

# Jian Cui

*cuijian0819.github.io*

(last update: March 9, 2026)

## EDUCATION

---

- University of Illinois Urbana–Champaign (UIUC)** *Aug. 2025 – Present*  
Ph.D. Student in Computer Science  
*Advisor:* Xiaojing Liao
- Indiana University Bloomington (IUB)** *Aug. 2023 – Aug. 2025*  
Ph.D. Student in Computer Science  
*Advisor:* Xiaojing Liao
- Korea Advanced Institute of Science and Technology (KAIST)** *Mar. 2015 – Feb. 2022*  
B.S. & M.S. in Electrical Engineering  
*Advisor:* Seungwon Shin

## RESEARCH INTEREST

---

Security & Privacy of Agentic AI, AI (Agent) for Security, Data-driven Security

## PUBLICATION

---

1. “Les Dissonances: Cross-Tool Harvesting and Polluting in Multi-Tool Empowered LLM Agents” (to appear)  
Zichuan Li\*, **Jian Cui**\*, Xiaojing Liao, Luyi Xing  
*\*2nd place in Berkeley RDI MOOC Hackathon - Safety track*  
*The Network and Distributed System Security Symposium (NDSS’26)*
2. “The Odyssey of robots.txt Governance: Measuring Compliance Implications of Web Crawling Bots in Large Language Model Services”  
**Jian Cui**\*, Mingming Zha\*, Xiaofeng Wang, Xiaojing Liao  
*The ACM Conference on Computer and Communications Security (CCS’25)*  
*\*Distinguished Paper Award*
3. “Tweezers: A Framework for Security Event Detection via Event Attribution-centric Tweet Embedding”  
**Jian Cui**, Hanna Kim, Eugene Jang, Dayeon Yim, Kicheol Kim, Jinwoo Chung, Yongjae Lee, Seungwon Shin, Xiaojing Liao  
*The Network and Distributed System Security Symposium (NDSS’25)*
4. “Malla: Demystifying Real-world Large Language Model Integrated Malicious Services”  
Zilong Lin, **Jian Cui**, Xiaofeng Wang, Xiaojing Liao  
*The 33rd USENIX Security Symposium (USENIX Sec’24)*  
*\*Top15 finalist in the CSAW Best Applied Research Paper Competition, 2024*
5. “Ignore Me But Don’t Replace Me: Utilizing Non-Linguistic Elements for Pretraining on the Cybersecurity Domain”  
Eugene Jang, **Jian Cui**, Youngjin Jin, Dayeon Yim, Jinwoo Chung, Yongjae Lee, Seungwon Shin  
*Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL’24 Findings)*
6. “DRAINLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs”  
Hanna Kim, **Jian Cui**, Eugene Jang, Chanhee Lee, Yongjae Lee, Jinwoo Chung, Seungwon Shin  
*ISOC Network and Distributed System Security Symposium (NDSS’24)*

7. “DarkBERT: A Language Model for the Dark Side of the Internet”  
Youngjin Jin, Eugene Jang, **Jian Cui**, Jinwoo Chung, Yongjae Lee, Seungwon Shin  
*The 61st Annual Meeting of the Association for Computational Linguistics (ACL’23)*
8. “Meta-Path-based Fake News Detection Leveraging Multi-level Social Context Information”  
**Jian Cui**, Kwanwoo Kim, Seung Ho Na, and Seungwon Shin  
*31st ACM International Conference on Information and Knowledge Management (CIKM’22)*
9. “MECaNIC: SmartNIC to Assist URLLC Processing in Multi-Access Edge Computing Platforms”  
Taejune Park, Myoungsung You, **Jian Cui**, Youngjin Jin, and Seungwon Shin  
*The 30th IEEE International Conference on Network Protocols (ICNP’22)*
10. “Safeguard-by-Development: A Privacy-Enhanced Development Paradigm for Multi-Agent Collaboration Systems”  
**Jian Cui**, Zichuan Li, Luyi Xing, Xiaojing Liao  
*\*1st place in Berkeley RDI AgentX Competition - Safety track (under review)*
11. “No Model Is an Island: Enabling Adversarial Attacks on Neural Network Pipeline at Binary Level”  
Kexin Chen\*, Zichuan Li\*, Zilong Lin, **Jian Cui**, Qixu Liu, Luyi Xing  
*(under review)*
12. “OAuth in the MCP Wonderland: Exploring Compliance of OAuth Security Best Practices in MCP Ecosystems”  
**Jian Cui**, Minsun Shim, Zhou Li, Xiaojing Liao  
*(under review)*

