Karlsruhe Institute of Technology

ENERGY LAB 2.0

Institute for Automation and Applied Informatics (IAI)

Bachelor's / Master's Thesis

Creation of realistic benign behavior for cyber range VM clients with ML methods

To detect attacks from advanced persistent threats (APT), researchers require data of such attacks to analyse them and subsequently develop detection methods. The emulation and recording of realistic APT attacks requires a flexible infrastructure to accommodate for the changing needs of different APT attack scenarios.

Our cyber range, working title attack range open stack (AROS), is such a flexible infrastructure. Using Ansible, Terraform and OpenStack, we are able to provision and setup code-defined infrastructures in an automated and repeatable manner. With our cyber range, we implement and recreate known APT attacks to create datasets and research APT attacks and detection approaches. For this, we create a target infrastructure and execute a real cyber attack, which is then recorded thoroughly.

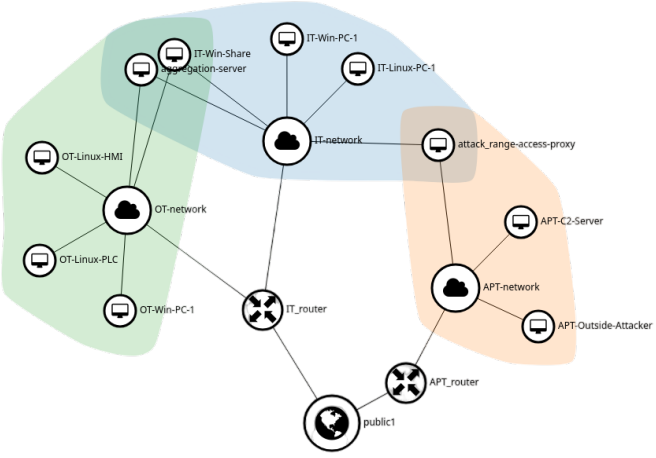
Main Tasks:

- Evaluate different methods to create benign behavior
- Evaluate the use of ML and AI agents
- Create working prototype to generate live benign behavior in VMs with a given profile and time constraint or until stopped
- Ensure the prototype works with our cyber range
- Evaluate your work against other solutions

Education, experience and skills:

- Studies in Computer Science or adjacent
- Basic understanding of machine learning
- Basic knowledge of operating systems, system calls and network traffic

What we need is a method to automatically generate realistic, normal / benign behavior for all our hosts. The generated behavior has to feature a significant variance, so learning algorithms cannot easily detect our benign behavior as a repeating pattern. It has to manifest in network communication and OS logs and system calls. This can be usual office PC uses, web browsing, etc.



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 familiarisation period possible

Richard Rudolph
Robust Secure Automation (RSA)
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