Mingrui Ma

(+86) 135 6004 8588
mingruimageek@gmail.com
jkpathfinder.github.io

Education

Sep 2022 – Present
M.Eng. in Computer Science, Cyber Security, *Huazhong University of Science and Technology (HUST)*, Wuhan, Hubei, China, *Overall Ranking 1/133*
Expected Graduation: June 2025

Sep 2018 – June 2022
B.Eng. in Computer Science, Information Security, *HUST*, Wuhan, Hubei, China, *GPA 3.87/4.00*
Graduating with distinction

Research Interest

AI + Data Analytics, AI Applications, Large Language Models, AI Security, Natural Language Processing

Publications & Preprints

[1] **Mingrui Ma**, Lansheng Han, and Chunjie Zhou. Research and application of artificial intelligence based webshell detection model: A literature review, 2024. https://arxiv.org/abs/2405.00066

[2] **Mingrui Ma**, Lansheng Han, and Chunjie Zhou. Large language models are few-shot generators: Proposing hybrid prompt algorithm to generate webshell escape samples, 2024. https://arxiv.org/abs/2402.07408

[3] **Mingrui Ma**, Lansheng Han, and Chunjie Zhou. Research and application of transformer based anomaly detection model: A literature review, 2024. https://arxiv.org/abs/2402.08975

[4] **Mingrui Ma**, Lansheng Han, and Chunjie Zhou. Btad: A binary transformer deep neural network model for anomaly detection in multivariate time series data. Advanced Engineering Informatics, 56:101949, 2023. https://doi.org/10.1016/j.aei.2023.101949

[5] ZHU Lina, **MA Mingrui**, and ZHU Dongzhao. Detection method for c language family based on graph neural network and generic vulnerability analysis framework. Netinfo Security, 22(10):59, 2022. http://netinfo-security.org/CN/Y2022/V22/I10/59

[6] **Ma, Mingrui**, Lansheng Han, and Yekui Qian. Cvdf dynamic—a dynamic fuzzy testing sample generation framework based on bi-lstm and genetic algorithm. Sensors, 22(3), 2022. https://www.mdpi.com/1424-8220/22/3/1265

Academic Services

Nov 2024 – Present
"Computers and Electrical Engineering" (JCR Q2, IF 4.0), *Elsevier*

Oct 2024 – Present
"Neurocomputing" (JCR Q2, IF 5.5), *Elsevier*

Sep 2024 – Present **"International Journal of Intelligent Systems" (JCR Q1, IF 5.0)**, *WILEY*

Jul 2024 – Present **"IEEE Transactions on Knowledge and Data Engineering (TKDE)" (JCR Q1, CCF-A, IF 8.9)**, *IEEE*

Jul 2024 – Present **"International Journal of Machine Learning and Cybernetics" (JCR Q2, IF 3.1)**, *Springer*

Jul 2023 – Present **"IEEE Transactions on Intelligent Transportation Systems (TITS)" (JCR Q1, IF 7.9)**, *IEEE*

May 2023 – Present **"Applied Intelligence" (JCR Q2, IF 3.4)**, *Springer*

Research Experience

Oct 2024 – Present **Large Language Model Prompt Injection Attack Testing Tool**, *Project Leader*, Co-op Project

- Conduct a comprehensive literature review on current techniques for prompt injection (PI) attacks against Large Language Model (LLM)
- Design and develop an automated PI attack testing framework, integrating a correlation-based PI algorithm that combines Direct Attacks (DAs) and Indirect Attacks (IAs), and a hierarchical adversarial sample generation algorithm to overcome defense vulnerabilities
- Collaborate with a local high-tech company and leverage its AI platform's acceleration capabilities to build advanced automated algorithms for efficient, large-scale testing of PI attacks

Jun 2024 – Present **Yu Heng - Intelligent Penetration Testing and Risk Assessment System with Autonomous Planning, Execution, and Feedback**, *Project Leader*, The 6th CHINA Graduate AI Innovation Competition

- Lead a 4-member team to develop a generalized analytical framework for multi-agent data interaction and task execution
- Develop an automated domain-specific user query execution framework, utilizing reinforcement learning and prompt paradigms to enhance system adaptability and precision
- Apply the system to automate penetration testing across various application scenarios, the project won the First Prize (Top 1%) in the competition with high performance in detection accuracy, risk assessment, and execution speed

Mar 2023 – Jul 2024 **IntelliSense - Cross-Domain Implicit Space-Oriented Malicious Code Adversarial Detection and Source Tracking System**, *Project Leader*, The Fundamental Research Funds for the Central Universities, Grant: YCJJ20230464

