Yi Wu

Ph.D. Candidate
Department of Electrical Engineering & Computer Science
University of Tennessee, Knoxville

Phone: +1 (732) 640 4149
Email: ywu83@vols.utk.edu
Home: http://web.eecs.utk.edu/~ywu83/

Education

2019–2024 (Expected)	Ph.D. Candidate, Computer Science, University of Tennessee, Knoxville
	Advisor: Dr. Jian Liu
2017–2019	M.Sc., Computer Engineering, Rutgers University
	Advisor: Dr. Yingying Chen
2014–2018	B.Sc., Automation, University of Electronic Science and Technology of China

Research Interests

My research interests encompass the areas of **Embedded/Wearable Computational Sensing Software**, **Cybersecurity & Privacy**, and **Smart Fitness Tracking**. Particularly, I utilize machine learning and signal processing techniques to develop advanced software for various domains, including facial tracking and fitness tracking. Additionally, I develop malware to conduct security analysis of IoT devices such as AR/VR headsets, wireless chargers, and voice assistants.

Work Experience

Research Intern at Truveta. Sept 2023 - Present, Seattle, WA (Remote)

LLM Pre-training & Fine-tuning, Medical Image De-identification.

- Pre-trained a BERT encoder from scratch leveraging over 450,000 clinical notes data.
- Fine-tune the pre-trained model for clinical notes normalization and other downstream tasks.
- Developed a Transformer-based network to classify whether the detected texts contain personal identifiable information.

Research Intern at Snap Inc. May 2023 - Aug 2023, New York, NY

- Developed an MLP-based encoder to encode places on SnapMap into location embeddings.
- Developed a Transformer-based encoder to encode the user's location history into high-level user embeddings.
- Enhanced the location identification accuracy on SnapMap by 189% in simulation through mapping user embeddings to location embeddings leveraging contrastive learning.

Research Experience

Embedded/Wearable Computational Sensing Software

- **EMG-based 3D Facial Reconstruction.** Build a wearable biosensing software that can continuously track 2D facial landmarks and further render 3D facial animations through lightweight single-ear biosensors. **(MobiCom 2021)**
- **mmWave-based Respiration Monitoring.** Developed a CNN-based sequence-to-sequence network to reconstruct fine-grained respiratory waveform from coarse-grained mmWave radar signal.
- **Multi-modal Running Gait Analysis.** Developed a multi-modal and multi-task running gait analysis system that can monitor the runner's cadence, foot pressure distribution, and strike pattern leveraging acoustic-IMU sensor fusion.
- **Cycling Fitness Tracking.** Designed an innovative smart seat pad that continuously and unobtrusively track five cycling-specific metrics leveraging under-hip fabric sensors. **(IMWUT/UbiComp 2023)**

Security & Privacy Analysis and Corresponding Defenses on Virtual Reality

- **Keystroke Inference.** Developed a malware and corresponding mitigation that can stealthy log VR sensory data in background, and further infer the user's keystroke, including both random passwords and natural language paragraphs. **(S&P/Oakland 2023)**
- **Speech Eavesdropping.** Developed a malware and corresponding mitigation that can stealthy log AR/VR sensory data in background, and infer sensitive information (e.g., speech content) from live human speech. **(MobiCom 2021)**

Security & Privacy Analysis and Corresponding Defenses on Voice Assistants

- **Advanced Hidden Voice Attack.** Present an advanced hidden voice attack and corresponding mitigation against ASR software that can bypass classifier-based defense. **(AsiaCCS 2021)**
- **Universal & Synchronization-free Attack.** Present a systematic approach to generate subsecond audio adversarial perturbations to alter the recognition results of audio inputs in a targeted and synchronization-free manner. **(CCS 2020)**
- **Semi-black-box Attack.** Propose the first semi-black-box attack against the Kaldi ASR system that can force it to yield false predictions. **(DySPAN 2019)**

Security & Privacy Analysis and Corresponding Defenses on Wireless Charging

- **Hijacking Attack.** Design and implement a hijacking attack and corresponding mitigation in which the adversary can completely take control of the charging process through injecting deliberately manipulated Qi messages into the communication channel.
- **Eavesdropping Attack.** Design and implement an eavesdropping attack and corresponding mitigation in which the adversary can snoop Qi messages and further infer the activities of the smartphone being charged. **(ACSAC 2021)**

Awards & Honors

2023 Outstanding Graduate Research Assistant of UTK
2023 S&P Student Travel Award
2022 ACM SigMobile Research Highlights 2022
2021 ACSAC Student Conference Grant
2021 CCS Student Conference Grant
2019 DySPAN Student Travel Award
2015 Merit Scholarship of UESTC

Publications

Conferences

[1] **Yi Wu**, Luis Gonzalez, Zhenning Yang, Gregory Croisdale, Cagadas Karatas, Jian Liu, "SmarCyPad: A Smart Seat Pad for Cycling Fitness Tracking Leveraging Low-cost Conductive Fabric Sensors", in Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (**IMWUT/Ubicomp 2023**), Cancún, Mexico, November 2023.

