Spencer Starks

spencer.starks@live.com | linkedin.com/in/spencer-starks | github.com/Spencer10010 | spencerstarks.com

Education

Georgia Institute of Technology — Atlanta, GA
Master of Science in Cybersecurity — *Graduating Dec. 2025*
- Specialization: Information Security

Georgia Institute of Technology — Atlanta, GA
Bachelor of Science in Computer Science, Overall GPA: 3.9/4.0 — *Graduated Dec. 2024*
- Threads: Systems & Architecture, Info Internetworks

Skills / Courses

Languages: Python, C, C++, Java, Bash, PowerShell, SQL, JavaScript, HTML/CSS, ARM Assembly, Verilog
Courses: Secure Computer Systems, Network Security, Information Security, Information Security Policies, Cybersecurity of Drones, Advanced Operating Systems, Database Design, Systems and Networks, Software Engineering, Enterprise Computing
Tools: Git, Docker, Wireshark, Autopsy, John the Ripper, OpenSSL, Jira, Bitbucket, GDB, CMake, CyberChef, VirusTotal API, UML, SQL Server Management Studio, LaTEX, Jupyter Notebook
Hardware/Platforms: Raspberry Pi, Nvidia Jetson Nano, Linux (Ubuntu, Pop!_OS, Mint), Windows 10/11, MacOS

Experience

Software Engineer - Co-Founder — Aug. 2023 – Dec. 2024
Chunio — *Atlanta, GA*
- Spearheaded an agile startup team in developing a full-stack platform utilizing Django, Next.js, NGINX, and PostgreSQL
- Computed the best laptop choice through a linear combination of its specs and user feedback to provide tailored product choices
- Automated the collection of thousands of laptops to repopulate the database and keep the laptop product listings up to date

Head Teaching Assistant - Data Structures and Algorithms — May 2023 – Dec. 2024
Georgia Institute of Technology, College of Computing — *Atlanta, GA*
- Managed 10 Teaching Assistants, wrote and graded exams, and handled all course logistics for the undergrad and grad sections
- Taught and organized recitations for 30+ students on topics ranging from binary search trees to graph algorithms
- Provided feedback to student's homework focusing on code efficiency and edge case performance
- Coordinated and conducted weekly office hours open to 1,000+ students both in-person and virtually

Full Stack Software Engineer Intern — Aug. 2023 – Dec. 2023
MessageGears — *Atlanta, GA*
- Developed on both the front and back end of the Accelerator application leveraging Java, Angular, and React
- Diagnosed and resolved 20+ bugs and defects in Accelerator through Regression and Functional testing enhancing user experience
- Collaborated with a subteam of 8 utilizing the scrum methodology in daily meetings to enhance development
- Integrated React technologies in Accelerator to transition legacy code based on JSP and Angular within 2 months

Projects

BluSwarm: Swarm Spoofing Detection System | Lead Developer | *C++, BLE, ESP-NOW, NMEA* — Jan. 2025 – April 2025
- Built a multi-device spoofing detection system using ESP32s that compares GPS distances against BLE RSSI-based estimates
- Implemented real-time communication between ESP32s using ESP-NOW and consensus-based logic to identify spoofed GPS
- Integrated phones, laptops, and microcontrollers using custom Python serial interfaces and NMEA protocols for pipelined testing

Browser TLS 1.2 Vulnerability Analysis | Team Member | *Python, OpenSSL, WireShark, Git* — Feb. 2025 – April 2025
- Developed a Python TLS server to investigate variations in certificate validation, cipher negotiation, and mutual TLS support
- Captured and analyzed browser behavior using developer tools and Wireshark along with analyzing TLS Extensions like OCSP
- Evaluated browser reactions to various certificate configurations, including incorrect values, alternative names, and expired certs

Website Penetration Testing Simulation | Analyst | *Python, SQL, OpenSSL, Docker* — Jan. 2024 – March 2024
- Exploited XSS and CSRF vulnerabilities in web apps to execute unauthorized actions and inject malicious scripts
- Conducted SQL Injection attacks on vulnerable websites by manipulating query strings and input fields to access restricted data
- Performed RSA Forgery attacks on cryptographic signatures and exploited Length Extension vulnerabilities in hash functions

Secure File Permission System in Xv6 | Sole Developer | *C, SHA-256, Docker, Git* — March 2024 – May 2024
- Developed a user-space isolation and login system implementing user identifiers, file ownership, and access controls
- Designed secure authentication mechanism using Salt and SHA-256 for password storage resistant to rainbow table attacks
- Applied AES-256 for inter-process communication to enhance the security of transmissions of data across the system