Changjia Zhu

940-205-1786 changjiazhu@gmail.com Google Scholar LinkedIn

Education

University of South Florida **Jan. 2023 – Present**
Ph.D., Major: Computer Science & Engineering, GPA: 4.0/4.0 (A+) *Tampa, FL*

University of North Texas **Aug. 2021 – Dec. 2022**
M.S., Major: Inorganic Chemistry, GPA: 4.0/4.0 (A+) *Denton, TX*

University of Science and Technology of China **Aug. 2016 – Jun. 2020**
B.S., Major: Material Chemistry *Hefei, China*

Technical Skills

Programming: Python, C, SQL, Bash
Machine Learning & NLP: Deep Learning, PyTorch, Hugging Face Transformers, TensorFlow, BERTopic
Large Language Models: Prompt Engineering, Font-based Indirect Prompt Injection, MCP Tools
Cloud & Systems: Docker, Kubernetes, Google Cloud, AWS, Azure, Linux (capability, syscall, cache benchmarking)
Security & Networking: Server Side-channel Analysis (Memory Bus Locking, Prime+Probe,), CPU Cache Analysis, Wireless Signal Operation, LLM Safeguard
Data & Visualization: Pandas, NumPy, Plotly, Scrapfly
Collaboration & Tools: Git, VS Code, Overleaf, Docker Compose, Google Colab
Languages: English (fluent), Mandarin (native)

Work Experience

Graduate Teaching/Research Assistant **Jan. 2023 – Present**
University of South Florida

Graduate Teaching/Research Assistant **Aug. 2021 – Dec. 2022**
University of North Texas

Graduate Research Assistant **Jul. 2020 – May 2021**
Zhejiang University

Research Projects

WILD Attack: Stealthy Undermining of Wi-Fi-Based Geolocation Through Remote Crowdsourced Data Injection
Jan. 2025 – Present

- Proposed a novel remote localization spoofing method that manipulates Wi-Fi-based positioning systems without requiring physical proximity to the target.
- Designed strategies to remotely gather Wi-Fi environment data and selectively influence geolocation outcomes across multiple platforms, including Google, Apple, WiGLE, and A-Map.
- Analyzed the behavior of widely used geolocation services and identified vulnerabilities in their reliance on unauthenticated, crowd-sourced data. Demonstrated that falsified data can tamper with or erase entries in geolocation service databases.
- Evaluated the feasibility of infrastructure-level geolocation manipulation, demonstrating real-world impacts such as large-scale denial-of-service, ride-hailing misdirection, and GPS-less device poisoning.

When Your Reviewer is an LLM: Biases, Divergence, and Prompt Injection Risks
Mar. 2025 – Sep. 2025

- Conducted the first systematic evaluation of LLMs (GPT-5-mini) as academic peer reviewers, benchmarking them against human reviewers using 1,441 papers from ICLR 2023 and NeurIPS 2022.
- Applied topic modeling and clustering to compare the thematic emphases of human vs. LLM reviewers, revealing systematic differences in how the research papers' strengths and weaknesses are identified.
- Investigated LLM susceptibility to prompt injection by embedding hidden adversarial instructions into PDF submissions.
- Demonstrated that specific instructions forced the LLM to assign a perfect 10/10 score in 30% of peer review cases and to list only a single paper weakness in another 30% of cases.

Invisible Prompts, Visible Threats: Malicious Font Injection in External Resources for Large Language Models
Jan. 2025 – Aug. 2025

- Proposed a novel strategy leveraging malicious fonts to embed hidden adversarial prompts invisible to human readers but fully parsed by LLMs.

- Designed two critical attack scenarios: (i) Malicious Content Relay and (ii) Sensitive Data Leakage with MCP tools.
- Showed that in GPT-4o and Claude-3, hidden adversarial prompts resources achieved up to 70% success rates and could exfiltrate user information via MCP tools, leaking 100% of low-sensitivity data and 30% of high-sensitivity data.
- Identified deficiencies in current LLM security frameworks and highlighted the urgent need for mechanisms that ensure both semantic and visual content integrity.

