Karlsruhe Institute of Technology

Research group: Prof. Dr. rer. nat. Martina Zitterbart

Machine Learning for Active Network Defense

Praxis der Forschung

RESEARCH TOPIC: NETWORK SECURITY, MACHINE LEARNING

DESCRIPTION

Machine learning – especially deep reinforcement learning – is currently one of the most prominent research areas in computer science. Bleeding edge prototypes continuously claim new records in various fields: CMU's Libratus beat four of the most professional poker players while Google's AlphaGo Zero succeeded against the world's best chess programs (after only four hours of self-training). Countless examples from other domains underline the importance of machine learning, from personal assistants to self-driving cars and smart health care.

Given their adaptability and high processing speed it comes as no surprise that machine learning is an emerging trend in the fast-paced cat-and-mouse game that is computer security – prominently demonstrated by the Mayham AI, which competed against human security experts in the DEFCON 24 capture the flag challenge. While autonomous computer systems have taken first steps in the art of cyber defense, their full integration into the landscape of network security remains a challenge.

ASSIGNMENT

Current approaches to predict adversarial behavior either focus on single-stage attack scenarios or provide a coarse-grained model to determine the next stage of a multi-stage attack. Our primary goal is to extend existing solutions to anticipate adversarial behavior in a more fine-grained way. For this, we want to determine the precise parameterization of various attacks in ongoing multi-stage attack scenarios in advance (e.g., the next type of attack, its timing, its source and the targeted services). To achieve this, the project will cover the following tasks:

- Data acquisition and analysis of multi-stage attack scenarios
- Application of different machine learning techniques (HMMs, ANNs, Bayesian networks)
- Design and implementation of fine-grained prediction mechanisms

The details of this topic can be discussed individually. Just contact us at the initial PdF meeting (poster session) or send as a mail (see below).

PREREQUISITS

- A background or strong interest in machine learning
- Basic knowledge of communication networks (Telematik, EiR)
- Familiarity with at least one programming language

Advisor: Hauke Heseding, Robert Bauer
E-mail: hauke.heseding@kit.edu
Phone: 608-46403
Building Kaisterstaße 40, room 3.07