- Led an 8-member team to develop a system for detecting and tracking malicious code, improving detection accuracy, stability, and efficiency
- Designed a novel method for fusing multi-dimensional graph tensors of code, combining semantic, syntactic, and other features into a streamlined, informative representation that retained original traits while reducing storage costs
- Contributed to tracking polymorphic malicious code, analyzing multi-domain features to uncover hidden malicious behaviors
- Achieved a 2.2x higher detection speed and 98.6% accuracy compared to industry tools (Kaspersky, WEBDIR+, Avast), with a 40% improvement in detecting obfuscated data
- Project outcomes include two patents (first and fourth inventor), one software copyright (first designer), two national competition awards (The 18th "Challenge Cup" National College Student Curricular Academic Science and Technology Works Competition, Grand Prize (Top 0.5%), and The 2nd China Graduate Network Security Innovation Competition, First Prize (Top 0.5%)), and one provincial award (The 14th Hubei Province "Challenge Cup" College Student Curricular Academic Science and Technology Works Competition, First Prize (Top 1%))

Sep 2022 – Oct 2024 **AI + Data Analytics for Big Data Platform**, *Key Project Member*, The National Key Research and Development Program of China, Grant: 2022YFB3103403

- Developed an AI-driven automated method for log and evidence generation, used natural language processing (NLP) techniques and machine learning algorithms to extract high-value information from raw data, and created standardized log structures for downstream analysis
- Designed a versatile filtering mechanism supporting algorithms such as Pearson correlation, gray correlation analysis, and precise time range filtering, which efficiently removed irrelevant or unfavorable data and ensured accuracy in data collection
- Contributed to two patents (as first inventor) and one journal paper (as first author)

Invention Patents & Software Copyrights

Patent 1 **A Method, Device, and System for Evidence Generation Based on Multivariate Collaborative Analysis**, *NO: 2024031901604420*, Primary Inventor

Patent 2 **A Normalized Log Generation Method Based on the Entropy Increase Principle**, *NO: 2023112102142270*, Primary Inventor

Patent 3 **A Method for Multidimensional Graph Tensor Fusion Representation and Embedding of Codes**, *NO: 2023052300567880*, Primary Inventor

Patent 4 **A Method and System for Implicit Intelligence Tracking of Malicious Code under Polymorphic Concealment**, *NO: 2023052300572110*, Fourth Co-inventor

Patent 5 **A Network Penetration Testing Method and System Based on State Feedback**, *NO: 2024111501321623*, Fifth Co-inventor

Patent 6 **A Penetration Testing System and Method Based on Multi-Agent Collaboration**, *NO: 2024111301341650*, Ninth Co-inventor

Copyright 1 **IntelliSense - Cross-Domain Implicit Space-Oriented Malicious Code Adversarial Detection and Source Tracking System**, *NO: 11285657*, Primary Designer

Copyright 2 **Automated Attack Path Generation System for Non-Control Flow Hijacking of Binary Programs V1.0**, *NO: 13116013*, Fifth Designer

Selected Projects

Apr 2023 – Jun 2024 **RUSTSBI Open-Source Project**, *Major Contributor & Core Member*, RUST Community
Contributed to 2 Pull-Requests as a major contributor, both of which have been reviewed and merged

Dec 2022 **AMWD 2022: Alibaba Cloud Security WEBSHELL Text Detection Algorithm Competition (International Level)**, *Core Project Member*, Alibaba
Completed the Webshell text categorization task with BERT neural network model, World Ranking 61 (TOP 10%)

Nov 2022 **The 1st China Graduate Network Security Innovation Competition (National Level)**, *Core Project Member*, **National Champion & National Record Holder**
Conducted malicious code similarity detection with ensemble learning and neural networks

Honors & Awards

2024 **(School Level) Academic Excellence Award** (The highest individual honor for graduate students, only 2 out of 20,085 candidates received this distinction)

2024 (Enterprise Level) HUAWEI Scholarship (Ranked Top 1/133)

2024 (School Level) Technology Innovation Scholarship

2024, 2023 **(National Level) National Scholarship** (Ranked Top 0.2% among all graduates)

2023 **(Province Level) GENGSHU Prize** (The highest research group honor for graduate students, only 3 groups received this distinction)

2023 (School Level) Merit graduate

2023 (School Level) Zhixing Scholarship

2022 (School Level) Graduation Design of Distinction

2024, 2023, 2022 (School Level) The Top Prize Scholarship

Research Interns

Sep 2024 – Present **Institute of Software, Chinese Academy of Sciences**, *AI Algorithm Engineer*, Beijing, China
Develop a specialized domain knowledge Q&A Agent for chip developers and users to streamline prototype construction time

Jun 2024 – Sep 2024 **Fortune Global 500 Tech Company (name confidential per agreement)**, *AI Algorithm Engineer*, Shenzhen, China

- Developed an LLM Agent-based intelligent summarization algorithm and an automated multi-classification process using RAG technique
- The algorithm was successfully deployed company-wide and actively used by over 200,000 employees, receiving high praise from the company's leadership
- Authored 2 research papers (first author), currently under review for publication

Teaching Experience

Sep 2022 – Mar 2023 **Teaching Assistant** for the Graduate Course "Computer Virus Propagation Models", HUST

Mar 2023 – Jun 2023 **Teaching Assistant** for the Undergraduate Course "Comprehensive Practice of Network Security", HUST

Skills

Programming languages: Python, C/C++, Go, PHP, Matlab, etc.

Frameworks & Tools: PyTorch, Tensorflow, Qt, LaTeX, etc.