Peng Huang

penghuang@zju.edu.cn ·

https://desperado1999.github.io

Education

Zhejiang University (ZJU), Hangzhou, China 2020 – Present

Ph.D. Candidate in CyberSpace Security. (Supervised by Prof. Zhongjie ba)

Zhejiang University (ZJU), Hangzhou, China 2016 – 2020

B.S. in Information Science and Electrical Engineering

Research Interests

Internet of Things, Signal Processing, Privacy-Preserving Technologies.

Publications

[NDSS'23] InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise.
Peng Huang, *Yao Wei, Peng Cheng, Zhonejie Ba, Li Lu, Feng Lin, Fan Zhang, and Kui Ren. In 30th Annual Network and Distributed System Security Symposium (NDSS), 2023. (Acceptance rate: 16.2%)*

[Okland'24] Text-CRS: A Generalized Certified Robustness Framework against Textual Adversarial Attacks.
Xinyu Zhang, Hanbin Hong, Yuan Hong, ***Peng Huang****, Binghui Wang, Zhongjie Ba, Kui Ren. In 45th IEEE Symposium on Security and Privacy (S&P), 2024, San Francisco, CA, USA. (Accepted)*

[Okland'24] ALIF: Low-Cost Adversarial Audio Attacks on Black-Box Speech Platforms using Linguistic Features.
Peng Cheng, Yuwei Wang, ***Peng Huang****, Zhongjie Ba, Xiaodong Lin, Feng Lin, Li Lu, Kui Ren. In 45th IEEE Symposium on Security and Privacy (S&P), 2024, San Francisco, CA, USA. (Accepted)*

Honors and Awards

2023 Outstanding Graduate Student of the Year [2022-2023, Zhejiang University]

Professional Services

Reviewer: IEEE Internet of Things Journal(IoT-J); ACM Transactions on Internet of Things (TIOT).

Presentations

Conference Talk [NDSS'23] Mar. 2023
InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise