Curriculum Vitae

Arastoo Zibaeirad
azibaeir@uncc.edu

RESEARCH INTEREST

My primary research interests center on the intersection of cybersecurity and software engineering, with a focus on the security of Large Language Models. I am particularly interested in testing and applying these models to enhance cybersecurity measures and improve software systems. While my main focus is on securing LLMs, I also have a keen interest in adversarial machine learning, specifically in making AI models more explainable, interpretable, and robust in adversarial settings. This secondary focus on the interpretability and explainability of AI complements my broader goal of advancing AI security across various domains.

EDUCATION

University of North Carolina at Charlotte, USA — Aug 2023 - present
Ph.D. in Computer Science

University of North Carolina at Charlotte, USA — Aug 2022 - Anticipated Dec 2024
M.Sc. in Computer Science
- Thesis title: Automatic Benchmarking Large Language Models for Software Vulnerability Detection and Patching

Iran University of Science and Technology, Iran — Aug 2014 - Mar 2019
B.Sc. in Electrical Engineering
- Thesis title: Adaptive Full-Duplex Real-Time Temperature Monitoring and Control System

HONORS AND AWARDS

University of North Carolina at Charlotte Graduate Scholarship (Full Tuition Award), USA 2023
New Mexico State University Graduate Scholarship (Full Tuition Award), USA 2022
Huawei ICT Competition, Huawei HQ, CN 2018
- Won 1st prize in Huawei's global competition on Network Routing, Switching, and Security, held at Huawei's Headquarters in Shenzhen, China.
Iran Univesity of Science and Technology Undergraduate Scholarship (Full Tuition Award), IR 2014

RESEARCH AND TEACHING EXPERIENCE

University of North Carolina at Charlotte, USA — Jan 2024 - present
Computer Science Researcher

- Developed an automated framework for evaluating large language models in software vulnerability detection and patching, integrating novel data collection methods and automated evaluation metrics to improve accuracy and reliability in real-world codebases.

- Developed generative adversarial models to simulate and launch DDOS attacks, effectively testing and evaluating the resilience of black-box machine learning models.

University of North Carolina at Charlotte, USA — Aug 2023 - May 2024
Teaching Assistant

- Assisted in teaching two courses: IT Infrastructure and Security (ITIS-3246) and Network Security (ITIS-8167).

- Provided support to students with their lab work in Linux, networking, and security.

- Facilitated a deeper understanding of course material through one-on-one and group tutoring sessions.

New Mexico State University- Collaborated with DoE, USA Aug 2022 - Aug 2023
Computer Science Researcher

- Worked on detecting and mitigating cyber and cyber-physical system attacks using various techniques, including game theory, graph theory, blockchain, and machine learning.

- Worked on the explainability and interpretability of black-box DDoS detection systems.

New Mexico State University, USA Aug 2022 - Dec 2022
Teaching Assistant

- Assisted in teaching Operating System course (CS 474)

PROFESSIONAL EXPERIENCE

Golrang System Tehran, Iran Mar 2022 – Aug 2022
Software Developer
Golrang System is a leading holding company with a diverse portfolio that includes software products and networking solutions.

- Implemented an automated system using PingCastle to efficiently detect and manage folder sharing in Active Directory, enhancing overall security.

- Developed a tool to aggregate information on software and security system versions, integrating it with the CVEdetails API to check for up-to-date status and display results for continuous monitoring and security assurance.

Andisheh Negar Pars Tehran, Iran May 2019 – Mar 2022
Researcher & Software Developer
Andisheh Negar Pars specializes in delivering security solutions and network infrastructure services to a variety of companies, focusing on innovative and robust security measures.

- Led the development and integration of security software for Incident Response in an enterprise-level, distributed, and private SIEM environment, successfully completing a large project on historical event correlation and integrating projects such as MISP, TheHive, and Cortex.

- Implemented advanced log sequencing and developed a log management application using NoSQL Elasticsearch, integrating Event Query Language (EQL) and Domain Specific Language (DSL) to enhance anomaly detection and incident alerting.

- Conducted in-depth research on open-source and commercial security solutions including ELK stack, Elastalert, MISP, Sagan, TheHive, Cortex, and User & Entity Behavior Analytics (UEBA), resulting in the development of an advanced open-source application for event correlation and incident alerting.

- Customized detection rules based on the MITRE ATT&CK framework, integrated multiple security tools using APIs with Django Rest Framework, and optimized Elasticsearch and Logstash performance, significantly enhancing the application's logging and alerting capabilities while managing an Elasticsearch cluster using Docker.

PUBLICATIONS

1. **Zibaeirad, A.**, Koleini, F., Bi, S., Hou, T., & Wang, T. (2024). A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities. *arXiv preprint* arXiv:2407.07966.

2. **Zibaeirad, A.**, & Vieira, M. (2024). SysLLMEval: A Comprehensive Benchmarking Framework for Evaluating Large Language Models in Software Vulnerability Detection and Patching. *Submitted to ACM International Conference on the Foundations of Software Engineering (FSE) 2025*.

LEADERSHIP AND VOLUNTEER ACTIVITIES

Student Scientific Association (Iran University of Science and Technology) 2016 - 2017
President

- Organize and conduct annual conferences, workshops, and extra curriculum classes to promote the latest advancements in electrical engineering.
- Coordinate collaborative projects with industry partners to provide hands-on experience for students.

Innovation and Research Club (Iran University of Science and Technology) 2017 - 2018
Technical Lead

- Manage club communications, schedule meetings, and maintain accurate records of all club activities and decisions.
- Coordinate administrative tasks, handle correspondence, and assist in organizing events and projects to ensure smooth club operations.