ABANISENIOLUWA KOLAWOLE OROJO

Waco, TX | b.korojo@gmail.com | (254) 400-5915
github.com/AKOrojo | linkedin.com/in/abaniseorojo | Google Scholar
ORCID: 0009-0005-9448-1929 | LaBackDoor Lab

Research Profile

Computer Science Ph.D. candidate working at the intersection of **artificial intelligence and security**, with a focus on **AI-driven threat detection, adversarial robustness, and the security of AI systems and the critical infrastructure they touch**. I build agentic Large Language Model (LLM) systems for autonomous vulnerability discovery and remediation, develop ML models for attack prediction, and study how access control and network protocols hold up under adversarial conditions. Published author (*USENIX Security* under review, ACSAC, IEEE, ACM, Springer) and strong programmer in **Python, Rust, and C/C++**. I intend to continue working on the defensive AI-security problems that determine whether advanced AI is deployed safely, and to help build lasting Black leadership in this field.

Education

Baylor University — **Expected Dec 2027**
Doctor of Philosophy in Computer Science — *Waco, TX*

- Advisors: Dr. Pablo Rivas and Dr. Erika A. Leal
- Focus: AI-driven cybersecurity, AI/LLM system security, threat detection, network-protocol security, distributed access control
- Affiliated Labs: LaBackDoor Cybersecurity Research Lab, Baylor Multimedia Lab

Baylor University — **Expected Aug 2025**
Master of Science in Computer Science — *Waco, TX*

Webster University — **July 2022**
Master of Science in Cybersecurity — *St. Louis, MO*

- Thesis: "Navigating the Digital Maze: Exploring the Intersection of Social Media, Privacy, and Security"

Webster University — **May 2020**
Bachelor of Science in Computer Science, Minor in Management — *St. Louis, MO*

- **Valedictorian**, Undergraduate Class of 2020

AI & Security Research Experience

Baylor University — LaBackDoor Cybersecurity Research Lab — **June 2023 – Present**
Graduate Research Assistant — AI & Systems Security — *Waco, TX*

- **Agentic AI for autonomous security (primary research):** architected **Autopatch**, an agentic LLM system that autonomously discovers, remediates, and verifies infrastructure vulnerabilities end to end via a six-agent LangGraph pipeline, with a policy-gated, signed execution sandbox (command allowlists, risk scoring) wired to OpenVAS/Trivy/Nuclei and NVD/EPSS/CISA-KEV feeds. Released **SysRepair-Bench**, the companion evaluation benchmark. (*USENIX Security 2026*, under review.)
- **ML for threat detection & adversarial robustness:** developed a Multi-Recurrent Neural Network (MRN) in PyTorch for time-series forecasting of software-vulnerability trends, achieving a **32.78%** improvement over ARIMA and LSTM baselines.
- **LLMs for network defense:** engineered **ByteFlow**, a byte-level LLM (T5/LLaMA) for deep packet inspection and automated network-traffic intelligence, and **TrAice**, a distributed Python system for high-volume PCAP analysis across TCP/IP and DNS.
- **Securing AI training data at scale:** led data collection and design of a language-model framework over a **250,000-message** corpus to surface reliable firsthand accounts from adversarial, real-world conflict-zone data (ASONAM 2024).
- **Access control & threat detection:** architected **AW-TRBAC**, a dynamic access-control framework for large-scale distributed NoSQL databases with node-identity management and data anonymization, and integrated it with semantic variational autoencoders for dynamic threat detection.
- **Critical-infrastructure security:** designed **MAADER**, a cyber-physical testbed combining emulation, simulation, and physical components to analyze attacks on critical infrastructure; automated provisioning of **30+** reproducible virtualized security-lab environments using Terraform, Ansible, and Proxmox.

Micro1 — **2025 – 2026**
Cybersecurity AI Trainer (Part-time, Remote) — *Remote*

- Author training data and evaluation benchmarks for security-focused LLMs, covering exploit analysis, alert triage, incident-response playbooks, and adversary-behavior characterization.

Apex Ezone — **Aug 2021 – Dec 2022**
Security Engineer Intern — *United Kingdom (Remote)*

- Cut phishing incidents **40%** and incident-response time **30%** through automated OSINT workflows; ran continuous Splunk SIEM monitoring and Nessus/Nmap vulnerability assessments to harden TLS/SSL configurations.

Selected Publications

Under Review

6. **A. Orojo**, et al. "An AI-Driven Agentic System for Automated System Patching." Submitted to *USENIX Security Symposium*, 2026.

