YIFAN LIAO

Research Interests: AI4security & ADS testing

personal web
lyf1998118@gmail.com
+86 17754927977
github
Chongqing, China
Linkedin

BIO

I'm a research assistant at NUS Research Institute in Chongqing, where I am supervised by Prof. Huang Zhiyong. I obtained my M.Comp. in Artificial Intelligence at National University of Singapore (NUS). Before Joining NUS, I received my B.Eng. in Mechanical Engineering at Chongqing University (CQU) in 2021.

SKILLS

Languages: Python, JavaScript, Java, HTML.

Technologies: Linux, Docker, Kubernetes.

PROJECTS

Web Security

Detect and Explaining Tamper-based attacks — **Still reviewing**

This project detects and explains attack-induced anomalies in web applications by learning behavioral normalities during runtime, modeling them with first-order logic, and generating executable Python scripts, leveraging LLMs in the learning process to enhance detection and explanation.

Cyber Security

Learning Verifiable Invariant to Detect Evasive Intrusion Attacks — **Still reviewing**

This project addresses the pressing concern of Advanced Persistent Threat (APT) attacks by proposing Refuter, an advanced intrusion detection technique. Refuter identifies disguising processes in APT attacks by leveraging emerging language models' agents to construct normal behavioral invariants of system processes. It raises intrusion alarms based on inconsistencies between a target program's behaviors and its claimed process intentions.

ADS Testing

Boost the Fuzzers of ADS through Explanation-driven and Diversity-enhancing — **Project Webpage**

This project addresses the need for a diversity-driven and explanation-oriented solution by introducing DivX, which enhances existing ADS fuzzers. It achieves this by discovering diversified failures across different driving scenarios and deriving actionable explanations. These explanations help summarize failure patterns, generate test cases, and provide runtime remedies to avoid potential accidents.

EDUCATION

9/2021 - 6/2023 **Master, National University of Singapore (Supervisor: Prof. JS Dong)** — **Artificial Intelligence**

Thesis: Boost the Fuzzers of ADS through Explanation-driven and Diversity-enhancing
GPA: 3.5/5

6/2020 - 6/2021 **Visiting student, University of Cincinnati** — **Mechanical Engineer**

GPA: 3.67/4

9/2016 - 6/2021 **Bachelor, Chongqing University** — **Mechanical Engineer**

GPA: 3.38/4

EXPERIENCE

6/2023 – 6/2024 **Research Assistant (P.I: Prof.Yang Liu)** — **Singapore Govtech**

- Lead a web security project, developing a comprehensive end-to-end web tamper detection toolset.
- Assisted in a system log detection project by building the evaluation platform through investigating and running log detection algorithms (DeepLog, LogAnomaly, Logrobust, etc.) and several CVE PoCs.

`Web Security / LLM for Security / Log Detection`

12/2022 – 6/2023 **Research Intern (P.I: Dr. Hoon Wei Lim)** — **NCS Group (Singtel's Subsidiary)**

- Assist in a cyber security project by participating in experimental deployment through researching and running APT29 attacks, as well as running tasks involving disguising processes.

`APT Attack Detection / LLM for Security`

12/2019 – 6/2020 **Robotics Intern** — **Chongqing Kaibao Robotic Company**

- Apply the extended Kalman filter to obtain accurate sensor data for robot navigation

`Robotics / Matlab`

SERVICES

PRDC 2023 (Chair: Prof.JS Dong) - Program Committee

LANGUAGES

English - Fluent, **Chinese** - Native