Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering

[Online Administration Praktische Arbeiten]

[Dept. T Admin Tools]

zurück Logout

Projektarbeit 2020 - HS: PA20_tebe_02

Allgemeines:

Titel:	Machine Learning driven control of Moving Target Defense (MTD) for cybersecurity
Anzahl Studierende:	2
Durchführung in Englisch möglich:	Ja, die Arbeit kann vollständig in Englisch durchgeführt werden und ist auch für Incomings geeignet.

Betreuer:

HauptbetreuerIn:	Bernhard Tellenbach, tebe
NebenbetreuerIn:	Gürkan Gür, gueu

Zugeteilte Studenten:

Diese Arbeit ist vereinbart mit:
- Levi Cailleret, caillev (IT)
- Sascha Kyburz, kybursas (IT)

Fachgebiet:

IS	Information Security

Studiengänge:

IT	Informatik

Zuordnung der Arbeit :

InIT	Institut für angewandte Informationstechnologie

Infrastruktur:

benötigt keinen zugeteilten Arbeitsplatz an der ZHAW

Interne Partner :

Es wurde kein interner Partner definiert!

Industriepartner:

Es wurden keine Industriepartner definiert!

Beschreibung:

The asymmetry between attackers and cybersecurity is a big problem since the former has a long time to assess the targets security standing (e.g., vulnerabilities, configuration, potential attack vectors) and perform reconnaissance. The idea of moving-target defense (MTD) is to impose the same asymmetric disadvantage on attackers by making systems dynamic and therefore harder to explore and predict with a constantly changing system and its ever-adapting attack surface. This is fundamentally a control problem which can be addressed via different algorithms including Machine Learning (ML) such as Reinforcement Learning (RL). **The main objective of this BS thesis is to investigate RL as a decision tool for MTD based evasion techniques**.

Goals

The goals of this thesis are as follows:

- You learn about Reinforcement Learning and how to use related techniques in a network security related case study.
- We have a better understanding of technical challenges regarding MTD and how to control it via RL techniques
- We have a simulated decision module (research grade) that can generate efficient and effective security countermeasures in terms of network configuration after an attack is detected (detection itself is out of scope.)
- We have performance evaluation results from our decision module based on some experimental scenarios

Tasks

To reach those goals, you have to complete the following tasks:

- Identify and examine related literature and solutions to understand the State-of-the-Art (SotA) in this field
- Learn about RL and MTD so that you have the knowledgebase to use them to build the thesis deliverables
- Design, implement and evaluate a decision module that provides security countermeasures against network attacks in a simulated environment

zurück Logout