# MENG CHEN

meng.chen@zju.edu.cn
**College of Computer Science and Technology, Zhejiang University**

## EDUCATION BACKGROUND

**Zhejiang University** — Hangzhou, China
Ph.D. in Cyber Science and Technology, advised by Dr. Li Lu — Sep. 2021 – Jun. 2026 (expected)

**Zhejiang University** — Hangzhou, China
B.E. in Software Engineering, GPA: 3.89/4 (Top 5%) — Sep. 2017 – Jun. 2021

## RESEARCH INTEREST

My research interests lie in AI security with a specific focus on adversarial examples and backdoor learning, especially their practical threats to intelligent audio systems. By "*debugging*" deep learning, i.e., investigating failures in learning-based systems, my research seeks to help build more trustworthy AI systems in security-critical tasks.

## RESEARCH EXPERIENCE

**Research Assistant** — Nov. 2020 – Present
Advised by Dr. Li Lu. — MUSLab, Zhejiang University

- Mainly worked on speech signal processing and adversarial example attacks against voiceprint recognition.
- Finished my undergraduate thesis entitled "Impersonation Attack on Voiceprint Authentication Systems Based on Adversarial Examples", which was awarded the *Outstanding Bachelor Dissertation Award*.

## PUBLICATIONS

[1] **Meng Chen**, Xiangyu Xu, Li Lu*, Zhongjie Ba, Feng Lin, Kui Ren. "Devil in the Room: Triggering Audio Backdoors in the Physical World", in *Proceedings of the 33rd USENIX Security Symposium (USENIX Security'24)* , pp.1-18, Philadelphia, PA, USA, 2024. (Artifacts in preparation) [PDF] [Demo]

[2] **Meng Chen**, Li Lu*, Jiadi Yu, Zhongjie Ba, Feng Lin, Kui Ren. "AdvReverb: Rethinking the Stealthiness of Audio Adversarial Examples to Human Perception", *IEEE Transactions on Information Forensics and Security (IEEE TIFS)* , vol.19, pp.1948-1962, 2024. [PDF] [Demo] [Code]

[3] **Meng Chen**, Li Lu*, Junhao Wang, Jiadi Yu, Yingying Chen, Zhibo Wang, Zhongjie Ba, Feng Lin, Kui Ren. "VoiceCloak: Adversarial Example Enabled Voice De-Identification with Balanced Privacy and Utility", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (ACM IMWUT)* , vol.7, no.2, pp.48:1-48:21, 2023. [PDF] [Demo] [Blog]

[4] **Meng Chen**, Li Lu*, Jiadi Yu, Yingying Chen, Zhongjie Ba, Feng Lin, Kui Ren. "A Non-intrusive and Adaptive Speaker De-Identification Scheme Using Adversarial Examples", in *Proceedings of the 28th ACM Annual International Conference On Mobile Computing And Networking (ACM MobiCom'22)* , pp.853-855, Sydney, NSW, Australia, 2022. (**Best Poster Runner-up Award**) [PDF]

[5] **Meng Chen**, Li Lu*, Zhongjie Ba, Kui Ren. "PhoneyTalker: An Out-of-the-Box Toolkit for Adversarial Example Attack on Speaker Recognition", in *Proceedings of the 41st IEEE International Conference on Computer Communications (IEEE INFOCOM'22)* , pp.1419-1428, London, United Kingdom, 2022. [PDF]

[6] Lei Wang, **Meng Chen**, Li Lu*, Zhongjie Ba, Feng Lin, Kui Ren. "VoiceListener: A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (ACM IMWUT)* , vol.7, no.1, pp.32:1-32:22, 2023. [PDF] [Code]

[7] Qianniu Chen, **Meng Chen**, Li Lu*, Jiadi Yu, Yingying Chen, Zhibo Wang, Zhongjie Ba, Feng Lin, Kui Ren. "Push the Limit of Adversarial Example Attack on Speaker Recognition in Physical Domain", in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems (ACM SenSys'22)* , pp.710-724, Boston, MA, USA, 2022. [PDF]

## Professional Services

**Journal Reviewer:** IEEE Transactions on Network Science and Engineering (TNSE)

## Honors & Awards

**Longhu Scholarship**, Zhejiang University 2023
**Best Poster Runner-up Award**, ACM MobiCom 2022
**Student Conference Grant**, IEEE INFOCOM 2022
**Suzhou Yucai Scholarship**, Zhejiang University 2022
**Outstanding Bachelor Dissertation Award**, Zhejiang University 2021
**Outstanding Graduate**, Zhejiang University 2021
**First-class Scholarship**, Top 3%, Zhejiang University 2020
**Provincial Government Scholarship**, Top 3%, Zhejiang Province 2019