# Nanzi Yang

Postdoctoral Associate, Department of Computer Science & Engineering, University of Minnesota
Email: yang9467@umn.edu
Google Scholar: Nanzi Yang

## Research Interests

Trustworthy AI systems; AI system security; cloud security; security of AI agents and orchestration protocols (MCP, A2A).

## Education

**Xidian University**, Xi'an, China
Ph.D. in Cyberspace Security 2019 – 2024

**Xidian University**, Xi'an, China
B.S. in Information Engineering 2014 – 2018

## Employment

**University of Minnesota**, Minneapolis, MN, USA
Postdoctoral Associate, Department of Computer Science 2024 – Present
Host: Professor Kangjie Lu

## Peer-reviewed Publications

### Refereed Publications

1. The Dark Side of Flexibility: Detecting Risky Permission Chaining Attacks in Serverless Applications
   Xunqi Liu*, **Nanzi Yang***, Chang Li, Jinku Li, Jianfeng Ma, and Kangjie Lu(*co-first authors).
   To appear in Proceedings of the 2026 Annual Network and Distributed System Security Symposium (NDSS'26), 2026.

2. Dangers Behind Access Control: Understanding and Exploiting Implicit Permissions in Kubernetes.
   **Nanzi Yang**, Xingyu Liu, Wenbo Shen, Jinku Li, and Kangjie Lu.
   In Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS'25), 2025

3. Towards Understanding and Defeating Abstract Resource Attacks for Container Platforms.
   Wenbo Shen, Yifei Wu, Yutian Yang, Qirui Liu, **Nanzi Yang**, Jinku Li, Kangjie Lu, and Jianfeng Ma
   IEEE Transactions on Dependable and Secure Computing(TDSC'25), 2025.

4. Take Over the Whole Cluster: Attacking Kubernetes via Excessive Permissions of Third-party Applications.
   **Nanzi Yang**, Wenbo Shen, Jinku Li, Xunqi Liu, Xin Guo, and Jianfeng Ma.
   In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS'23), 2023.

5. Attacks are forwarded: breaking the isolation of MicroVM-based containers through operation forwarding.
   Jietao Xiao*, **Nanzi Yang***, Wenbo Shen, Jinku Li, Xin Guo, Zhiqiang Dong, Fei Xie, and Jianfeng Ma(*co-first authors).
   In Proceedings of the 32nd USENIX Security Symposium (Security'23), 2023

6. Demons in the Shared Kernel: Abstract Resource Attacks Against OS-level Virtualization.
   **Nanzi Yang***, Wenbo Shen*, Jinku Li, Yutian Yang, Kangjie Lu, Jietao Xiao, Tianyu Zhou, Chenggang Qin, Wang Yu, Jianfeng Ma, and Kui Ren(*co-first authors).
   In Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS'21), 2021.

### Under Review

1. Compatibility at a Cost: Systematic Discovery and Exploitation of MCP Clause-Compliance Vulnerabilities.
   **Nanzi Yang**, Weiheng Bai, and Kangjie Lu.
   Under review at IEEE Symposium on Security and Privacy (S&P)

## Industry-Recognized Security Impact

- Discovered and responsibly disclosed **10+ CVEs** in production cloud systems, Selected CVE IDs include:
  - Abstract resource attacks on microVM-based containers (CVE-2022-0358, RedHat, score 7, moderate severity);
  - Kubernetes RBAC and applications (e.g., CVE-2024-9779, RedHat, score 7.5, high severity);
  - Serverless platforms and function-level permission chaining (e.g., CVE-2024-37293, AWS Github, score 7.8, high severity).
- Received two **security bounties from Google Bug Hunter** for vulnerabilities in Kubernetes-related cloud services.

## Grant and Proposal Writing Experience

- Contributed substantially to the preparation of **three faculty-led funding proposals** on AI system security and cloud infrastructure hardening, submitted to AWS and Google security funding award programs (drafting technical approach, milestones, and evaluation plans).

## Mentoring and Teaching Experience

**Guest Lecturer**
*CSCI 5271: Introduction to Computer Security*, University of Minnesota, Fall 2025

**Teaching Assistant**
*Computer System Security*, Xidian University, Summer 2022

**Research Mentoring**

- Mentored four Master's students during Ph.D, and two mentored projects led to **co-first-author publications** at top-tier security conferences (Security'23, NDSS'26).
- Mentoring two Ph.D students during PostDoc in UMN, one student is expected to graduate next year.

## Service

- Reviewer, IEEE Transactions on Communications
- Assisting my PostDoc advisor in reviewing manuscripts for NDSS, ACM CCS, and RAID.

## Awards and Honors

- National Scholarship (Awarded by the Ministry of Education, China), 2022
- National Scholarship (Awarded by the Ministry of Education, China), 2023
- Google Security Bug Bounty

## Talks and Presentations

- Demons in the Shared Kernel: Abstract Resource Attacks Against OS-level Virtualization, CCS 2021.
- Attacks are forwarded: breaking the isolation of MicroVM-based containers through operation, USENIX Security 2023.
- Take Over the Whole Cluster: Attacking Kubernetes via Excessive Permissions of Third-party Applications, CCS 2023.
- Dangers Behind Access Control: Understanding and Exploiting Implicit Permissions in Kubernetes Applications, CCS 2025.