

Abanisenioluwa K. Orojo

Waco, TX | b.korojo@gmail.com | labackdoor.com | linkedin.com/in/abaniseorojo | github.com/LaBackDoor

Carrer Profile

Highly motivated cybersecurity professional with a robust blend of research, practical security engineering, and DevSecOps expertise. Experienced in simulating advanced cyber attack vectors, designing secure containerized infrastructures, and integrating machine learning techniques for threat forecasting. Proven track record in developing secure microservices architectures, implementing rigorous vulnerability assessments, and architecting comprehensive access control frameworks across cloud and cyber-physical systems. Passionate about leveraging cutting-edge technologies to enhance security operations and mitigate emerging threats in dynamic environments.

Experience

CyberSecurity AI Trainer, micro1 – Remote Dec 2024 – Present

- Simulated over 10 cyber attack vectors on large language models in a Docker-based VM environment, identifying and mitigating up to 85% of targeted vulnerabilities.
- Designed and maintained secure Docker setups that reduced environment deployment time by 30%, ensuring consistent and reproducible cybersecurity simulations.
- Compiled comprehensive technical reports quantifying discovered vulnerabilities and implementing strategic mitigation measures, improving AI system resilience by 60%.

Cybersecurity Research Assistant, Baylor University – Waco, TX Jun 2023 – Present

- Developed and demonstrated a novel approach using Multi-Recurrent Neural Networks (MRNs) for superior time-series forecasting in cybersecurity, outperforming traditional models by 32.78% with fewer parameters.
- Successfully organized and led a cybersecurity summer camp, imparting key cyber threat awareness and prevention strategies to 30 students, increasing cybersecurity literacy by 90%.
- Provisioned over 30 cybersecurity labs using Proxmox, Ansible, and Terraform, streamlining practical training and enhancing technical skill development.
- Developed **TrAice**, a tool leveraging LLMs (e.g., Llama3) for analyzing network traffic data from PCAP files and log files, improving cybersecurity education and detection capabilities.

Security Coordinator, Apex Ezone – Remote Aug 2021 – Present

- Architected Django-based microservices for an eSports training and fantasy betting platform, implementing PostgreSQL for structured data management and Redis for caching and messaging.
- Strengthened organizational security by monitoring and analyzing threats using IDS and SIEM tools, conducting log analysis with Splunk, and performing vulnerability assessments with Nessus and NMAP.
- Investigated phishing emails, domains, and IPs using open-source tools, reducing phishing incidents by 40% and improving incident response times by 30%.
- Rescanned and recommissioned mitigated systems to ensure network stability while continuously researching emerging threats and vulnerabilities.

Education

Baylor University, Waco, TX, USA January 2023 – December 2025
Doctor of Philosophy in Computer Science

- GPA: 3.53/4.0, **Specialization:** Major in Computer Science

Webster University, Saint Louis, MO, USA May 2021 – August 2022
Master of Science in Cybersecurity

- GPA: 3.83/4.0, **Specialization:** Combined Major in Cybersecurity

Webster University, Saint Louis, MO, USA October 2017 – May 2020
Bachelor of Science in Computer Science, Minor in Management

- GPA: 3.54/4.0; CS-only: 4.0, **Specialization:** Combined Major in Computer Science and Minor in Management

Publications

Leveraging Secure Social Media Crowdsourcing for Gathering Firsthand Account in Conflict Zones , A. K. Orojo et al. (ASONAM '24)	2024
Predicting Software Vulnerability Trends with Multi-Recurrent Neural Networks: A Time Series Forecasting Approach , A. K. Orojo et al. (NLPAICS '24)	2024
A Unified Framework Incorporating AW-TRBAC and Semantic Variational Autoencoders for Dynamic Threat Detection and Access Control , A. K. Orojo et al. (DCS-Water '24)	2024
Access Control Evaluation in Distributed NoSQL Environments , G. Speegle, A. K. Orojo et al. (SACMAT 2025) (Under Review)	2025
AI-Driven Cybersecurity: Fine-Tuned LLMs for Packet-Level and Multi-Modal Network Traffic Analysis , A. K. Orojo et al (NeurIPS 2025) (Under Review)	2025

Projects

Quantum Safe Zero Trust Security for Cyber-Physical Systems with Post-Quantum OpenZiti	LaBackDoor/Post-Quantum
<ul style="list-style-type: none">Designed and implemented a quantum-safe version of OpenZiti for Cyber-Physical Systems (CPS) to mitigate risks posed by quantum-enabled adversaries.	
PANACEA - Policy Analysis and NoSQL Access Control Evaluation Approach	LaBackDoor/PANACEA
<ul style="list-style-type: none">Developed a fine-grained access control system for NoSQL databases, applying policies and generating dynamic access control views.	
DDoS Attack Simulation Framework	LaBackDoor/DDos-Attack
<ul style="list-style-type: none">Built an automated research framework for simulating Distributed Denial of Service (DDoS) attacks in a controlled environment.	
HTTP2 MegEx: Client and Server Implementation (Java)	AKOrojo/Http2_Megex
<ul style="list-style-type: none">Developed a comprehensive implementation of HTTP/2 protocols based on RFC7540, including both client and server components.	
Packed Malware Analysis Using Hardware Performance Counters	
<ul style="list-style-type: none">Conducted research under Dr. Eric Leal on the feasibility of malware unpacking via hardware-assisted loop profiling. Employed hardware performance counters to analyze packed malware, contributing to improved malware detection techniques. Findings and publications available at Google Scholar.	

Technologies

Languages: Python, Java, JavaScript, TypeScript, SQL, Bash, YAML, Go, Terraform HCL

Technologies: Docker, Kubernetes, OpenZiti, Proxmox, vSphere, Redis, PostgreSQL, MongoDB, Django, Flask, FastAPI, Ansible, Terraform, Splunk, Nessus, NMAP, IDS/IPS, SIEM, OpenSSL, LibOQS, PQ Crypto, Hadoop, Spark, Pandas, NumPy

Cybersecurity Tools: Burp Suite, Metasploit, Wireshark, OSINT tools, Snort, Suricata, TrAice (custom network analysis tool), AW-TRBAC framework, NoSQL access control evaluation systems

Machine Learning & AI: PyTorch, TensorFlow, Scikit-learn, BERT, LLMs, NLP-based cybersecurity tools

Certifications

HashiCorp Terraform Associate (003), CompTIA Security+, CompTIA Network+, Microsoft Certified: Azure Fundamentals, Microsoft Certified: Azure Security Engineer Associate