刘子正

性别: 男　　出生日期: 1996年2月25日

邮箱: lzz@purdue.edu　　电话/微信: (+86) 135-0403-9426　　个人主页：https://cangjie103.github.io

教育背景

2021.08-目前	普渡大学，美国	计算机科学	博士在读
	导师: Bharat K. Bhargava (IEEE Life Fellow)		
2018.08-2019.12	哥伦比亚大学，美国	计算机科学	理学硕士
	导师: Henning Schulzrinne (ACM Fellow, IEEE Fellow)		
2017.08-2018.05	伊利诺伊大学芝加哥分校，美国	电气与计算机工程	国家留学基金委公派交换生
2014.09-2018.06	东北大学，中国	计算机科学与技术	学士

科研经历

2021.08-目前　　分布式系统/人工智能/移动网络 隐私与安全　　普渡大学

项目1 (隐私计算 / 人工智能安全): 利用多方安全计算设计一种具备隐私保护和拜占安全的去中心化联邦学习聚合方案. (合作: 罗格斯大学，苏黎世联邦理工学院)

项目2 (卫星通信 / 人工智能安全): 基于星地网络特有的威胁模型，为其设计通信信道感知的联邦学习投毒攻击的防御方案. (合作: 弗吉尼亚理工大学)

项目3 (形式验证 / 协同攻击): 在分布式系统中，使用形式验证的手段为基于机器学习的入侵检测系统提供关于潜在的协同攻击的证据，以提高检测系统对协同攻击检测的准确率. (合作: 弗吉尼亚理工大学)

项目4 (车联网安全): 在车联网基于地理位置的路由协议 GeoNetworking (ETSI EN 302 636 / IEEE 1609.3) 中发现安全漏洞. 设计实验评估隐患危害并提出解决方案.

项目5 (5G网络安全): 将 5G 移动宽带网络中已发现的攻击模式总结为 3GPP 技术规范文档中的措辞模式. 用自然语言处理技术在新兴 5G 技术 (物联网，车联网，无人机网络) 的技术规范文档中找到潜在安全漏洞，以便针对这些技术在按照规范文档实施之前修补安全漏洞.

2019.01-2019.12　　基于家用路由器的物联网设备信息保护系统　　哥伦比亚大学

项目 通过机器学习方法检测来自家用物联网设备的潜在信息泄漏或流量异常，实时更新路由器端防火墙以保护用户信息及设备的隐私与安全.

2017.08-2018.05　　基于数据融合的室内导航系统　　伊利诺伊大学芝加哥分校

本科毕设 基于 Raspberry Pi 开发手持室内导航系统，解决 GPS 或其他卫星定位系统在室内信号较弱的问题. 手持导航仪收集来自陀螺仪、WiFi 接口等信号源的信号数据. 通过数据融合和校正算法判断用户在室内所在位置. 用 Dijkstra 算法为用户提供当前位置到目的地的最短路径.

学术成果

- **Liu, Zizheng**, Bharat K. Bhargava, and Nagender Aneja. "STARFed: Link-Aware Defense Against Poisoning Attacks in Satellite-Terrestrial Federated Learning." IEEE Transactions on Network Science and Engineering (2025). (IF:7.9, JCR1区，博士项目2) [PDF]
- **Liu, Zizheng**, Shaan Shekhar, and Chunyi Peng. “Breaking Geographic Routing Among Connected Vehicles.” In 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 42-54. IEEE, 2023. (CCF B，录用率: 47/235 = 20%，博士项目4) [PDF]
- **Liu, Zizheng**, Bharat K. Bhargava, Nagender Aneja, and Ruy de Oliveira. "RDCollab: Reasoning and Detecting CollaborativeAttacks in Autonomous UAV Networks." 投稿至 IEEE Transactions on Dependable and Secure Computing. (博士项目3)
- Zhang, Zhehui, Yanbing Liu, Qianru Li, **Zizheng Liu**, Chunyi Peng, and Songwu Lu. “Dependent Misconfigurations in 5G/4.5 G Radio Resource Control.” ACM CoNext 2023 (Proceedings of the ACM on Networking (PACMNET)) (2023). (CCF B，录用率: 4/41 = 9.8%) [PDF]
- **Liu, Zizheng**, and Chunyi Peng. “Poster: Security Analysis for Emerging Cellular Network Technologies.” NSF AI Institute for Future Edge Networks and Distributed Intelligence (AI-EDGE Institute) Annual Meeting (2022). (博士项目5) [PDF]
- **Liu, Zizheng**, and Chunyi Peng. “Quality Measurement over Quality Data Reuse in Cellular Networks.” 2nd NSF Workshop on Overcoming Measurement Barriers to Internet Research (WOMBIR-2) (2021). [PDF]
- **Liu, Zizheng**, Gaston Ormazabal, Henning Schulzrinne, and Aman Singh. "Pitfalls of MUD File Generation and Design Flaws of Smart Home IoT Devices " 技术报告 (2019). (硕士科研项目) [PDF]

学术兼职

期刊评审: IEEE Transactions on Information Forensics and Security, Computer Networks, Computer Communications

荣誉奖励

- 受邀参加加州大学伯克利分校 Simons Institute 举办的 “Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation” 项目中的安全计算研讨会 (2025)
- 普渡大学计算机系优秀助教奖 (10/277, 2024秋季学期)
- DSN’23 Student Travel Grant (2023)
- 伊利诺伊大学芝加哥分校工程博览会优秀本科毕业设计 (2018)
- 中国国家留学基金委优秀本科生国际交流奖学金 (2017)
- 本科期间两次获得国家奖学金 (2015, 2017), 多次获得校一或二等奖学金 (2015, 2016, 2017)

教学经历

- 普渡大学 CS448 关系数据库系统导论 助教: 2024, 2025, 2026春季学期
- 普渡大学 CS176 Python 数据工程 助教: 2024, 2025秋季学期
- 普渡大学 CS536 数据通信与计算机网络 助教: 2023春季学期
- 哥伦比亚大学 COMS4701 人工智能 助教: 2019秋季学期

技能特长

- 博士及硕士期间参与多领域 (网络安全, 人工智能安全, 密码学) 安全与隐私相关的项目, 具有在交叉领域中寻找并解决科研问题的能力. 其中包括多次参与美国国家科学基金会 (NSF) 资助项目, 与世界一流大学计算机科学家和密码学家保持长期且活跃的科研合作关系, 具有国际学术视野.
- 博士及硕士期间具有丰富的助教经验. 助教课程包括本科生级别和研究生级别课程, 课程规模从小班 (十余人) 到大班 (百余人) 不等. 助教期间与教授和学生皆保持良好关系并在未来学期常被教授指认再次助教其课程, 曾获优秀助教奖(获奖率3.6%). 具备专业英语水平 (托福 108/120, GRE 325/340) 和全英文授课的能力.
- 具有全栈解决应用密码学科研问题的能力 (设计协议, 证明, 编程实现, 写作). 目前主要从事的科研工作为将多方安全计算和零知识证明中的密码学技术应用到人工智能中涉及的隐私计算场景.
- 熟悉 3GPP, ETSI 以及 IEEE 发布的多种网络协议栈的技术规范. 在博士和硕士期间都有搭建实验室规模的有线或无线网络测试平台以验证科研想法的经验.