Anna Gerchanovsky

Computer Science Ph.D. Student

WEB: annagerchanovsky.com | **MAIL:** anna@gerchanovsky.com | **GIT:** agercha

Education

Ph.D. Computer Science *August 2024 – Present*
Duke University, *Durham, NC* 4.00/4.00

M.S. Electrical and Computer Engineering *August 2023 – May 2024*
Carnegie Mellon University, *Pittsburgh, PA* 4.00/4.00

B.S. Electrical and Computer Engineering, Minor in Computer Science *August 2019 – May 2023*
Carnegie Mellon University, *Pittsburgh, PA* 3.66/4.00

University Honors

Research

Graduate Student Researcher *August 2024 – Present*
Duke University Durham, NC

- Develop and deploy tools that harness LLMs in order to enhance various aspects of security including usability and verification.
- Design user studies to evaluate the abilities of these tools on human subjects.
- Collaborate with graduate students and other members of the research team to develop new attack vectors and features.

Research Intern *May 2023 – August 2024*
Carnegie Mellon Cylab Pittsburgh, PA

- Conducted literature reviews and analyzed success of and recreated results of existing work in the field, while working on projects in adversarial machine learning for image classifiers and adversarial attacks inducing bias in large language models.
- Developed adversarial models and implement adversarial algorithms and evaluate performance of a variety of models.
- Presented weekly progress reports to a group of professors, post doctoral fellows, and PhD students summarizing my work, analyzing results, and proposing next steps.

Teaching

Computer Security Teaching Assistant *August 2024 – December 2024*
Duke University Durham, NC

- Published and graded weekly labs for a class of 26 students.
- Led review sessions covering course material, including cryptography, network security, and program security.
- Held 2 hours of office hours weekly to assist students with assignments and course material.

Introduction to Computer Security Teaching Assistant *January 2022 – May 2024*
Carnegie Mellon Department of Electrical and Computer Engineering Pittsburgh, PA

Received Departmental Outstanding Teaching Assistant Award

Head TA Duties (as of August 2023)

- Oversaw a team of 7 teaching assistants by distributing responsibilities and tasks.
- Held weekly meetings to manage task progress, establish responsibilities, and familiarize staff with upcoming material.
- Managed on boarding for new and returning course staff.
- Handled communication between course staff or students and instructors.

General TA Duties

- Set up and graded homework assignments on software security, cryptography, web security, and human factors in security.
- Held 2 hours of office hours weekly to assist students with assignments and course material, as well as monitored course forum and answer student questions - covering topics like assembly, buffer overflows, XSS attacks, and SQL injections.
- Led recitations to promote student understanding of course material via hands on activities.
- Developed material for and lead student bootcamps on cryptography.
- Proctored and grade three exams per semester.

Work Experience

Software Engineering Intern *May 2022 – August 2022*
Meta Seattle, WA

• Established error and status logging for the general machine learning model processing team with the goal of analyzing project performance and progress.
• Wrote and tested object oriented code in Python.
• Improved test coverage for machine learning pipelines.

Automation Engineering Intern *May 2021 – August 2021*
Nucor Tubular Products Louisville, KY

• Integrated IBA suite for monitoring PLCs controlling plant performance. Executed daily report design and generation projects for several areas of the plant in order to better analyze and improve on past performance.
• Documented changes made and communicating them to the team.
• Led training sessions for team members to build familiarity with the new IBA system.

Mentorship

Peer Advisor *August 2023 – May 2024*
Carnegie Mellon University Department of Electrical and Computer Engineering Pittsburgh, PA

• Advised undergraduate students in the Electrical and Computer Engineering Department. Discussed course selection, program options, scheduling issues, work life balance. Referred students to appropriate resources when necessary.
• Hosted individual office hours and group advising sessions.
• Participated in events organized by the School of Engineering or Electrical and Computer Engineering Department.

Model Coordinator *August 2023 – April 2024*
Lunar Gala Pittsburgh, PA

• Facilitate the recruitment and audition process of the modeling department of the Lunar Gala student fashion show in Carnegie Mellon University.
• Provide feedback and support during semi-weekly team practice.
• Organize and design practice activities and choreography.

Tutor *August 2020 – December 2023*
Young Tutoring Remote

• Designed one-on-one lesson plans for students in K-12.
• Evaluated and measure student understanding and progress in a variety of subjects including computer science, math, and language arts.

Projects

Gender Bias in Gemma2b Social Media Content
project report

Course project developing tests for gender bias in the Gemma LLM while generating content relating to social media.

PyPi face-recognition Evasion
github repo: agercha/EvasionAttacksFaceRecognition

Evaluate and analyze raw accuracy of facial recognition on raw and edited datasets.

Storytime Video Generation
github repo: agercha/StoryTimeGenerator

Fine tuned GPT3 models to generate and film a specific genre of YouTube video.

Relevant Coursework

Foundations of Privacy	Graduate level course covering introductory privacy concepts like differential privacy, PATE, and federated learning
Secure Software Systems	Graduate level course covering the design and testing of secure software systems
Fantastic Bugs and Where to Find Them	PhD level discussion and project based course focused on bugfinding research
Ethics and Robotics	Graduate level discussion based course covering ethical ramifications of automation and AI
Art and Machine learning	Graduate level project based course covering applications of generative machine learning to art
Introduction to Machine Learning	Undergraduate level homework based course covering the implementation of various algorithms

Skills

Programming Languages Python, C, C++, C0, Swift, SML, JavaScript, CSS
Software Xcode, SystemVerilog, Matlab, Iba Suite