David L. Adei

Doctoral Student • Department of Computer Science • North Carolina State University

Website: lokingdav.github.io — Email: lokingdav@gmail.com — Github: github.com/lokingdav

Professional Summary

My research centers on systems security and privacy-preserving technologies, with a current focus on developing advanced techniques to secure telephone networks, mitigate telecom fraud, and expand the STIR/SHAKEN caller authentication framework. My first PhD paper earned both the *Distinguished Paper Award* and *Distinguished Artifact Award* at the ACM Conference on Computer and Communications Security in October 2024. I am pursuing a PhD following six years of industry experience in software engineering.

Education

1. **Ph.D in Computer Science (CS), North Carolina State University — Raleigh, NC, USA**
   August 2022 - Present — Advised by Dr. Bradley Reaves.
   Relevant Coursework: Cryptography (A+), LLMs In Security (A+), Algorithms Design & Data Structures (A+), Operating Systems Security (A), Cellular and Telephone Networks Security (A), Software Security (B+), Computer & Network Security (B) and Advance Network Security (TBD).

2. **BSc in Computer Science — Kwame Nkrumah Univ. of Science & Technology — AR, Ghana.**
   August 2015 - July 2019
   Bachelor of Science in Computer Science, First Class Honors — Graduated as Best Computer Science Student.

Research Publications

1. **Jäger: Automated Telephone Call Traceback**
   David Adei, Varun Madathil, Sathvik Prasad, Bradley Reaves, Alessandra Scafuro
   Association for Computing Machinery (ACM) Conference on Computer and Communications Security (CCS) October 2024
   (1) Distinguished Paper Award · (2) Distinguished Artifact Award

Research Preprints

1. **How to Recover a Cryptographic Secret From the Cloud**
   David Adei, Chris Orsini, Alessandra Scafuro, Tanner Verber
   Available on Cryptology ePrint Archive: https://eprint.iacr.org/2023/1308

Expertise & Skills

Languages:	Python, C++, JavaScript, JAVA, PHP, HTML & CSS
Frameworks:	Node.js, React.js, Vue.js, Express.js, Laravel, Flask
Tools:	Docker, Ansible, Terraform, Git, PostgreSQL, MySQL, MongoDB, Redis, LaTeX
Platforms:	Linux, Web, MacOS, Amazon Web Services, Google Cloud Platform, Trusted Execution Environments
Soft Skills:	Mentoring, Efficient Time Management, Leadership, Problem-Solving, Teamwork, Attention to Detail, Written & Oral Communication

Employment & Experience

1. **Graduate Research Assistant — NC State University — Raleigh, NC, USA.**
   In-Person Aug. 2022 - Present
   - Developed secure cryptographic protocols for privacy-preserving call traceback and a scalable system to process 50,000 call records per second while minimal system resources.
   - Implemented performant Witness Encryption Scheme based on BLS signatures in C++, achieving 200% increase in speed.
   - Implemented credential-less secret recovery protocol using Trusted Execution Environments(TEEs) and blockchain.
   - Implemented a security game with deceptive prompt-injecting attacks on Large Language Models (LLM) to solve cryptographic puzzles.
   - Researched Peer-to-Peer (P2P) networks and distributed systems to enhance performance and security.
   - Technologies: C++, Python, Docker, Bash Scripting, Blockchain, AWS Nitro Enclave, MongoDB, Clickhouse Columnar Database, Large Language Models.

2. **Senior Developer — Scopic Software — Rutland, MA, USA.**
   Remote, Contractual Oct. 2021 - Aug. 2022
   - Implemented web applications for image manipulation, 3D modeling, and data synchronization between Teamwork.com and Jira Cloud with overall 35% increased in client satisfaction.
   - Refactored core modules to improve frontend speed by 56%, reducing page load times significantly.
   - Resolved critical production bugs, reducing server downtime by 48% and bug rates by 36%.
   - Containerized 4 projects with Docker, cutting deployment time by 90%.
   - Upgraded outdated SDKs an API backend to reduce system crashes and increased uptime by 80%.
   - Technologies: Python, PHP, Vue.js, React, Node.js, MySQL, Docker.

3. **Senior Software Engineer — Cmunily — Raleigh, NC, USA.**
   Remote, Contractual Nov. 2020 - Oct. 2021
   - Replaced legacy web app with a cross-platform, offline-first mobile app, improving speed by 26% and user engagement by 48%.
   - Redesigned monolithic ad-matching platform into a microservices architecture, improving scalability by 40%.
   - Technologies: Python, PHP/Laravel, Vue.js, MongoDB, PWA, Apache Cordova, IndexedDB, Docker, JWT, Micro Services.

4. **Software Engineer — Clearcare Solutions Ltd — Stafford, England.**
   Remote, Contractual Nov. 2019 - Oct. 2020
   - Migrated legacy PHP app for 1,000 DAUs to Laravel, improving performance by 630x and increasing DAUs by 23%.
   - Overhauled frontend, enhancing user interface and boosting UX satisfaction by 15%.
   - Technologies: PHP/Laravel, Vue.js, Python, MySQL, Docker, Vagrant.

5. **Senior Software Engineer — W3MSYS Company Limited — Accra, GA, Ghana.**
   Hybrid Jan. 2017 - Nov. 2019
   - Led the development of a nationwide healthcare management system with 1,000 DAUs.
   - Designed a rate-limited Role-Based Access Control microservice handling 10,000 API requests/hour, achieving 99.99% uptime.
   - Managed a team of 3 developers through Agile resulting in 24% increase in team productivity.
   - Technologies: Python, PHP/Laravel, Vue.js, React.js, Node.js, Service Workers, MongoDB, MySQL, Docker.

6. **Software Engineer — Freelancing.**
   Remote, Contractual Sept. 2015 - Jan. 2017

- Collaborated with clients to design tailored software solutions, optimizing business operations.
- Delivered high-impact features across a variety of platforms and technologies.
- Technologies: Python, Java, Laravel, VueJS, ElectronJS MySQL, REST APIs, Node.js, MongoDB, AWS.

Open Source Contributions

1. **Witness Encryption Based on BLS Signatures**
   C++ library with Python bindings. Implements Witness Encryption Scheme (WES) based on BLS Signatures. — https://github.com/wspr-ncsu/BLS-Witness-Encryption
2. **Jäger: Automated Telephone Call Traceback — ACM CCS Distinguished Artifact Award**
   Python implementation of Jäger system components. Integrates Oblivious PRF protocol, Group Signatures, BLS signatures and WES. — https://github.com/wspr-ncsu/jaeger
3. **How to Recover a Cryptographic Secret From the Cloud**
   Python implementation of a cloud-based secret recovery mechanism using blockchain and AWS Nitro Enclave in the presence of a malicious cloud provider. — https://github.com/wspr-ncsu/Secret-Recovery

Awards & Honors

1. **Distinguished Paper Award at ACM CCS 2024**
   Jäger: Automated Telephone Call Traceback — ACM Conference on Computer and Communications Security (CCS), Oct 2024
2. **Distinguished Artifact Award at ACM CCS 2024**
   Jäger: Automated Telephone Call Traceback — ACM Conference on Computer and Communications Security (CCS), Oct 2024

Posters

1. **PrivyTrace: Privacy-preserving trace back/forward of phone calls**
   David Adei, Bradley Reaves
   Network and Distributed System Security Symposium (NDSS), Feb 2023

Volunteer Experience

1. External Reviewer – IEEE S&P 2023
2. Web Development Team Lead – Google Developer Students Club Nov. 2018 - Sept. 2019
3. Research Assistant – Kwame Nkrumah University of Science & Technology Apr. 2017 – May 2019
4. President of Computer Science, Kwame Nkrumah University of Science & Technology Sept. 2017 - Sept. 2018