Peer-Reviewed

5. **A. Orojo**, E. El-Mahmoud, E. A. Leal, P. Rivas. "ByteFlow: A Byte-Level LLM for Deep Packet Inspection and Network Intelligence." *WAITI Workshop, ACSAC '25*, IEEE, pp. 357–365, 2025. DOI: 10.1109/ACSACW69556.2025.00046.

4. **A. Orojo**, E. El-Mahmoud, S. Hutton, et al. "A Unified Framework Incorporating AW-TRBAC and Semantic Variational Autoencoders for Dynamic Threat Detection and Access Control." *International Conference on Artificial Intelligence (ICAI '25)*, 2025.

3. **A. K. Orojo**, W. C. Elumelu, O. O. Orojo. "Predicting Software Vulnerability Trends with Multi-Recurrent Neural Networks: A Time Series Forecasting Approach." *1st Intl. Conf. on NLP & AI for Cyber Security (NLPAICS '24)*, ACL, pp. 42–47, 2024.

2. **A. Orojo**, E. El-Mahmoud, G. Speegle. "Assessing the Impact of Access Control Policies on Data Accessibility in Distributed NoSQL Environments." *Intl. Conf. on Security & Management (SAM '25)*, 2025.

1. **A. Orojo**, P. Bhagat, J. Wilburn, M. J. Donahoo, N. Vishwamitra. "Leveraging Secure Social Media Crowdsourcing for Gathering Firsthand Account in Conflict Zones." *IEEE/ACM ASONAM 2024*, Springer LNCS vol. 15212, pp. 160–170, 2025. DOI: 10.1007/978-3-031-78538-2_14. (NSF Grant No. 2245983.)

Full publication list (incl. MHV '26, BEARS/ICAI '25, technical reports) available on Google Scholar and DBLP.

Technical Skills

AI / ML:	PyTorch, TensorFlow, Scikit-learn, LLMs (LLaMA, T5, GPT), agentic systems (LangGraph), deep learning, time-series forecasting, threat-detection modeling
Languages:	Python, Rust, C/C++, Go, Java, Bash, SQL, JavaScript, TypeScript
Security:	Threat detection & modeling, adversarial ML, applied cryptography, reverse engineering, malware analysis, IDS/IPS, SIEM (Splunk), Nessus, Nmap, OpenVAS, secure SDLC
Systems / Infra:	OS & kernel internals (Linux, Windows, macOS), distributed systems, Docker, Kubernetes, Terraform, Ansible, Proxmox, CI/CD, OPA
Networking:	TCP/IP, DNS, BGP, QUIC, TLS/SSL, PKI, HTTP/2, PCAP analysis, Wireshark
Data:	PostgreSQL, Redis, MongoDB, NoSQL, Hadoop HDFS, Spark

Selected Open-Source Research Software

SysRepair-Bench (*Python, LLM evaluation, agentic systems*) — benchmark suite for evaluating LLM-based agents on autonomous vulnerability discovery, remediation, and patch verification across real-world software. [repo]

Stackforge (*Rust, Python*) — high-performance, modular networking stack and automata framework with native Python bindings; self-directed. [repo]

DDoS Attack Simulation Framework (*Terraform, Ansible*) — infrastructure-as-code framework that replicates adversary techniques in controlled environments to validate detection and mitigation. [repo]

Secure Crowdsourcing Dataset (*Python*) — 250,000-message Telegram corpus supporting the ASONAM 2024 publication on crowdsourced intelligence in conflict zones. [repo]

Teaching, Mentorship & Leadership

Director — Cybersecurity Summer Camp **Summer 2023, 2025**
Central Texas Cyber Range, Baylor University *Waco, TX*

- Developed and directed the cybersecurity training curriculum, achieving a **90%** increase in participants' threat-awareness and prevention understanding; supported industry training on AI, security, and cyber-physical systems.

Coach & Former Team Lead — CCDC **2023 – Present**
Collegiate Cyber Defense Competition, Baylor University *Waco, TX*

- Coach Baylor's cyber-defense competitors in live blue-team defense against a professional red team, following two years as team lead.

Teaching Assistant — Data Communications **Jan – May 2023**
Baylor University *Waco, TX*

- Mentored 30+ students in TCP/IP networking, routing protocols, DNS, and data-communications principles.

Honors & Certifications

Honors: SWCCDC Regionals — 2nd Place (2025), 3rd Place (2024) · National Cyber League — Top 30 nationally (∼475 teams, 2020–2024) · Undergraduate Valedictorian (2020).

Certifications: CompTIA Cybersecurity Analyst (CySA+) · SOC Analyst Level 2 · MITRE ATT&CK (RangeForce) · LPI Linux Essentials.

Academic & Professional Profiles

Google Scholar | ORCID | DBLP | ACL Anthology | ResearchGate | OpenReview