Yuanda Wang

517-721-9800 | yuandawang.msu@gmail.com | Linkedin | Personal Website

Education

Michigan State University East Lansing, Michigan
Doctor of Philosophy in Computer Science 2020.01 – 2024.12 *(expected)*

◇ Advisor: Dr. Qiben Yan

North China Electric Power University Beijing, China
M.S. in Electrical Engineering 2016 – 2019

Xi'an Jiaotong University Xi'an, China
B.S. in Electrical Engineering 2012 – 2016

Research Experience

SEcure and Intelligent Things Lab, Michigan State University January 2020 – Present
Department of Computer Science and Engineering, Ph.D. student

- Advisor: Dr. Qiben Yan
- Research area: Generative AI security, Speech AI, LLM security, Side-channel attacks, IoT security.

Knox Lab, Samsung Research America September 2022 – December 2022
Research intern

- Advisor: Dr. Xun Chen
- Research area: Mobile Security, AI security.

Camputer (Camera & Computer) Lab, Duke Kunshan University July 2019 – October 2019
Research intern

- Advisor: Dr. David J. Brady, professor from ECE department, Duke University.
- Research area: Computer Vision, High-performance Camera Array, Deep Learning.

Technical Skills

Programming Languages: Python, C++, C, JavaScript, MATLAB, Verilog, SQL.
Framework and Platform: PyTorch, TensorFlow, Numpy, CUDA, Jupyter.
Operating Systems: Ubuntu, MacOS, Windows.

Highlighted Projects

ClearMask | Generative AI Security

- ClearMask is a noise-free defense mechanism to protect human speech from malicious voice synthesis.
- This work is submitted to USENIX Security 2025.

ClearAI | Healthcare & Speech Enhancement

- ClearAI is an AI-driven speech enhancement tool to improve the speech quality of Parkinson's disease patients.
- We combine audio style transfer and speech reconstruction to focus on hypophonic speech enhancement.

VSMask | Generative AI Security

- VSMask is a real-time defense against voice synthesis attack. It can add imperceptible perturbation into human speech sample and then mislead voice synthesis models.
- By leveraging predictive generation model and universal adversarial perturbation, VSMask can protect your voice in real-time scenarios, like phone call, online meetings, and real-world talks.

GhostTalk Attack | Mobile Security & Side-channel Attack

- GhostTalk is the first attack leveraging malicious charging cables to inject inaudible voice command to smartphone voice assistants, and it can also eavesdrop inaudible audio signal from smartphones.
- We successfully launch GhostTalk attack on 9 mainstream smartphones and achieve 100% attack success rate. Besides malicious command injection, GhostTalk can also hack private information from voice assistants.

SDR–Lite | Wireless & Cross-Technology Communication

- SDR–Lite can enable all commercial WiFi devices with SDR receiver functions without any firmware modification. It can be used for multiple applications like RF fingerprinting, spectrum monitoring and ZigBee decoding.

Publications

Conference

- *ClearAI: AI-Driven Speech Enhancement for Hypophonic Speech*
  Yuanda Wang, Qiben Yan, Thea Knowles, Daryn Cushnie-Sparrow.
  2024 IEEE International Conference on E-health Networking, Application & Services (**HealthCom**), 2024.
- *WavePurifier: Purifying Audio Adversarial Examples via Hierarchical Diffusion Models*
  Hanqing Guo, Guangjing Wang, Bocheng Chen,**Yuanda Wang**, Xiao Zhang, Xun Chen, Qiben Yan, Li Xiao.
  International Conference on Mobile Computing and Networking (**MobiCom**), 2024.
- *Protecting Activity Sensing Data Privacy Using Hierarchical Information Dissociation*
  Guangjing Wang, Hanqing Guo, **Yuanda Wang**, Bocheng Chen, Ce Zhou, Qiben Yan.
  2024 IEEE Conference on Communications and Network Security (**CNS**), 2024.
- *Understanding Multi-Turn Toxic Behaviors in Open-Domain Chatbots*
  Bocheng Chen, Guangjing Wang, Hanqing Guo, **Yuanda Wang**, Qiben Yan.
  The 26th International Symposium on Research in Attacks, Intrusions and Defenses(**RAID**) , 2023.
- *PhantomSound: Black-Box, Query-Efficient Audio Adversarial Attack via Split-Second Phoneme Injection*
  Hanqing Guo, Guangjing Wang, **Yuanda Wang**, Bocheng Chen, Qiben Yan.
  The 26th International Symposium on Research in Attacks, Intrusions and Defenses(**RAID**) , 2023.
- *VSMask: Defending Against Voice Synthesis Attack via Real-Time Predictive Perturbation*
  Yuanda Wang, Hanqing Guo, Guangjing Wang, Bocheng Chen, Qiben Yan.
  The 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks(**WiSec**) , 2023.
- *SpecPatch: Human-In-The-Loop Adversarial Audio Spectrogram Patch Attack on Speech Recognition*
  Hanqing Guo, **Yuanda Wang**, Nikolay Ivanov, Li Xiao, Qiben Yan.
  The ACM Conference on Computer and Communications Security (**CCS**) , 2022. (Accept ratio: 22.0%)
  Best Paper Honorable Mention
- *GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line*
  Yuanda Wang, Hanqing Guo, Qiben Yan.
  The Network and Distributed System Security (**NDSS**) Symposium, 2022. (Accept ratio: 16.2%)
- *SDR Receiver Using Commodity WiFi via Physical-layer Signal Reconstruction*
  Woojae Jeong, Jinhwan Jung, **Yuanda Wang**, Shuai Wang, Seokwon Yang, Qiben Yan, Yung Yi, Song Min Kim.
  International Conference on Mobile Computing and Networking (**MobiCom**), 2020. (Accept ratio: 16.1%)

Journal

- *Beyond Boundaries: A Comprehensive Survey of Transferable Attacks on AI Systems* (under review)
  Guangjing Wang, Ce Zhou, **Yuanda Wang**, Bocheng Chen, Hanqing Guo, Qiben Yan.
- *A Practical Survey on Emerging Threats from AI-driven Voice Attacks: How Vulnerable are Commercial Voice Control Systems?* (under review)
  Yuanda Wang, Qiben Yan, Nick Ivanov, Xun Chen.
- *URadio: Wideband Ultrasound Communication System for Smart Home Applications*
  Qiben Yan, Qi Xia, **Yuanda Wang**, Pan Zhou, Huacheng Zeng.
  IEEE Internet of Things Journal, January 2022.

Award

Dissertation Completion Fellowship (DCF) 2024, Michigan State University.
The ACM Conference on Computer and Communications Security (CCS) 2022: Best Paper Honorable Mention.
IEEE Conference on Communications and Network Security (CNS) 2020: Student Travel Award.

Invited Talk

Michigan State University Graduate Student Seminar: The Great Outage — Facebook Global Outage on Oct.4.