Shadow Hunting in the Cloud: Unearthing and Undermining the Target Application in a Vast Ocean of Servers
Jan. 2023 – Dec. 2024

- Proposed a novel paradigm to exploit co-location risks in Function-as-a-Service platforms, including Google Cloud Run, AWS Lambda, and Azure Function Apps.
- Developed the Server Coverage Navigator to analyze and bypass opaque server isolation mechanisms, enabling attacker instances to cover all available servers in cloud providers' data centers, with scalability up to 1,000 servers.
- Designed the Target Victim Locator to identify attacker/victim server sharing using only public API interactions within 15 seconds, and enabled the proliferation of at least three attacker instances to co-locate with the target victim for follow-up server sharing attacks.
- Demonstrated real-world impact including multi-vector denial-of-service and side-channel Prime+Probe attacks.

Selected Research Publications

1. **Zhu, C.**; Gera, P.; Han, X.; Neal, T.; Liu, Y. WILD Attack: Stealthy Undermining of Wi-Fi-Based Geolocation Through Remote Crowdsourced Data Injection. (Accepted by USENIX Security 2026) (1st author)
2. **Zhu, C.**; Xiong, J.; Lin, S.; Zhang, C.; Zhang, Y.; Liu, Y.; Li, L. Invisible Prompts, Visible Threats: Malicious Font Injection in External Resources for Large Language Models. (Accepted by EMNLP 2025 Findings) (Co-1st author) [PDF]
3. **Zhu, C.**; Xiong, J.; Lu, Z.; Liu, Y. Shadow Hunting in the Cloud: Unearthing and Undermining the Target Application in a Vast Ocean of Servers. (Under Review by IEEE S&P 2026) (1st author)
4. **Zhu, C.**; Ma, R.; Lu, Z.; Liu, Y.; Li, L. When Your Reviewer is an LLM: Biases, Divergence, and Prompt Injection Risks. (Under Review by Computers in Human Behavior) (1st author) [PDF]
5. **Zhu, C.**; Zhang, C.; Xiong, J.; Xu, X.; Li, L.; Liu, Y.; Lu, Z. Guardians and Offenders: A Survey on Harmful Content Generation and Safety Mitigation. arXiv preprint arXiv:2508.05775. 2025. (Under Review by ACM TIST) (Co-1st author) [PDF]
6. Wang, J.; **Zhu, C.**; Zhou, Y.; Li, L.; He, X.; Xiong, J. COGNITION: From Evaluation to Defense against Multimodal LLM CAPTCHA Solvers. (Under Review by USENIX Security 2026) [PDF]
7. Xiong, J.; Jiang, Z.; Xu, X.; Zhang, C.; **Zhu, C.**; Wang, N.; Wei, M.; Lu, Z.; Liu, Y.; Li, L. Large Language Models and Social Media Information Integrity: Opportunities, Challenges, and Research Directions. 2025. (Under Revision by ACM Computing Survey) [PDF]
8. **Zhu, C.**; Xian, W.; Song, Y.; Zuo, X.; Wang, Y.; Ma, S.; Sun, Q. Manipulating charge density in nanofluidic membranes for optimal osmotic energy production density. Adv. Funct. Mater. 2022, 32, 2109210. (1st author) [PDF]
9. **Zhu, C.**; Zuo, X.; Xian, W.; Guo, Q.; Meng, Q.-W.; Wang, S.; Ma, S.; Sun, Q. Integration of thermoelectric conversion with reverse electrodialysis for mitigating ion concentration polarization and achieving enhanced output power density. ACS Energy Lett. 2022. (1st author) [PDF]
10. Liu, X.; **Zhu, C.**; Yin, J.; Li, J.; Zhang, Z.; Li, J.; Shui, F.; You, Z.; Shi, Z.; Li, B.; Bu, X.-H.; Nafady, A.; Ma, S. Installation of synergistic binding sites onto porous organic polymers for efficient removal of perfluorooctanoic acid. Nat. Commun. 2022. (2nd author) [PDF]

Professional Services

Conference Reviewer: INFOCOM 2025
Conference Sub-Reviewer: CCS (2023, 2025, 2026), ICCCN 2025, INFOCOM (2024, 2026), CNS (2023, 2024), ACSAC (2023, 2024), USENIX (2023, 2024)
Journal Reviewer: ACM TOPS, Chemical Society Review, Nano Energy, Materials Horizons, Desalination, Journal of Power Sources, Crystal Growth & Design, Separation & Purification Technology, Materials Today Energy, Materials Today Communications, Polymer Chemistry, RSC Advances, Nanoscale Advances, European Polymer Journal, Journal of Applied Polymer Science, Environmental Research Communications, New Journal of Chemistry