Secu & IA – Project

Year : 2021-2022
Lecturer : Pierre Parrend

Project objectives

The goal of the project is to design, deploy and evaluate a data chain for the analysis of cybersecurity data. The data treatment will be performed as batch.

Choose the objective of your analysis:

- Objective 1
  - Anomaly detection for tracking attacks
- Objective 2
  - Adversarial attacks against classification

Choose the dataset to analyse among Cybersecurity Datasets for core networks:

- The UGR'16 Dataset
  - Data: https://nesg.ugr.es/nesg-ugr16/index.php
  - Scientific paper: https://nesg.ugr.es/nesg-ugr16/dataset_AuthorVersionFinal.pdf
- The Mawi dataset. Use exports from 3/3/2022 and 4/3/2022
  - https://mawi.wide.ad.jp/mawi/samplepoint-F/2022/202203031400.html
  - https://mawi.wide.ad.jp/mawi/samplepoint-F/2022/202203041400.html
  - Scientific paper: http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/08-Fontugne.pdf

Deliverables

The deliverables are:

- Analysis notebook, shared on google collab
- Analysis report (20 pages)
- Final oral group presentation (10 min) + demonstration (5 min)

Your report will present the detailed specification and implementation details on:

- The complete deployment of the data handling chain (including classification + anomaly detection)
- Characterization of the dataset under study
- Benchmark of 3 complementary analysis algorithms
- Conclusions about cybersecurity events in the dataset

The oral presentation is a security analysis review based on the report.

Specifications

The data handling chain will comply with following requirements:



The choice of the dataset, the design of the data handling chain as well as the choice of the analysis algorithm is part of the work.