ELAINE ZHU

zhu.lae@northeastern.edu https://elaine.foo Boston, MA

EDUCATION

Northeastern University **Sep 2022 - May 2026**

Bachelor of Science in Cybersecurity and Criminal Justice *Boston, MA*

- Honors: University Honors Program, Dean's List (all semesters), Magna Cum Laude
- Relevant courses: Object Oriented Design, Systems Security, Computer Networks, Programming Languages

PUBLICATIONS

- Longpre, S.*, **Zhu, E.***, Ezell, C.*, Ghosh, A.*, et al. (2026). *FLARE-AI: Flaw Reporting for AI.* International Conference on Machine Learning 2026. https://arxiv.org/abs/2606.31567
- **Zhu, E.**, Coombes, C., Teja, S., & Patterson, D. (2025). *FEEDBOT: Formative Design Feedback on Programming Assignments*. In Proceedings of the 30th ACM Conference on Innovation and Technology in Computer Science Education, 1, 576–582. https://doi.org/10.1145/3724363.3729063
- Khezresmaeilzadeh, T., **Zhu, E.**, Grieco, K., Dubois, D. J., Psounis, K., & Choffnes, D. (2025). *Echoes of Privacy: Uncovering the Profiling Practices of Voice Assistants*. Proceedings on Privacy Enhancing Technologies Symposium, 2, 71–87. https://doi.org/10.56553/popets-2025-0050

* = equal contribution

SELECTED EXPERIENCE

PricewaterhouseCoopers **Aug 2026 - Present**

Cybersecurity Consulting Associate *Boston, MA*

- Engineered a DMZ traffic anomaly detection system by training ML models and leveraging BigQuery and Google SecOps to analyze incoming traffic from 500+ hosts.
- Engineered AI agents to automate third party risk management (TPRM) processes such as assessing third party risks, contract risks, etc.

PricewaterhouseCoopers **Jul 2025 - Dec 2025**

Cybersecurity Consultant Co-op *Boston, MA*

- Conducted due diligence reviews of third-party vendors, analyzing documentation and controls to ensure alignment with regulatory and industry standards.
- Designed intelligent threat hunting agents in Python leveraging machine learning and natural language processing frameworks.

Cybersecurity and Privacy Institute at Northeastern University **Jan 2023 - Present**

Research Assistant *Boston, MA*

- Co-authored publications investigating voice assistants' profiling practices and custom pedagogical tools efficacy.
- Programmed Python scripts to automate processes such as web scraping, improving efficiency by up to 90%.
- Investigating surveillance pricing and price discrimination of food delivery platforms.

Northeastern University **Aug 2024 - Apr 2025; Jan 2026 - Apr 2026**

Teaching Assistant, Content Team Lead *Boston, MA*

- Optimized Racket-based autograder for CS2500, enhancing grading efficiency.
- Collaborated with professor to develop assignments for 500+ students, ensuring alignment with course objectives.
- Conducted lab sessions and office hours, providing technical guidance in Racket programming.

Fidelity Investments **Jun 2024 - Aug 2024**

Cybersecurity Intern *Boston, MA*

- Mapped technologies for Zero Trust Architecture initiative, improving security alignment with ZTA principles.
- Created technical documentation and ML security code using Python libraries including IsolationForest.

SKILLS

Languages: Python, Java, Racket, SQL, HTML, CSS, Bash, Pyret, JavaScript, TypeScript, C

Skills and tools: Wireshark, Ghidra, Burp Suite, Selenium, Linux, penetration testing, reverse engineering

PROJECTS

Landmarkr — October 2025

- Developed a React/TypeScript game with serverless backend, implementing caching strategy that reduced API calls by 90%.
- Built multi-tier caching architecture with timezone-aware invalidation reducing API calls by 90%.

AI Flaw Reporting Form — September 2025

- Built an AI flaw reporting system using Python with dynamic form logic and automated routing to stakeholders.
- Programmed schema validation pipeline using Pydantic models and pyld JSON-LD processing with automated semantic data transformation and cross-format serialization.

BGP Router — October 2024

- Developed a Python-based BGP router supporting IPv4 and JSON-formatted communications for route updates and data forwarding.
- Implemented advanced routing algorithms with longest prefix matching and a five-tiered decision process to ensure optimal route selection.

LEADERSHIP & SERVICE

NeurIPS 2026 Workshop on Child Safety in AI — Sep 2026

Program Committee; Reviewer

- A workshop bringing together researchers, practitioners, and policymakers to address the technical and sociotechnical challenges of protecting children in AI ecosystems.

Duolingo English Test — Sep 2023 - Dec 2024

Student Advisor / Auditor

- Audited software for the Duolingo English Test and ensured that testing infrastructure adheres to accessibility and security best practices.
- Presented findings to a group of 50+ Duolingo team members, including CEO Luis von Ahn.

PRESS & MEDIA

What You Say to Google Assistant and Alexa (but Not Siri) Gets Used for Ad Targeting. Here's How. — Sep 2023

Consumer Reports

Duolingo English Test for U.S. College Admissions — May 2024

US News

What voice assistants like Alexa know about you – and how they use it — Sep 2024

New Scientist

From programming to policy, Khoury undergrads research tough tech questions — May 2026

Khoury News

You Can Now Sound the Alarm on AI Behaving Badly — Jun 2026

WIRED

AWARDS

Exceptional Undergraduate Researcher — Mar 2026

Khoury College of Computer Sciences

- Awarded to one individual annually who showcases impact and technical rigor through their research contributions; nominated and voted on by faculty members in the college.

PEAK Fellowship Summit Awardee — Aug 2024; Jan 2025; Jan 2026

Northeastern University

- Awarded to individuals who demonstrate the ability to independently work on sophisticated research projects; awardees receive a $3000 stipend.