管佳乐

chialekuan@gmail.com | +1 (872) 806-9820

教育背景

印第安纳大学布鲁明顿分校 2020 年 8 月 — 2025 年 5 月
计算机科学博士项目 布鲁明顿, 印第安纳州
- 导师: Luyi Xing 和 XiaoFeng Wang

复旦大学 2016 年 9 月 — 2020 年 6 月
信息安全理学学士 上海, 中国
- 专业排名第一
- 获得复旦大学一等奖学金，上海奖学金(30/3000+)等奖学金

研究领域

Advancing Privacy Compliance and Optimization in Mobile and LLM Inference

论文发表

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

经历

华为 2012 实验室 2024 年 7 月 — 2024 年 10 月
网络安全与隐私保护工程师实习 北京, 中国
- 调查 PCC（隐私云计算）要求对现有大规模语言模型（LLM）推理服务优化的影响，全面分析了在内存管理、数据传输、请求批处理、并行优化、任务调度及披露合规等多个维度中所面临的挑战。针对每个优化维度，详细探讨了不同方案在隐私保护方面可能引发的风险和挑战，并提出了相应的应对策略。

- 对现有的 LLM 服务优化算法、开源框架及企业内部框架进行了对比分析，重点评估其在私有云环境下如何满足无状态计算和不可针对性（非目标化）的严格要求。通过对比不同方案在性能、隐私合规和安全性方面的表现，进一步探讨了在特定私有云架构下的适应性及其隐私挑战。

印第安纳大学布鲁明顿分校 2020 年 8 月 – 至今
研究助理 布鲁明顿, 印第安纳州

- 研究了苹果的隐私标签违规检测工具，揭示了 iOS SDK 和应用程序的不合规性，以及隐私违规在软件供应链中的传播。
- 研究了 iOS 上的跨应用信息泄露，并提出了一种多侧信道学习方法，可以将前台应用的检测准确率提高到 94.1%。项目获得了苹果安全团队的关注，相关演示可见项目网站。作为共同第一作者，论文发表于 ACM CCS 2023。
- 研究了 iOS SDK 和应用程序的隐私合规性，并提出了一种方法来评估隐私清单、软件供应链一致性和动态行为实践一致性的一致性。

SAP 2019 年 9 月 – 2020 年 3 月
软件开发实习 上海, 中国

- 通过开发新的缓存替换算法，优化了云存储系统的性能。
- 提交了两份集团专利申请。

奖项

Computer Science AI of the Year Award 2024
天池杯 AI 安全挑战者项目二等奖 2021

- Phase VII: Robust Mark Detection.
- Ranked 6th out of 26490 participants.

上海奖学金 2019

CVEs

CVE–2022–23776
CVE–2022–36268
CVE–2022–26262
CVE–2022–37192
CVE–2022–37193

教学

助教

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

学术服务

Artifact Evaluation Committee

- ACM Conference on Computer and Communications Security 2023

External Reviewer

- ACM Conference on Computer and Communications Security 2023
- ACM Workshop on Secure and Trustworthy Superapps 2023