Jiale Guan

guanjia@iu.edu | (872) 806-9820

Education

Indiana University Bloomington — Bloomington, IN
Ph.D. Program in Computer Science — Aug. 2020 – Dec. 2025
- Advisor: Luyi Xing and XiaoFeng Wang

Fudan University — Shanghai, China
B.Sc. in Information Security — Sep. 2016 – Jun. 2020
- Graduated with First Class Honors, ranked 1st

Research Interests

Security and Privacy in LLM Systems; AI for Security and Privacy

Experience

Bytedance — Beijing, China
Software Engineer Intern — Jul. 2024 – Sep. 2024
- Designed and implemented an LLM performance **benchmarking suite** based on a Two-Player Game model to evaluate privacy leakage in LLM inference pipelines, providing in-depth analysis of privacy risks across academic and industrial inference frameworks.
- Developed a **privacy-preserving** large language model inference pipeline for on-device and Private Cloud Compute-compliant environments, with a strong focus on optimizing memory management, data transmission, and scheduling.
- Built a **static analysis** tool to identify and mitigate privacy risks in LLM inference pipelines.
- Awarded **Best Intern** for contributions to privacy-compliant LLM inference; delivered a presentation summarizing results and recommendations to the team.

Indiana University Bloomington — Bloomington, IN
Research Assistant — Aug. 2020 – Present
- Explored the use of **LLM agent systems** to exacerbate side-channel information leakage by expanding the attack surface, effectively bypassing system-level privacy constraints.
- Designed and implemented a **LangChain-based agent pipeline** to develop a violation detection tool for Apple's privacy manifest constraints, enabling dynamic and comprehensive privacy compliance testing.
- Utilized **machine learning** to analyze multi-channel side-channel leakage in iOS, achieving 94.1% detection accuracy and proposing strategies to balance privacy and performance.

SAP Lab China — Shanghai, China
Software Engineer Intern — Sep. 2019 – Mar. 2020
- Developed an automated waste sorting system using Node.js, Redis, and RabbitMQ, presented as a demo at the 2nd China International Import Expo.
- Enhanced cloud storage system performance by designing a novel cache replacement algorithm, resulting in two approved patents.

Publication

- Jiale Guan, Yuhang Zhang, Linhai Song. "Privacy-Preserving LLM Serving: An Empirical Study on Private Inference for Large Language Models", Under Review.
- Jiale Guan, Fares Alharbi, Xueqiang Wang, Xiaojing Liao, Luyi Xing. "Privacy in Pieces: Evaluating Component-Level Adherence to iOS Privacy Manifests", The Network and Distributed System Security Symposium, 2025.
- Jiale Guan, Zihao Wang, XiaoFeng Wang, Wenhao Wang, Luyi Xing, Fares Alharbi. "The Danger of Minimum Exposures: Understanding Cross-App Information Leaks on iOS through Multi-Side-Channel Learning", The ACM Conference on Computer and Communications Security, 2023.
- Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, Luyi Xing. "Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels at Scale", USENIX Security Symposium, 2023.
- Luyi Xing, Xin'an Zhou, Jiale Guan, Zhiyun Qian. "The Dilemma in IoT Access Control: Novel Attacks and Design Challenges in Mobile-as-a-Gateway IoT", Black Hat Asia, 2023.
- Xin'an Zhou, Jiale Guan, Luyi Xing, Zhiyun Qian. "Perils and Mitigation of Security Risks of Cooperation in Mobile-as-a-Gateway IoT", The ACM Conference on Computer and Communications Security, 2022.
- Wanyue Xu, Liwang Zhu, Jiale Guan, Zuobai Zhang, Zhongzhi Zhang. "Effects of Stubbornness on Opinion Dynamics", The ACM International Conference on Information & Knowledge Management, 2022.

Awards

Best Intern Award 2024
Computer Science AI of the Year 2024
Luddy School Summer Fellowship 2023
Tianchi AI Security Challenger Program (6/26490) 2021
Shanghai Scholarship (Awarded to top 30 students university-wide) 2019

CVEs

CVE-2022-23776, CVE-2022-36268, CVE-2022-26262, CVE-2022-37192, CVE-2022-37193

Teaching

Associate Instructor

- Systems & Protocol Security & Information Assurance. SP23, SP24
- Cyber Defense Competitions. FA22, FA23

Skills

- **Language**: Python, C/C++, Rust, Swift, JavaScript
- **LLM**: LangChain, vLLM, DeepSpeed, PyTorch
- **Web (Full-Stack Experience)**: HTML/CSS, JavaScript, Node.js, MongoDB, Selenium
- **Security Tools**: Ghidra, IDA Pro, Hopper, Burp Suite, Frida, Radare2