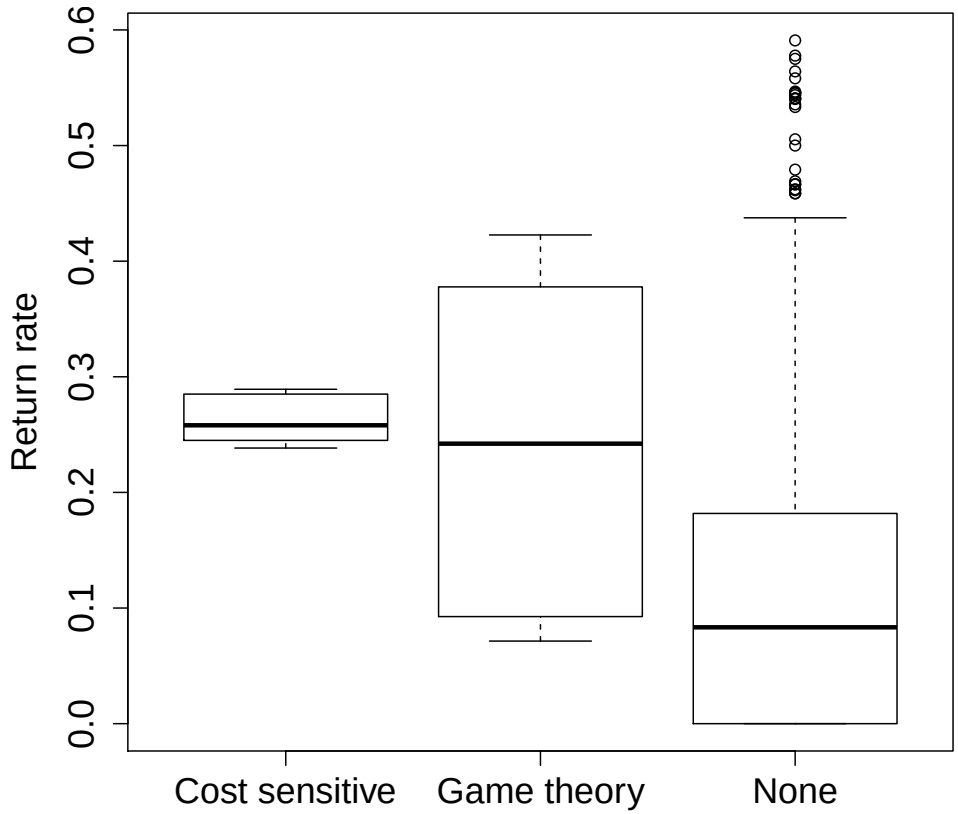
Attacker's Behaviour

Correlation Between Attack Length and Strategy Result

Environment	Strategy	Correlation	95% CI
Semi-real	Game-theory	0.11	[-0.02, 0.25]
	Cost sensitive	0.06	[-0.03, 0.15]
Simulated	Game-theory	0.35	[0.33, 0.36]
	Cost sensitive	0.41	[0.39, 0.42]

Attacker's Behaviour

Return Rate



CSIRT-MU

Attacker's Behaviour

Summary

The attackers reacted to the defence as follows:

- the attacks had longer duration
- they returned more often to continue in the attack
- the strategy result is less dependent on the length of the attack

Conclusion I

Lessons Learned

- the formal definition of requirements is not sufficient
- computational complexity of the strategies is often not reflected in the evaluation and have to be considered
- deployment in a real environment forces to address all aspects of the strategy

Conclusion II

Summary

- the most common evaluation is executed in simulated environment using replayed or simulated attacks
- we show that the evaluation using replayed attacks is not sufficient, since the attackers change in behaviour affects the evaluation results
- we found several changes in attacker behaviour due to the network defence

Conclusion III

Future Work

- we need a better, standardized methods for evaluation to enable objective comparison
- the evaluation should begin with simple, easily setup scenarios and continue to more realistic scenarios
- at least some of the evaluations should face real attackers

THANK YOU FOR YOUR ATTENTION!

www.kypo.cz

@csirtmu

Jana Medková

medkova@ics.muni.cz

UNIVERSITAS MASARYKIANA BRUNENSIS

ÚVT

CSIRT-MU