Karlsruhe Institute of Technology

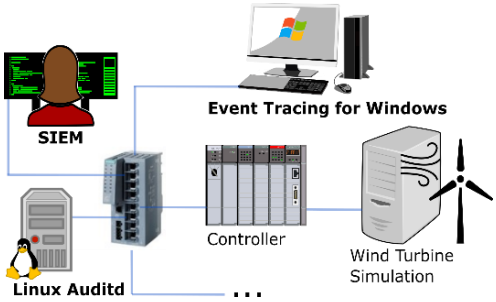
ENERGY LAB 2.0 Security Lab

Institute for Automation and Applied Informatics (IAI)

Earliest start: now

Master Thesis / HiWi

Fine-grained Provenance Graph-based Intrusion Detection on an Engineering Workstation



Background: The most dangerous attackers for critical infrastructures are the so-called Advanced Persistent Threat (APT) actors who often employ low and slow strategies with many system built-in tools[1]. Provenance graph constructed from system audit logs provides a high visibility of the internal workings of a modern computing system, hence it is traditionally used for forensic analysis on compromised devices. In the recent years, it gradually proves to be very promising also for real-time detection of APT actors.

However, to make provenance graph-based detection more practical and therefore really usable in industry, new ideas are still needed to address some issues like high performance overhead. With this proposed master thesis, we aim to make a contribution to it by solving a selected concrete problem, e.g., dependency explosion problem. The experimental devices are provided in our security lab (see the figure above).

Tasks:

- Literature review of major cyber-attacks, and common intrusion detection methods
- Get familiar with tools/frameworks for collecting system audit logs and constructing provenance graphs
- Come up with some new ideas about how to automate/optimize the entire workflow or a specific building block of provenance graph-based intrusion detection
- Implement and evaluate those new ideas

Benefits: Given the complexity of the problem, the student can first work as a HiWi for up to 6 months, if desired, and then continue the work as a master thesis. Throughout the work, the supervisor will work very closely with the student, to ensure that the student can deliver a thesis with good quality at the end. At the beginning (1-2 months), the supervisor will spend a reasonable amount of time to teach, guide and support the student with the appropriate materials. In this case, the student does not have to spend/waste lots of time for finding the appropriate literature. At the end, the student should have a solid understanding of cyber-attacks and common detection methods, and practical experience in researching on intrusion detection systems etc., which are a competence strongly desired by both security industry and academia.

Requirements: Highly motivated; knowledge and experience of data analysis; basic programming skills; adequate understanding of operating systems and network communication.

1. Q. Liu et al. 2022. Binary Exploitation in Industrial Control Systems: Past, Present and Future. *IEEE Access*, *10*, 48242 - 48273.

Contact: Qi Liu
Group: Robust Secure Automation (RSA)
Phone: +49 721 608-23973
E-mail: qi.liu@kit.edu

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