Ziping Ye

zipingy@seas.upenn.edu
www.linkedin.com/in/zipingye

OBJECTIVE

Pursue a Ph.D. to develop fundamentally trustworthy machine learning, focusing on correctness, robustness, fairness, and interpretability with mathematical guarantees.

EDUCATION

Master of Science in Engineering in Computer and Information Science (CIS/MSE) August 2023 - present
The University of Pennsylvania, School of Engineering and Applied Science

Bachelor of Science with Honors in Computer Science, Minor in Mathematics August 2019 - May 2023
The Pennsylvania State University, **Schreyer Honors College,** University Park GPA: 4.0/4.0
Honors Thesis: “Dragon Defender: Runtime Threat Detection for Cellular Devices”

College of Engineering **Student Marshal** for the Computer Science program for Spring 2023
Eta Kappa Nu (HKN) - EECS Honor Society and Golden Key International Honour Society

RESEARCH EXPERIENCE

Project: Explanation Assisted Adversarial Example Generation January 2023 - Present
Prof. Mehnaz’s Lab, Penn State Advisor: Shagufta Mehnaz

- **Motivation**: Attackers can also access model explanations that facilitate transparent machine learning systems for critical decision-making and potentially launch more powerful attacks. I studied the tension between different goals (e.g., security, privacy, transparency) and planned to propose explanation-assisted attacks
- Compared explanations for normal examples and adversarial examples generated by various algorithms from the same benign example; Compared different explanation techniques for the same set of examples

Project: Intrusion Detection for Cellular Network May 2021 - April 2023
Systems and Network Security (SyNSec) Research Group, Penn State Advisor: Syed Rafiul Hussain

- **Motivation**: Because the increasing scale and complexity of modern systems (e.g., cellular networks) make traditional rule-based defensive approaches ineffective, I applied cutting-edge machine learning techniques to protect cellular networks, the critical infrastructure of the digital world, from evolving attacks
- Designed and implemented a novel machine learning architecture in **PyTorch** that uses LSTM on top of BERT, which considers relationships between segments of messages (i.e., inter-window context) for intrusion detection
- Applied contrastive learning for BERT-based window encoder - encodes each window to an embedding; Trained LSTM-based message tagger that assigned benign/attack label to each incoming message
- Achieved **95.64% test accuracy** and **95.44% test F1 score** on 13 common cellular network attacks
- Selected for **Student Engagement Network Grant** and Schreyer Honors College’s Summer Research Grant

Project: Landscape of Neural Network and Its Robustness July 2020 - August 2021
Center for Computational Mathematics and Applications, Penn State Advisors: Jinchao Xu and Jonathan Seigel

- **Motivation**: In an attempt to understand why adversarial examples can fool state-of-the-art neural networks, I studied the neural network as a function of its input space (e.g., pixels in an image) to evaluate the impact of certain pixels on the prediction of each class (e.g., digit 0, cat)
- Found that neural network functions (e.g., ResNet, VGG, DenseNet) become more sensitive to changes in input pixels as training progresses, which explains why even slight changes in pixel values can cause the neural network to produce very different results
- Selected for College of Engineering **Equity REU** and Multi-Campus Summer REU research scholarship

PRESENTATIONS

- “Intrusion Detection for Mobile Networks,” PSU Student Engagement Network Poster Showcase Jan 2022
- “Landscape of Neural Network,” Penn State Undergraduate Research Exposition Apr 2021

HONORS AND AWARDS

Outstanding Undergraduate Research Achievement, 2023
The Evan Pugh Scholar Senior Award, 2022
Engagement Excellence Award, 2021
PSU President Sparks Award, 2021
David & Shirley Wormley Engineering Scholarship, 2020
PSU President’s Freshman Award, 2020
AP Scholar with Distinction Award, 2019

LEADERSHIP AND CIVIC ENGAGEMENT

Founding President, International and Multicultural Association of Schreyer Scholars (IMASS) October 2022 - April 2023

- Developed Mission Statement; Designed the organizational structure; Formed executive board
- Discussed collaboration and partnership with other student organizations and cultural departments
- Organized **Lunar New Year Celebration** and **Black History Month** at Schreyer Honors College
- Planned events for career development and promoting cross-cultural understanding and awareness
- The story was featured in Penn State News (New student organization supports multicultural Schreyer Scholars)

Student Leader, International Schreyer Scholars Engagement March - October 2022

- Connected with international and domestic Schreyer Scholars; Foster a genuine sense of belonging of international and multicultural scholars in the honors college community
- Helped international scholars with scheduling conflicts during their International Student Orientation and Schreyer Honors College Orientation; Sent targeted welcome emails to incoming international scholars
- Invited to join the "Building Belonging" workshop series, where Schreyer leadership and student leaders meet and exchange ideas and learn how to lead a student organization

Selected Delegate, United States Naval Academy Leadership Conference January 2023

- Selected as one of four Penn State delegates to network with more than 400 participants from over 45 military and civilian colleges; Attended speaker and panel sessions on leadership, integrity, and honor
- Engaged in small group discussions about "strength through adversity" and resilience

