Yuxin Chen

yxchen@uchicago.edu | yxchen.me | github.com/y-x-c

Education

University of Chicago — Chicago, USA
Ph.D. in Computer Science — *Sep. 2017 – July 2022*

University of Chicago — Chicago, USA
M.S. in Computer Science — *Sep. 2017 – June 2020*

Fudan University — Shanghai, China
B.S. in Computer Science and Technology — *Sep. 2013 – June 2017*

Industry Experience

Research Scientist, Bootcamp in Ads Core ML team, *Meta* — *Oct. 2022 - Nov. 2022*
(1) Design and develop a efficiency-aware ML model authoring library, which supports various critical projects, significantly improves dev. & execution efficiency (20% speed-up), and enables flexible AutoML explorations;
(2) Build a foundation model which can serve multiple ads domains and prediction tasks.

Ph.D. Software Engineer Intern, Ads Core ML team, *Meta* — *May 2021 - Aug. 2021*
(1) Design and develop a novel recommendation model architecture that is capable of elastically allocating model capacity to each example during inference, leading to $> 0.08\%$ revenue gain without further machine cost;
(2) Implement and explore sparsely-activated large capacity models (e.g., *switch transformer*), which lay the foundation of a series of further explorations.

Research

My research lies at the intersection of **machine learning** and **personal privacy**, where I design and apply machine learning models for personal privacy attacks and defense.

General keystroke inference attack via two-layer self-supervised DNNs.
(1) Develop a video-based keystroke inference attack using a single RGB camera, with no prior knowledge;
(2) Propose a two-layer *self-supervised* approach, where noisy finger tracking data from a video are processed, labeled and filtered to train *3DCNN keystroke inference models* that operate on the same video.

Novel active biometric authentication using DNN anomaly detection and classification.
(1) Propose to use electrical muscle stimulation (EMS) for active biometric authentication;
(2) Develope a robust authentication system that integrates two *DNN* models to resist both impersonation and replay attacks. Specifically, a *VAE-based anomaly detector* is built to verify whether a response was produced by the user and a *CNN challenge classifier* is built to detect replay attacks.

Usable voice identity protection tool based on voice conversion models.
(1) Study voice identity protection against voice cloning attacks;
(2) Develope a usable anonymization tool based on state-of-the-art *voice conversion models* that allows users to customize protected voices based on both vocal perception and protection strength.

Voice content protection leveraging weaknesses in microphones and ASRs.
(1) Design and engineer a wearable microphone jammer that can prevent *automatic speech recognition (ASR)* models from secretly recognizing voice content;
(2) Leverage the fact that when exposed to ultrasonic noise, commodity microphones will leak the noise into the audible range and disrupt ASRs.

Adversarial motion sensing using model fitting with data sifting.
(1) Demonstrate a reconnaissance attack that can continuously monitors and locates human inside a private property by sniffing ambient WiFi signals;
(2) Propose a consistency-based data sifting algorithm to improve model fitting results.

Publication

"Towards a General Video-based Keystroke Inference Attack". Zhuolin Yang*, **Yuxin Chen***, Zain Sarwar, Hadleigh Schwartz, Ben Y. Zhao, Haitao Zheng. In Proceedings of USENIX Security Symposium **(USENIX)**, Anaheim CA, August 2023.

"User Authentication via Electrical Muscle Stimulation". **Yuxin Chen**, Zhuolin Yang, Ruben Abbou, Pedro Lopes, Ben Y. Zhao, Haitao Zheng. In Proceedings of ACM CHI Conference on Human Factors in Computing Systems **(CHI)**, Yokohama, Japan, May 2021.

"Wearable Microphone Jamming". **Yuxin Chen***, Huiying Li*, Shan-Yuan Teng*, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, Haitao Zheng. In Proceedings of ACM CHI Conference on Human Factors in Computing Systems **(CHI)**, Honolulu, HI, April 2020. (**Best Paper Honorable Mention Award**)

"Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors". Yanzi Zhu, Zhujun Xiao, **Yuxin Chen**, Max Liu, Ben Y. Zhao, Haitao Zheng. In Proceedings of Network & Distributed System Security Symposium **(NDSS)**, 2020.

"Addressing Training Bias via Automated Image Annotation". Zhujun Xiao, Yanzi Zhu, **Yuxin Chen**, Ben Y. Zhao, Junchen Jiang, Haitao Zheng. arXiv:1809.10242v2, 2018.

"Acceptability of Voice Protection Tools". **Yuxin Chen**, Zain Sarwar, Wenxin Ding, Christian Cianfarani, Jiaqi Gao, Lea Schönherr, Ben Y. Zhao, Haitao Zheng. In submission.

** denotes equal contribution*

Awards

Finalist, Fast Company's 2020 Innovation by Design Awards *2020*

Honorable Mention Award, ACM CHI Conference on Human Factors in Computing Systems *2020*

University Unrestricted Fellowship, University of Chicago *2019*

Finalist, Interdisciplinary Context in Modeling *2016*

Outstanding Student, Fudan University *2015*

Bronze Medal, National Olympiad in Informatics, Chinese Ministry of Education *2012*

First Prize, National Olympiad in Informatics Province, Chinese Ministry of Education *2012*

Academic Experience

Research Assistant, SAND Lab, University of Chicago *Sep. 2017 – July 2022*
Supervised by Prof. Haitao Zheng and Prof. Ben Y. Zhao

Teaching Assistant, University of Chicago
CS234 Mobile Computing *Winter 2018, Winter 2019*
CS151 Introduction to Computer Science I *Autumn 2017*

Talks

User Authentication via Electrical Muscle Stimulation *May 2021*
ACM CHI Conference on Human Factors in Computing Systems (CHI), Yokohama, Japan.

Wearable Microphone Jamming and Beyond *June 2020*
ACM Chicago CHI Chapter, Chicago, IL, USA.

Wearable Microphone Jamming *May 2020*
ACM CHI Conference on Human Factors in Computing Systems (CHI), Honolulu, HI, USA.

Technical Skills

Programming: Python, C/C++, JavaScript, HTML/CSS, SQL, MATLAB, Assembly
Libraries: PyTorch, NumPy, Tensorflow, Caffe, Scikit-learn, OpenCV