

Peter D. Mora IV

69 Brown St, Box 8461 | Providence, RI 02912 | Phone: (985) 373-8119 | E-Mail: peter_mora@brown.edu |
LinkedIn: linkedin.com/in/peter-mora-iv

EDUCATION

Brown University, *Sc.B. Computer Science - Economics*, 3.8/4.0 GPA Providence, RI | **Expected Graduation May 2027**

Relevant Courses: Intro to Computer Systems, Intro to Computer Systems Security, Software Security and Exploitation, The Basics of Cryptographic Systems, Human Factors in Cybersecurity, Intro to Object-Oriented Programming, Program Design with Data Structures and Algorithms, Single Variable Calculus I & II, Discrete Structures and Probability, Linear Algebra

Awards: Native Forward STEM Scholarship (2x recipient), AFROTC CMLA Scholarship, AFROTC Superior Academic Honors Award (4.0 GPA in a semester)

SKILLS & INTERESTS

Technical Skills: Python (Advanced), Java (Advanced), C (Proficient), Assembly (Proficient), Linux/UNIX (Proficient), SQL (Basic), Reverse Engineering, Penetration Testing, Code Optimization, Machine Learning

Certifications: Google Cybersecurity Specialization, IBM AI Engineering Specialization (with Honors), Fundamentals of Quantitative Modeling, Privacy Law and Data Protection

Interests: Philosophy, Theology, Podcasts, Chess, CTFs

LEADERSHIP EXPERIENCE

Det 340, Air Educ./Training Command, US Air Force, *Deputy Squadron Commander* Worcester, MA | Aug 2023 – Present

- Graduated from AFROTC Field Training, an intense 3-week proving ground for cadets, in June 2025
- Led and mentored small groups under simulated high-intensity scenarios
- Created power point presentations and briefed 50+ cadets and cadre
- Communicated responses/action plans resulting from feedback to cadre and wing staff
- Facilitated wing and squadron level program planning and execution

CYBERSECURITY EXPERIENCE

Secturo, *Account Manager*

Remote | Sep 2025 – Present

- Acted as the primary liaison between clients and cybersecurity specialists to align solutions with evolving threat landscapes.
- Provided clients with insights into emerging security technologies and risk mitigation strategies.
- Partnered with engineering teams to translate client requirements into actionable technical solutions.

Immersive Cyber Education Program, US Air Force, *Intern*

Dayton, OH | July 2025 – Aug 2025

- Participated in a rigorous four-week summer program focused on developing cybersecurity leaders through immersive, hands-on training in cyber offense and defense.
- Completed intensive coursework covering network fundamentals, digital forensics, reverse engineering, industrial control system security, the cyber kill chain, Kali Linux, red teaming, and cyber defense.
- Led a team of eight people in a multi-day capstone "Hackfest" competition, applying cybersecurity skills to build, harden, and defend networks while executing offensive cyber operations.
- Developed critical thinking and technical leadership skills, preparing for future roles in cyberspace operations within the Department of the Air Force.

PROJECTS

Buffer Overflow CTF

Oct 2025

- Exploited ELF32 binaries using techniques such as a NOP sled, null-free shellcode injection, jmp *%esp, ret2libc chaining, canary evasion

Secure, Stateless Dropbox Client in Python

Apr 2025 – May 2025

- Implemented efficient file overwrites and sharing, preserving access by reusing symmetric keys, and securely distributing file access via per-user asymmetric key encryption and metadata HMAC updates.
- Hardened against brute-force, rollback, and pointer tampering attacks via layered integrity checks, signed key exchange, and encrypted metadata validation.

Network Intrusion Detection using Machine Learning

Oct 2024

- Trained a Random Forest Classifier model on the CIC-IDS 2017 dataset, achieving 99.7% accuracy in identifying malicious activity

Malloc Implementation in C

Nov 2024

- Achieved high throughput, 90+ % utilization for malloc, 99% utilization for free, and 60% utilization for realloc