Selected Participant, Deloitte Leadership Development Center October 2022

- Participated in business activities designed to introduce students to challenges and decisions they will face as leaders in various organizations for a simulated initiative - *Dinner And A Movie*; Received personalized feedback and leadership development plan
- Wrote executive summary and gave a virtual presentation; Made hiring decision; Addressed negative customer feedback
- Participated in a leaderless group discussion where members wrote a detailed job description for a new role (Director of Operations) and suggested a candidate for this role among two applicants

Committee Member, All Scholar Involvement Fair Planning Committee May - October 2022

- Attended regular meetings throughout the summer to discuss and plan for the event
- Designed and created marketing flyers, welcome sign, and sign-in survey and helped during the event
- Discussed planning for future years and strategies to promote student clubs during the debriefing meeting

Volunteer, CONNECT 2022 March 2022

- Helped with the setup, clean up, and registration table for Schreyer Honors College Annual Career Event

TEACHING AND MENTORING

Mentor, SHO TIME 2022 March - August 2022

- Participated in five training sessions (use of inclusive language, leadership, communication skills) and in planning for Schreyer Honors College Orientation (SHO TIME) 2022
- Affirmed as **Certified Peer Educator** (CPE) by National Association of Student Personnel Administrators (NASPA)
- Selected as Scholar representative to attend PSU President's Welcome Reception for International Students
- Led a group of thirteen first-year incoming Schreyer Scholars during the two-day SHO TIME
- Served as the table host for second/third-year incoming scholars; Led the discussion and answered questions

Teaching Assistant, Programming & Computation II: Data Structures (CMPSC 132) Fall 2020

- Worked with a group of ten teaching assistants in a computer science course at Penn State, assisting the professor in grading assignments for over 400 students
- Provided positive feedback on students' style of coding and computational efficiency in a timely manner

SOFTWARE PROJECTS

AutoDrive Challenge II (Penn State Advanced Vehicle Team Object Detection Department): Explored high-definition (HD) map used in autonomous driving and converted it into a database; Designed and implemented algorithms based on HD map for the highway challenges in **Python** and **PostgreSQL**; Communicated with other departments to test the correctness and performance of the developed algorithms; Gave Alpha, Beta, and final prototype presentation and co-authored Statement of the Work Report and Final Report.

Software Security: Implemented Buffer Overflow, Heap Overflow, Shell Code Injection, and Returned Oriented Programming attacks in **C**; Examined how stack changes during a function call and program control flow.

Access Control: Programmed an access control reference monitor in **C** that enforces various Mandatory Access Control (MAC) policies (e.g., Biba Integrity policy, Windows Mandatory Integrity Control (MIC) policy, Low Water-Mark Mandatory Access Control (LOMAC) policy) to protect integrity and confidentiality.

Web Security: Learned and implemented Structured Query Language (SQL) Injection attack, Cross Site Scripting (XSS) attack, and Cross-site request forgery (CSRF) attack.

Network Security: Implemented the Secure Shell Protocol (SSH) in **C** using the OpenSSL library; Developed a client-server system that provides secure file transfer; Developed a machine-in-the-middle (MITM) attack - *Server Spoofing*.

Dynamic Memory Allocator: Implemented a dynamic memory allocator in **C**; Supported malloc, free, realloc, coalesce, split, and mm_init functions; Wrote a heap checker to check invariants of heap memory; Utilized a segregated list to keep track of free blocks of different sizes for the best balance of throughput and memory utilization.

MiniOS: Implemented 4-level user and kernel space page table in **C**; Integrated dynamic memory allocator into MiniOS.

Channels (concurrent programming): Developed a synchronization primitive *channel* in **C**; Used semaphore to implement a buffered channel that supports send, receive, close, destroy, and select functionalities.

2D Drawing Application: Wrote a 2D drawing application in **Java**; Implemented undo and clear button and a status bar showing the mouse's current location; Supported common shapes (e.g., line, oval, rectangle) - filled/unfilled, line width, color, and gradient effect.

CPU: Designed and implemented a five-stage pipeline CPU using the Xilinx design package for FPGAs with **Verilog** codes for the R-type, I-type, and J-type instructions.

Room Scheduling System: Designed a database-driven application with Graphical User Interface (GUI) in **Java** and **SQL** for room scheduling with a given date and the number of seats; Implemented methods to add a room, drop a room, cancel a reservation, check the status by faculty and by date, and add to the waitlist.

MDADM Linear Device: Built a user-space application in **C** that manages the storage system with networking features; Implemented read, write, seek to disk, seek to block functionalities that allows user to interact with multiple disks as one linear device; Developed Least Recently Used (LRU) cache with 89.2% hit rate for random input with 4096 cache entries.

Iterative Methods Comparison: Compared the convergence rate and accuracy of widely-used iterative methods to solve linear systems, including Newton's method, Gauss-Seidel method, and successive over-relaxation (SOR) method for linear systems with different entries and dimensions using **MATLAB**.