Karlsruhe Institute of Technology

ENERGY LAB 2.0

Earliest start: 08.07.2025

Institute for Automation and Applied Informatics (IAI)

Bachelor‘s Thesis

Universal system audit and log data conversion into correct DARPA TC Engagement CDM records

The de-facto standard datasets for evaluating APT attack detection approaches are the DARPA Transparent Computing (TC) Engagement 3 and 5 datasets. Many attack detection approach implementations are evaluated using these datasets and thus feature a parser for this specific data format. The DARPA datasets themselves however are discussed critically, prompting the need for new, realistic APT attack datasets.

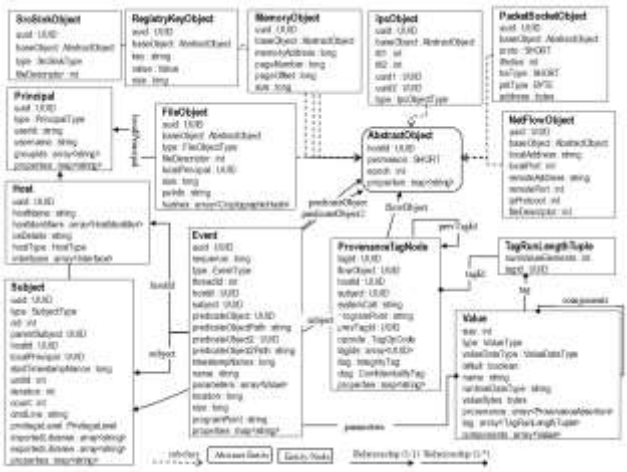
To provide a compatibility layer and enable the evaluation of detection approaches, we want to convert the raw audit log data from our cyber range dataset to the DARPA CDM data format. This will not only increase the compatibility of our dataset with other APT detection projects but also enable other researchers to convert their datasets to this established format.

Main Tasks:

- Familiarization with the TC Engagement datasets, their data format, existing code and auditing systems for Linux and Windows
- Evaluating the use and benefit of ML for data extraction, conversion and validation
- Implementation of a data conversion utility
- Evaluation of the of the converted data

Education, experience and skills:

- Studies in Computer Science
- Python, C++ or Java programming skills
- Basic understanding of bash and Python
- Basic understanding of machine learning and data types
- Basic knowledge of system calls and network traffic



Khoury et al. *An Event-based Data Model for Granular Information Flow Tracking*, 2020

What we offer:

- Possibility of contributing to scientific publications
- Close supervision
- Thesis in English or German possible
- Opportunity to work with machine learning models and research data
- Student assistant position or familiarization period possible

Richard Rudolph
Robust Secure Automation (RSA)
E-mail: richard.rudolph@kit.edu

Institute for Automation und Applied Informatics (IAI)
Karlsruhe Institute of Technology, Campus North
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen