ALMA RIKA NKEMLA FUDJO

F-1 Visa | +1 (404) 901-5342 | nkemlaalma@gmail.com | https://www.linkedin.com/in/almankemla

EDUCATION

University of California, Berkeley *May 2025 (Expected)*
Masters of Science in Information and Cyber Security GPA: 4.0

Georgia Institute of Technology *May 2023*
Bachelor of Science in Computer Engineering GPA: 3.68
Concentration in Cyber Security and Information Internetwork

EXPERIENCE

Base Rewards Startup | *Volunteer Cybersecurity Consultant* *Aug 2023 – Nov 2023*

- Employed an approach combining research, real-user testing, and continuous refinement to successfully integrate advanced security features in a mobile app
- Introduced and intergrated Multi-Factor Authentication with mobile-based secondary authentication into preexisting application infrastructure improving platform's security

Georgia Tech Research Institute | Secure Hardware Lab | *Research Assistant* *Aug 2022 – May 2023*

- Collaborated with a team to design digital cryptographic hardware with 99% resistance to malicious insertions
- Performed a comprehensive analysis and modified hash algorithms using Python producing mathematical alternatives up to 10 times faster while increasing collision resistance
- Harnessed Python and GTKWave to simulate hash functions on enhanced hardware, ensuring collision resistance contributing to a 15% increase in collision detection efficiency

Rubrik Inc. | *Software Engineering Intern* *Jun 2022 – Aug 2022*

- Developed a robust testing framework in Python for cloud product upgrades, resulting in a 40% reduction in testing time and a 75% increase in test coverage which enabled engineers to write 50% more unit tests
- Instated end-to-end and regression tests, reducing post-release defects by 20% and raising product stability by 15%
- Executed comprehensive code analysis to enforce secure coding practices, securing vulnerabilities in the code and reducing security risks by 30%

Georgia Tech Research Institute | Embedded System Cyber Security Lab | *Research Assistant* *Aug 2021 – May 2022*

- Conducted reverse engineering of a 1.5MB IoT device binary using Ghidra, unraveling data processing and network protocol intricacies, enabling further analysis and insight into firmware operation
- Utilized Universal Radio Hacker (URH) to dissect and decode 1000 Over-The-Air packets, revealing 14 radio frequency protocols' structures and paving the way for future protocol analysis
- Identified and documented 7 previously unknown vulnerabilities in the device's security, including unauthorized remote access and information disclosure issues

SKILLS

Programming: Java, Python, C/C++, Javascript, Assembly Language, VHDL, MATLAB, SQL, PHP, Go, Verilog
Software: IDA Pro, OllyDBG, GNU DeBugger, Universal Radio Hacker, Altera Quartus, ModelSim
Certifications: CompTIA Security+, GIAC Information Security Fundamentals
Tools: Git, WireShark, AWS, Github, Docker, VirtualBox, Burp Suite, MongoDB, ZAP, YARA
Technical Skills: Cloud Security, Reverse Engineering, Network Security, Incidence Response, Malware Analysis, Firewalls

PROJECTS

Static Malware Reverse Engineering *May 2021 – Aug 2023*

- Reverse engineered malware binaries (GreenCat, Michelangelo, etc.) using IDA uncovering critical insights in behavior
- Innovated an IDA Pro plugin to monitor control flow and data dependence each malware samples, leading to a 30% increase in analysis efficiency for malware assessment
- Leveraged Python, and Bash scripting to derive to over 50 custom malware signatures, enhancing threat detection accuracy by 25% in IDA and designed an analysis framework with YARA, resulting in a 40% reduction in analysis time

Advanced System Security for Linux Kernel *Jan 2023 – Mar 2023*

- Devised and integrated a robust kernel module into Linux, utilizing tracepoints and kprobes, enabling advanced monitoring and precise filtering of system calls using C
- Enhanced system security by reducing unauthorized system call occurrences by 30%, contributing to a 15% decrease in system crashes and a 25% reduction in the attack surface
- Achieved less than 2% system resource overhead using dymanic analysis and benchmarking, and fortified system security to prevent replay and DoS attack