Jiaming He

Chengdu 610059, China — he.jiaming@student.zy.cdut.edu.cn — (+86) 17358650030

EDUCATION

Chengdu University of Technology, Oxford brookes college, Chengdu, China
Enrolled: Sep. 2021 — Expected: Jun. 2025
B.S. in Software Engineering
Overall GPA: 73 (First class honors) **Rank: 3/102**

RESEARCH EXPERIENCE

Key Cyberspace Security Research Laboratory, University of Electronic Science and Technology of China (UESTC) Chengdu, China

Feb 2023 - Jan 2024

During my time in the Cyberspace Security Research Laboratory, I worked as a visiting student advised by Prof. Hongwei Li and Dr. Wenbo Jiang. My research projects was mainly about the security of mahchine learning models including the poisoning attacks, adversarial attacks and jailbreak. And our works are mainly submitted to IEEE Transactions on Dependable and Secure Computing.

Artificial Intelligence Research Group, Commonwealth Scientific and Industrial Research Organisation (CSIRO) Melbourne, Australia (Remote)

Jan 2023 - Present

During my time in the Artificial Intelligence Research Group, my research mainly focus on the security of Large models (e.g., Jailbreak of Large Language models and the backdoor attack on diffusion based Text2Image scenario.) And I also participate in the research of safe reinforcement learning and privacy protection of graph data.

PUBLICATIONS

”MTISA: Multi-Target Image-Scaling Attack” 2024 IEEE International Conference on Communication (ICC) ***Oral***

Jan 2024 - Accepted

”A Flexible Backdoor attack on Text-to-image generation models” IEEE Transactions on Dependable and Secure Computing (TDSC)

Jan 2024 - Submitted

”Backdoor Attacks against Image-to-Image Networks” IEEE Transactions on Dependable and Secure Computing (TDSC)

Nov 2023 - Submitted

”Rethinking the Design of Backdoor Triggers and Adversarial Perturbations: A Color Space Perspective” IEEE Transactions on Dependable and Secure Computing (TDSC)

Aug 2023 - Submitted

SKILLS

- **Programming:** C/C++, Python, Java, HTML
- **Language:** English (fluent), Mandarin (native)
- **Tool:** Latex, Microsoft Office