Qiming Zhang

(+1) 614-477-9533 | qzhang478@wisc.edu | qimingzhang.com

EDUCATION BACKGROUND

- **University of Wisconsin–Madison** *05/2025*
  B.S. in Computer Science, GPA: 3.9/4.0 Madison, WI
  Honors: Graduation with Distinction
  Advisor: Prof. Chaowei Xiao & Prof. Zhen Xiang

PUBLICATIONS / PREPRINTS

[1] Weidi Luo, **Qiming Zhang**, Tianyu Lu, Xiaogeng Liu, ... , Yizhe Zhang, Xusheng Xiao, Yinzhi Cao, Zhen Xiang, Chaowei Xiao. (2025). **Code Agent can be an End-to-end System Hacker: Benchmarking Real-world Threats of Computer-use Agent**. *Preprint arXiv:2510.06607*. Under Review for *ICLR 2026*.

[2] Weidi Luo*, Tianyu Lu*, **Qiming Zhang***, Xiaogeng Liu, Bin Hu, Yue Zhao, Jieyu Zhao, Song Gao, Patrick McDaniel, Zhen Xiang, Chaowei Xiao. (2025). **Doxing via the Lens: Revealing Location-related Privacy Leakage on Multi-modal Large Reasoning Models**. *ICCV Workshop on Building Foundation Models You Can Trust* **(Oral)**. Under Review for *ICLR 2026*.

RESEARCH EXPERIENCE

- **AI for Cybersecurity at Johns Hopkins University & University of Georgia** *03/2025 – 09/2025*
  Research Assistant, Advisor: Prof. Chaowei Xiao & Prof. Zhen Xiang Baltimore, MD
  - Conducted research on **AI for cybersecurity**, focusing on real-world attack surfaces in agentic LLM systems.
  - Built the **end-to-end experimental pipeline** for AdvCUA, including multi-host sandbox setup, task automation, and hard-coded evaluation, enabling scalable and reproducible assessment of OS-level threats in computer-use agents.
- **AI Safety & Privacy at Johns Hopkins University & University of Georgia** *04/2025 – 09/2025*
  Research Assistant, Advisor: Prof. Chaowei Xiao & Prof. Zhen Xiang Baltimore, MD
  - Investigated **AI safety** and **privacy risks** in multimodal large reasoning models (MLRMs), with emphasis on real-world geolocation leakage.
  - Built the **large-scale experimental pipeline** for DOXBENCH, including structured-output validation and automated evaluation across 11 state-of-the-art MLRMs/MLLMs.
  - Developed **GEOMINER**, a collaborative attack framework that decomposes geolocation into staged clue extraction and reasoning, revealing model overreliance on privacy-sensitive cues.
  - Proposed **CLUEMINER**, a framework for extracting, categorizing, and analyzing visual clues used by models, enabling systematic evaluation of inference-time privacy risks and reasoning behavior.

EXPERIENCE

- **Computer Sciences Learning Center, University of Wisconsin–Madison** *09/2024 – 12/2024*
  Peer Mentor Madison, WI
  - Diagnosed and resolved individual coding bottlenecks in 1-on-1 settings, emphasizing debugging methodologies (e.g., GDB, unit testing) over simple error correction.
  - Designed and delivered supplementary lecture materials for complex topics, helping students bridge the gap between theoretical proofs and practical implementation.
- **National Institute of Metrology** *06/2022 – 07/2022*
  Volunteer Beijing, China
  - Executed statistical analysis using Python, isolating key variables impacting measurement consistency.
  - Developed data visualizations for quarterly technical reports, synthesizing experimental results for senior research staff.
  - Maintained dataset integrity by implementing rigorous quality assurance protocols on calibration logs.

SERVICE

- **Peer Review**: ACL Rolling Review (ARR) Emergency Reviewer (May & July 2025)

SKILLS

- **Programming & Software**: Python, Java, Kotlin, JavaScript, React Native, C, SQL, MongoDB, MATLAB, Linux
- **Languages**: Chinese, English