[2] **Yi Wu**, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, Yingying Chen, "Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards", in Proceedings of the 44th IEEE Symposium on Security and Privacy (**S&P/Oakland 2023**), San Francisco, United States, May 2023.

[3] **Yi Wu**, Vimal Kakaraparthi, Zhuohang Li, Tien Pham, Jian Liu, Phuc Nguyen, "BioFace-3D: Continuous 3D Facial Reconstruction Through Lightweight Single-ear Biosensors", in Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (**MobiCom 2021**), New Orleans, United States, January 2022. **(Acceptance Rate: 17.4%) (ACM SigMobile Research Highlights 2022)**

[4] Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton R. Walker, **Yi Wu**, Jian Liu, Nitesh Saxena, Yingying Chen, Jiadi Yu, "Face-Mic: Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR Motion Sensors", in Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (**MobiCom 2021**), New Orleans, United States, January 2022. **(Acceptance Rate: 17.4%)**

[5] **Yi Wu**, Zhuohang Li, Nicholas Van Nostrand, Jian Liu,"Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging", in Proceedings of the 37th Annual Computer Security Applications Conference (**ACSAC 2021**), December 2021. **(Acceptance Rate: 24.5%)**

[6] **Yi Wu**, Xiangyu Xu, Payton R. Walker, Jian Liu, Nitesh Saxena, Yingying Chen, Jiadi Yu, "HVAC: Evading Classifier-based Defenses in Hidden Voice Attacks", in Proceedings of the 16th ACM ASIA Conference on Computer and Communications Security (**AsiaCCS 2021**), Hong Kong, China, June 2021. **(Acceptance Rate: 18.5%)**

[7] Zhuohang Li, **Yi Wu**, Jian Liu, Yingying Chen, Bo Yuan, "AdvPulse: Universal, Synchronization-free, and Targeted Audio Adversarial Attacks via Subsecond Perturbations", in Proceedings of the 27th ACM Conference on Computer and Communications Security (**CCS 2020**), November 2020. **(Acceptance Rate: 16.9%)**

[8] **Yi Wu**, Jian Liu, Yingying Chen, Jerry Cheng, "Semi-black-box Attacks Against Speech Recognition Systems Using Adversarial Samples", in Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks (**DySPAN 2019**), Newark, New Jersey, November 2019.

Joural Paper & Magazine Article

[1] **Yi Wu**, Xiande Zhang, Tianhao Wu, Bing Zhou, Phuc Nguyen, Jian Liu, "3D Facial Tracking and User Authentication through Lightweight Single-ear Biosensors", IEEE Transactions on Mobile Computing (Under Submission), 2024.

[2] **Yi Wu**, Vimal Kakaraparthi, Zhuohang Li, Tien Pham, Jian Liu, Phuc Nguyen, "BioFace-3D: 3D Facial Tracking and Animation via Single-ear Wearable Biosensors", ACM GetMobile, 2022.

Posters

[1] **Yi Wu**, Zhuohang Li, Nicholas Van Nostrand, Jian Liu, "Poster Abstract: Security and Privacy in the Age of Cordless Power World", in Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems (**SenSys 2020**), Yokohama, Japan, November 2020.

Patents

[1] Jian Liu, VP Nguyen, **Yi Wu**, Xiande Zhang, Tianhao Wu, "User Authentication and Photo-realistic Facial Animation Rendering via Ear-worn Biosensors", U.S. Provisional Application, September, 2023.

[2] Jian Liu, Çağdaş KARATAŞ, **Yi Wu**, Luis Alonso González Villalobos, "A Smart Seat Pad for Cycling Fitness Tracking Leveraging Low-cost Conductive Fabric Sensors", U.S. Provisional Application, July 2023.

[3] Jian Liu, Phuc Nguyen, **Yi Wu**, Vimal Kakaraparthi, Zhuohang Li, Tien Pham, "SYSTEMS AND METHODS FOR HUMAN-MOUNTED BIOSENSORS AND PROCESSING BIOSENSOR INFORMATION", U.S. Provisional Patent Application 63/376, 854, September 2022.

Teaching Experience

Teaching Assistant, The University of Tennessee, Knoxville

- COSC 356 Computer Architecture (Fall 2019, Spring 2020)
- COSC 361 Operating Systems (Fall 2020, Fall 2021, Fall 2022, Spring 2023)
- ECE 315 Signals and Systems I (Spring 2022)
- ECE 469/569 Mobile/Embedded System Security (Spring 2021, Fall 2021)

Skills

- **Programming**: Python, C++, Javascript, Matlab, Kotlin, HTML, CSS, Latex, Git, Linux, SQL
- **Tools & Libraries**: PyTorch, Keras, HuggingFace, OpenCV, Scikit-learn, Numpy, Scipy, Pandas, Unittest
- **Cloud Computing Platforms**: AWS, GCP, Azure

Professional Activities

Technical Program Committee: IEEE COMPSAC 2023

Reviewer: The Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) (2022, 2023), IEEE Transactions on Image Processing (2022), IEEE Transactions on Mobile Computing (2023), IEEE Transactions on Neural Systems & Rehabilitation Engineering (2023), IEEE COMPSAC (2023)