Karlsruhe Institute of Technology


Institute for Automation and Applied Informatics (IAI)

Earliest start: now

Bachelor or Masterthesis

Large Language Models solving Capture The Flag Challenges in the context of Critical Infrastructure

The emergence of powerful Large Language Models (LLMs) raises questions about their potential capabilities in offensive security scenarios. This research explores these capabilities in a controlled environment using with Capture The Flag (CTF) challenges, particularly focusing on critical infrastructure contexts. Understanding how LLMs can reason about and execute security exploits is crucial for future security assessments and defensive strategies. The thesis involves collecting and designing suitable CTF challenges and developing a framework to systematically assess how LLMs approach and solve these security challenges through tool interaction and autonomous reasoning.

Master's students are free to use our high-performance computer clusters for the work on their theses.

Tasks

- Create specialized CTF scenarios focusing on critical infrastructure systems
- Utilizing State of the Art LLM-based agents capable of attempting these CTF challenges
- Benchmark and analyze LLM performance in solving security challenges

Requirements

- Studies in MINT field
- Programming and Machine Learning experience
- Basic knowledge of LLMs and prompt engineering
- Experience with Docker/Ansible is preferred

Interested? Then please send an e-mail with your resume and transcript of records. Contact: gustav.keppler@kit.edu

Gustav Keppler
Secure Energy System
E-mail: gustav.keppler@kit.edu

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