Karlsruhe Institute of Technology

Institute for Automation and Applied Informatics (IAI)

ENERGY LAB

Student work (HiWi)

Dataset Annotation for Provenance-Based Intrusion Detection and Investigation Research

Tasks:

- **Preparation:** Get familiar with the target dataset **AVIATOR** [1]
- **Data Annotation:** Perform fine-grained ground truth labelling on system activity logs according to predefined guidelines, e.g. [2], for intrusion detection and investigation research.
- **Quality Assurance:** Review and validate annotated data to ensure consistency and high quality.
- **Documentation:** Maintain clear records of annotation processes, challenges, and feedback for research teams.
- **Tool Support:** Assist in refining annotation tools and methodologies for provenance-based analysis.

Advisor:
Qi Liu

Required skills (Wish list):
- Basic understanding of cyber attacks
- Adequate understanding of operating systems
- Familiarity with security events is a plus

Language(s):
English

Starting date:
As soon as possible

For more information, please contact:

Qi Liu
Phone: +49 721 608 23973
E-Mail: qi.liu@kit.edu

Interested students are welcome to send me your CV and transcript of records.

References
[1] Qi Liu, Kaibin Bao, and Veit Hagenmeyer, “AVIATOR: A MITRE emulation plan-derived living dataset for Advanced Persistent Threat detection and investigation”, in Proceedings of 2024 IEEE International Conference on Big Data.
[2] Jason Liu, Adil Inam, Akul Goyal, Kim Westfall, Andy Riddle, and Adam Bates. Reapr: Recovery every attack process. https://bitbucket. org/sts-lab/reapr-ground-truth, 2023.

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