

YUXIA ZHAN

60 Fifth Avenue, New York, NY 10011

✉ yuxia.zhan@nyu.edu 🏠 kalamoo.github.io 🎓 Google Scholar

EDUCATION

New York University

Ph.D. in Computer Science

Advisor: Prof. Michael Walfish

New York, NY, USA

Sept. 2024 - June 2029 (Expected)

Shanghai Jiao Tong University

M.Eng. in Computer Science (GPA: 3.92 / 4.0)

Summa Cum Laude

Advisor: Prof. Haojin Zhu @ NSEC Lab

Shanghai, China

Sept. 2021 - Mar. 2024

Shanghai Jiao Tong University

B.Eng. in Computer Science (GPA: 89.23 / 100)

IEEE Pilot Class and Zhiyuan Honors Program

Shanghai, China

Sept. 2017 - June 2021

RESEARCH INTEREST

My current research focuses on **verifiable computing** (especially attestation), including approaches with **trusted hardware** (e.g., TPM, SGX, TDX, SEV-SNP, and GPU TEE) and without them (e.g., relying on **zero-knowledge proofs**).

Previously, I have investigated privacy challenges in VR/AR/XR environments and safety concerns in cyber-physical systems (CPS). Besides, I am passionate about any work that attempts to address the privacy issues within the advertising ecosystem.

PUBLICATIONS

Yuxia Zhan, Yan Meng, Lu Zhou, Yichang Xiong, Xiaokuan Zhang, Lichuan Ma, Guoxing Chen, Qingqi Pei, Haojin Zhu, “VPVet: Vetting Privacy Policies of Virtual Reality Apps”, in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2024. [\[link\]](#)

Yuxia Zhan, Yan Meng, Lu Zhou, Haojin Zhu, “Vetting Privacy Policies in VR: A Data Minimization Principle Perspective”, in *IEEE Conference on Computer Communications Workshops (INFOCOM WK-SHPS)*, 2023. [\[link\]](#) 🏆 **Best Poster Award**

Yan Meng, **Yuxia Zhan**, Jiachun Li, Suguo Du, Haojin Zhu, Xuemin Shen “De-Anonymizing Avatars in Virtual Reality: Attacks and Countermeasures”, in *IEEE Transactions on Mobile Computing (TMC)*, 2024. [\[link\]](#)

Muchen Pan, Yan Meng, **Yuxia Zhan**, Guoxing Chen, Haojin Zhu, “PipID: Light-Pupillary Response Based User Authentication for Virtual Reality”, submitted to *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2025. (To appear)

Raymond Muller, Ruoyu Song, Chenyi Wang, **Yuxia Zhan**, Jean-Philippe Monteuiis, Yanmao Man, Ming Li, Ryan Gerdes, Jonathan Petit, Z. Berkay Celik, “Investigating Physical Latency Attacks against Camera-based Perception”, accepted by *IEEE Symposium on Security and Privacy (S&P)* 2025. [\[link\]](#)

Jiachun Li, Yan Meng, **Yuxia Zhan**, Le Zhang, Haojin Zhu, “Dangers behind Charging VR Devices: Hidden Side Channel Attacks via Charging Cables”, in *IEEE Transactions on Information Forensics and Security (TIFS)*, 2024. [\[link\]](#)

Yan Meng, **Yuxia Zhan**, Jiachun Li, Suguo Du, Haojin Zhu, Xuemin Sherman Shen, “De-anonymization Attacks on Metaverse”, in *IEEE Conference on Computer Communications (INFOCOM)*, 2023. [\[link\]](#)

Brandon Falk, Yan Meng, **Yuxia Zhan**, Haojin Zhu, “POSTER: Reavatar: Virtual Reality De-anonymization Attack through Correlating Movement Signatures”, in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2021. [\[link\]](#)

EXPERIENCES

Research Intern @ IMDEA Software

Hosted by Prof. Juan Caballero and mentored by Dr. Srdjan Matic
Large-scale measurement on disposable email ecosystem.

*Madrid, Spain
Apr. 2024 - Aug. 2024*

Summer Intern @ Purdue

Hosted by Z. Berkay Celik
Latency attack towards object detection (OD) system.

*West Lafayette, IN, USA (Remote)
June 2023 - Jan. 2024*

Research Assistant @ SJTU

Advisor: Prof. Haojin Zhu
Compliance of VR APPs' privacy policies.
Behaviour-based de-anonymization attack in VR.

*Shanghai, China
Sept. 2020 - Mar. 2024*

TEACHING

CSCI-UA.0202: Operating Systems (Undergrad)

Instructor: Prof. Michael Walfish

NYU, Fall 2025

CSCI-UA.0310: Basic Algorithms (Undergrad)

Instructor: Prof. Areeba Ikram

NYU, Summer 2025

CS7350: Network Security (Graduate)

Instructor: Prof. Haojin Zhu

SJTU, Spring 2023

HONORS AND AWARDS

- | | |
|---|--|
| • SOSP Student Travel Grant | <i>ACM SIGOPS, 2024</i> |
| • Graduated with Distinction | <i>Graduate School of SJTU, 2024</i> |
| • National Scholarship for Graduate Students (Top 1%) | <i>Ministry of Education (China), 2023</i> |
| • ACM CCS iMentor Student Travel Grant | <i>ACM CCS, 2023</i> |
| • Best Poster Award (Solely selected from all poster submissions) | <i>IEEE INFOCOM, 2023</i> |
| • First-Class Master's Academic Scholarship | <i>Graduate School of SJTU, 2021-2023</i> |
| • Zhiyuan Honors Degree of Engineering (Top 3%) | <i>Zhiyuan College of SJTU, 2021</i> |
| • Zhiyuan Honorary Scholarship (Top 5%) | <i>Zhiyuan College of SJTU, 2017-2021</i> |
| • Special Freshman Scholarship | <i>SJTU, 2017</i> |

MISCELLANEOUS

- **Languages:** Mandarin Chinese (native), English (professional fluency), Spanish (beginner).
- Stray animal rescuer and cat foster.
- Tennis, football (soccer), hiking.

Last updated: 2025-10-25