Ruxi Gu

Residence: Wuhan, China

E-mail: 2021302141194@whu.edu.cn ✻ *Telephone number:* 13026121612

Education

Bachelor's degree in Cyberspace Security *2021.9 - Present*
School of Cyber Science and Engineering, Wuhan University *Wuhan, China*

- Final GPA: 3.83/4.00
- A^+ Courses:
  Linear Algebra (90), Probability Theory and Mathematical Statistics (95), Discrete Mathematics (93),
  Circuits and Analog Electronics (97), Digital Logic and EDA (94),
  Computer Organization Practice (97), Data Structure Practice (95), Artificial Intelligence Practice (98) and more.
- CET4 Grade: 629/710

High School Diploma *2018.9 - 2021.6*
Wuhan Foreign Languages School *Wuhan, China*

Research Interest

AI Security My research interest lies in Artificial Intelligence (AI) Security & Privacy, where I explore the weakness of Deep Learning models in their lifecycles (e.g., Adversarial Attack, Backdoor Attack) and their countermeasures. I also made efforts on turning these weaknesses into good use, applying on privacy protection and Intellectual Property (IP) protection of deep learning models.

Research Team

NIS&P Lab NIS&P Lab focuses on three branches of security research: cloud computing security, wireless system security, and Big data and artificial intelligence security. We are interested in the security and privacy issues behind various information systems and hope to find practical and meaningful solutions for the physical world. Professor Qian Wang is the leader of the laboratory. I am a member of the laboratory.

Project experience

Yinyiweirong: Efficient Privacy Protection Image Recognition Platform *2023.6 - Present*
Wuhan University, Advisor: Prof. Kun He *Wuhan, China*

- This work combs the Technology roadmap of privacy protection prediction in recent years, emphatically describes the development of privacy protection neural network prediction protocol, and points out that the previous work has the problem of poor connection between linear layer and nonlinear layer protocols. To solve this problem, an efficient privacy protection neural network prediction framework Hare is designed under the semi honest adversary model, which can protect user privacy data and Convolutional Neural Network model parameters in cloud prediction services.
- As a member in this program. This project participates in the 16th National College Student Information Security Contest.

Zhiandun: Leader in Artificial Intelligence Security Guard *2023.4 - Present*
Wuhan University, Advisors: Prof. Qian Wang, Prof. Linchen Zhao *Wuhan, China*

- Zhiandun is the first independent security integrated defense platform integrating the analysis of adversarial attack mechanism in China, and its core technology is all based on the cutting-edge achievements of team members. This platform serves the artificial intelligence technology industrialization market, builds comprehensive defense guarantees for intelligent models, achieves safe and reliable deployment and application services of artificial intelligence systems in various fields, and promotes the development and industrialization process of artificial intelligence technology in China.
- As a core member in this program.

Competition Awards

First Prize *2023.6*
2023 CATTI Cup National Translation Competition *China*

Third Prize *2022.12*
2022 National English Competition for College Students *China*

Technical skills

Programming Languages	C/C++, Python, Java
Libraries	Numpy, Pytorch
Developer Tools	VS Code, Pycharm, IDEA
Other Tools	LaTeX, Markdown, Adobe Photoshop, Audition and Premiere

Language proficiencies

Chinese	Native
English	Fluent in Speaking
Japanese	Relatively Familiar

About Me

Hobbies Playing Go, especially against AI; Reading, the favorite writer is Geling Yan; Playing tennis, currently studying.

Personality I will actively step out of my comfort zone and welcome new technologies and challenges. By learning these new technologies, I can continuously improve myself and make breakthroughs. I will actively seek possible solutions to the difficulties in my own learning process, including online search and asking others; I am also willing to share my experience with others, so that they are not constrained by information gaps.