Xiaotian Zhou

xzz5503@psu.edu

EDUCATION

The Pennsylvania State University, Pennsylvania, U.S. Aug 2023 - Now
Master of Science, Computer Science and Engineering
Advisor, Prof. Syed Rafiul Hussain

ShanghaiTech University, Shanghai, China Aug 2019 — Jun 2023
Bachelor of Engineering, Computer Science and Technology Overall GPA: 3.82
Thesis, Adversarial Attacks on Audio Spoofing Countermeasures.
Supervisor, Prof. Fu Song
Awards, Merit Student (2019-2020)
Experience, Visiting Student at University of California, Berkeley (Aug 2021 - May 2022, GPA 4.0)

RESEARCH INTERESTS

Formal Methods, Proof Assistants, Computer Security, Programming Languages.

PROJECTS

Verified Parser for Network Protocols Penn State University
Advisor, Prof. Syed Hussain; *Collaborator*, Prof. G. Gary Tan. Sep 2023 - Now

- Research and understand the vulnerabilities of parsers in network protocols like 5G,
- Apply and modify existing verified parser tools to parse protocols like ASN.1.

Adversarial Attacks on Audio Spoofing Countermeasures ShanghaiTech University
Supervisor, Prof. Fu Song. Aug 2022 - May 2023

- Research and understand adversarial attacks in Machine Learning and Speaker Verification System spoofing countermeasures,
- Implement various adversarial attacks using PyTorch,
- Design attacks and experiment with different approaches to find the most effective attack.

TEACHING EXPERIENCE

Teaching Assistant ShanghaiTech University

Mathematical Analysis I Fall 2020

Mathematical Analysis II Spring 2021 and Spring 2023

COURSE PROJECTS

Dynamic Storage Allocator CSE 473 at Penn State

- Implement a dynamic storage allocator, i.e., a heap, in C, using various optimizations, like segregated lists.

Deep Equilibrium Network SI 251 at ShanghaiTech

- Research and summarize the topic of deep equilibrium network,
- Conduct extensive research on existing models, and develop new mathematical revelations.

An End-to-End Encrypted File Sharing System CS 161 at Berkeley

- Designing and implementing a secure file-sharing system using various cryptographic schemes in GoLang.

SKILLS

- **Relevant Coursework:** Computer Security, Cryptography, Machine Learning, Operating Systems, Convex Optimization;
- **Programming Languages:** C, C++, Python, Coq;
- **Software:** git, LaTeX, Linux, PyTorch;
- **Languages:** English, Chinese.