## PROFESSIONAL EXPERIENCE

---

**Applied Scientist Intern** (*Host: Pranav Garg, Shweta Garg*)

*Amazon Web Services, United States*

*May. 2024 - Aug. 2024*

**Research Intern**

*S2W Inc., South Korea*

*Feb. 2022 - June. 2023*

## INVITED TALK

---

**Towards Trustworthy Agent Development Framework: From Attacks to Defenses**

*Palo Alto Networks, United States*

*Aug. 2025*

**A Security Controlled Development Paradigm for Multi-Agent Collaboration Systems**

*AG2 (AutoGen) Community Talk, Virtual*

*Aug. 2025*

**The Odyssey of robots.txt Governance: Measuring Convention Implications of Web Bots in Large Language Model Services**

*UIUC CS 210 - Ethical & Professional Issues*

*Nov. 2025*

## HONORS AND AWARDS

---

CCS 2025 Distinguished Paper Award

*Oct. 2025*

1st Place – Safety Track, UC Berkeley RDI AgentX Competition

*Aug. 2025*

2nd Place – Safety Track, UC Berkeley RDI LLM Agents Hackathon

*Feb. 2025*

The Internet Society NDSS Symposium Fellowship

*Feb. 2025*

Indiana University Luddy Doctoral Summer Fellowship

*Aug. 2023*

The 2023 Korea Financial Security Institute Paper Award

*Oct. 2023*

The 2023 Korea Cyber Security Paper Award

*Sept. 2023*

The 27th Samsung Humantech Paper Award

*Feb. 2021*

## ACADEMIC ACTIVITIES & SERVICES

---

Program Committee, ACM ASIA Conference on Computer and Communications Security (AsiaCCS'27)  
Program Committee, NDSS Workshop on AI System with Confidential Computing (AISCC'24)  
Reviewer, ACL Rolling Review (2025)  
Reviewer, IEEE Transactions on Privacy and Security (TOPS'26)  
Reviewer, IEEE Transactions on Information Forensics and Security (TIFS'24)  
Reviewer, Computers & Security (2024)  
Artifact Evaluation Committee, Network and Distributed System Security Symposium (NDSS'25)  
Artifact Evaluation Committee, USENIX Security Symposium (Security'24, Security'25)  
Artifact Evaluation Committee, ACM Conference on Computer and Communications Security (CCS'24)  
External Reviewer, ACM Conference on Computer and Communications Security (CCS'24, CCS'25)  
External Reviewer, The Web Conference (TheWebConf'24)  
External Reviewer, IEEE Symposium on Security and Privacy (IEEE S&P'24, S&P'25)  
External Reviewer, IEEE European Symposium on Security and Privacy (EuroS&P'24, EuroS&P'25)  
External Reviewer, USENIX Workshop on Automotive and Autonomous Vehicle Security (VehicleSec'25)  
Volunteer, ACM Conference on Computer and Communications Security (CCS'25)

## TEACHING

---

### Teaching Assistant

*UIUC CS562: Advanced Topics in Security, Privacy and ML*

*Fall 2025*

### Teaching Assistant

*KAIST TS251: Data Science Overview*

*Spring 2020, Spring 2021*

## LANGUAGE SKILLS

---

**Chinese (Mandarin), Korean:** Native

**English:** Professional