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/

Research Interests

My research interests encompass the areas of **mobile sensing & computing**, **human-computer interaction**, and **cyber-security & privacy**. Particularly, I utilize machine learning and signal processing techniques to create next-generation applications for human-computer interaction, smart health monitoring, and identifying potential security/privacy issues on IoT devices (e.g., AR/VR headsets, wireless chargers, and voice assistants).

Skills

- **Programming**: Python, Javascript, Matlab, HTML, CSS, Latex, Git, Linux
- **Toolkit**: PyTorch, Keras, Scikit-learn, Numpy, Scipy, Pandas

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 Experience

3D Facial Reconstruction Through Lightweight Single-ear Biosensors

- Built a wearable biosensing system that can continuously track 2D facial landmarks, and further render 3D facial animations leveraging 1D CNN.
- Extensive experiments involving multiple participants and various settings show that the system can accurately track 53 facial landmarks with only 1.85 mm average error and 3.38% normalized mean error.

Cycling Fitness Tracking Leveraging Under-hip Fabric Sensors

- Design an innovative smart seat pad that can continuously and unobtrusively track five cycling-specific metrics, including cadence, per-leg stability, leg strength balance, riding position, and knee joint angle leveraging fabric sensors.
- Our system can accurately estimate the cycling cadence with an average error of 0.98 rounds per minute, quantify the cycling stability for each leg, detect cycling imbalance, distinguish five riding positions with an accuracy of 95.22%, and continuously track the knee joint angle with an average mean error as low as 8.18 degrees.

Inferring Keystrokes on VR Devices Leveraging Unrestricted Motion-Position Sensors

- Present an eavesdropping attack which leverages motion-position sensors on VR to infer user's keystroke.
- Our attack can recover the user's passwords with up to 84.9% recognition accuracy if three attempts are allowed and achieve an average of 87.1% word recognition rate for paragraph inference.

Inferring Live Speech and Speaker Identity via Subtle Facial Dynamics Captured by AR/VR IMU Sensor

- Present an eavesdropping attack which leverages speech-associated subtle facial dynamics captured by zero-permission motion sensors in AR/VR headsets to infer highly sensitive information from live human speech, including speaker gender, identity, and speech content leveraging 2D CNN.

Security and Privacy Vulnerability Analysis of Qi Wireless Charging

- Design and implement a hijacking attack in which the adversary can completely take control of the charging process.
- Design and implement an eavesdropping attack in which the adversary can snoop Qi messages and further infer the activities of the smartphone being charged.

Security and Privacy Vulnerability Analysis Against Voice Assistants

- Present an advanced hidden voice attack against ASR systems that can bypass classifier-based defense.
- Propose the first semi-black-box attack against Kaldi ASR system that can force it to yield false predictions.

Awards & Honors

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

Journals & Magazines

[1] **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.

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 Techonologies (**IMWUT 2023**), **(Under Major Revision)**

[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 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.

Professional Activities

Technical Program Committee: IEEE COMPSAC 2023

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