JIALIANG DONG

(+61) 0421725221 jialiang.dong@unsw.edu.au

ENGLISH PROFICIENCY

IELTS Test: 7.0

EDUCATION

The University of New South Wales September 2023 - In progress
PhD. Candidate in Cyber Security

North China Electric Power University September 2020 - June 2023
Master of Philosophy in Computer Science and Technology *Acquired June 2023*

North China Electric Power University September 2015 - June 2019
Bachelor in Computer Science and Technology *Acquired June 2019*

PUBLICATIONS

- [*Conference*] "Ghosts in DBMS: Revealing the Security Impacts of Silent Fixes" **Jialiang Dong**, Zihan Ni, Willy Susilo, Siqi Ma *International Conference on Data Security and Privacy Protection (DSPP)*, 2025
- [*Conference*] "From Surface to Semantics: Semantic Structure Parsing for Table-Centric Document Analysis" Xuan Li, **Jialiang Dong (co-corresponding)**, Raymond Wong, *European Conference on Artificial Intelligence (ECAI)*, 2025
- [*Conference*] "What Lies Beneath: An Empirical Study of Silent Vulnerability Fixes in Open-Source Software" **Jialiang Dong**, Xinzhang Chen, Willy Susilo, Nan Sun, Arash Shaghaghi, Siqi Ma, *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* , 2025
- [*Conference*] "Enhancing Security in Third-Party Library Reuse - Comprehensive Detection of 1-day Vulnerability through Code Patch Analysis" Shangzhi Xu, **Jialiang Dong**, Weiting Cai, Juanru Li, Arash Shaghaghi, Nan Sun, Siqi Ma, *Network and Distributed System Security Symposium (NDSS)*, 2025
- [*Journal*] "WEDA: Exploring Copyright Protection for Large Language Model Downstream Alignment" Shen Wang, **Jialiang Dong (co-first)**, Longfei Wu, Zhitao Guan *IEEE/ACM Transactions on Audio, Speech and Language Processing (TASLP)*, 2024
- [*Journal*] "Transferable Adversarial Distribution Learning: Query-Efficient Adversarial Attack against Large Language Models" Huoyuan Dong, **Jialiang Dong**, Shaohua Wan, Shuai Yuan, Zhitao Guan, *Computer & Security (COSE)*, 2023
- [*Conference*] "A Textual Adversarial Attack Scheme for Domain-Specific Models" **Jialiang Dong**, Shen Wang, Longfei Wu, Huoyuan Dong, Zhitao Guan, *International Conference on Machine Learning for Cyber Security (ML4CS)*, 2023
- [*Conference*] "Adversarial Attack and Defense on Natural Language Processing in Deep Learning: A Survey and Perspective" Huoyuan Dong, **Jialiang Dong**, Shuai Yuan, Zhitao Guan, *International Conference on Machine Learning for Cyber Security (ML4CS)*, 2023
- [*Journal*] "A Sentence-level Text Adversarial Attack Algorithm against IIoT based Smart Grid" **Jialiang Dong**, Zhitao Guan, Longfei Wu, Xiaojiang Du, Mohsen Guizani, *Computer Networks*, 2021

AWARDS & HONORS

- NDSS'25 Fellowship. January 2025
- ACM MMAsia'24 Best Student Presentation Award. December 2024
- National Scholarship for Postgraduate Student, North China Electric Power University. December 2021
- Outstanding Postgraduate Model, North China Electric Power University. December 2021

· First Prize, Excellent Student of Academic Performance, North China Electric Power University. December 2021
· National Excellence Award, Innovation and Entrepreneurship Competition of College Students. August 2018

SKILLS AND TEACHING EXPERIENCE

Computer Skills	Python, C/C++, JAVA, LaTeX.
Language Skills	Mandarin (Native), English.
Teaching Experience	Teaching Assistant in UTS - Software Architecture Teaching Assistant in UNSW - Cyber Resilience. Teaching Assistant in NCEPU - Baidu Summer AI Training Camp.