



Dr. Yufei Chen

<https://yfchen1994.github.io>

Department of Computer Science, City University of Hong Kong
No.83, Tat Chee Ave, Kowloon Tong, Kowloon, Hong Kong SAR, China
✉ yufeichen8[AT]cityu.edu.hk  [Google Scholar](#)  [GitHub](#)

EDUCATION

City University of Hong Kong
Ph.D., Computer Science
Department of Computer Science

Sept. 2019 - Jun. 2024
Supervisor: Cong Wang

Xi'an Jiaotong University
Ph.D., Control Science and Engineering
Ministry of Education Key Lab for Intelligent Networks & Network Security (MOE KLINNS)

Feb. 2018 - Dec. 2023
Supervisor: Chao Shen

Xi'an Jiaotong University
Master's Student, Control Science and Engineering
MOE KLINNS

Sept. 2016 - Jan. 2018
Supervisor: Chao Shen

Xi'an Jiaotong University
B.Eng., Electrical Engineering
School of Electrical Engineering

Sept. 2012 - Jun. 2016

Xi'an Jiaotong University
B.B.A., Business Administration
School of Management

Feb. 2014 - Jun. 2016

PUBLICATIONS

I am currently a postdoc with City University of Hong Kong. I received my dual Ph.D. from City University of Hong Kong and Xi'an Jiaotong University. I also worked at Qihoo 360 as a research intern on intelligence security in 2018. My research interests include *data-driven cyber security*, *security and privacy issues of AI systems*, and *behavioral biometrics*. Recently I have published papers in journals and conferences in the area of AI security and behavioral analysis, including *USENIX Security*, *NDSS*, *NeurIPS*, *IEEE TDSC*, *IEEE TIFS*, *IEEE TNNLS*, etc.

Journals:

- [J1] Sen Peng, **Yufei Chen**, Jie Xu, Zizhuo Chen, Cong Wang, and Xiaohua Jia. "Intellectual Property Protection of DNN Models," *World Wide Web*, online published, 2022. DOI: 10.1007/s11280-022-01113-3.
- [J2] Kaidi Jin, Tianwei Zhang, Chao Shen, **Yufei Chen**, Ming Fan, Chenhao Lin, and Ting Liu. "Can We Mitigate Backdoor Attack Using Adversarial Detection Methods?," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, early access, 2022. DOI:10.1109/TDSC.2022.3194642.
- [J3] Xinyan Li, **Yufei Chen**, Cong Wang, and Chao Shen. "When Deep Learning Meets Differential Privacy: Privacy, Security, and More," *IEEE Network*, vol. 35, no. 6, pp. 148-155, 2021.
- [J4] **Yufei Chen**, Chao Shen, Cong Wang, Qixue Xiao, Kang Li, and Yu Chen. "Scaling Camouflage: Content Disguising Attack Against Computer Vision Applications," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 18, no. 5, pp. 2017-2028, 2021.
- [J5] Chao Shen, Zhao Wang, Chengxiang Si, **Yufei Chen**, and Xiaojie Su. "Waving Gesture Analysis for User Authentication in the Mobile Environment," *IEEE Network*, vol. 34, no. 2, Apr. 2020.
- [J6] **Yufei Chen**, Chao Shen, Qian Wang, Qi Li, Cong Wang, Shouling Ji, Kang Li, and Xiaohong Guan. "Security and Privacy Risks in Artificial Intelligence Systems," *Journal of Computer Research and Development*, vol. 56, no. 10, pp. 2135-2150, 2019. (*in Chinese*)

- [J7] Chao Shen, **Yufei Chen**, Yao Liu, and Xiaohong Guan. “Adaptive Human-Machine Interactive Behavior Analysis With Wrist-Worn Devices for Password Inference,” *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, vol. 29, no. 12, pp. 6292-6302, Dec. 2018.
- [J8] Chao Shen, **Yufei Chen**, and Xiaohong Guan. “Performance Evaluation of Implicit Smartphones Authentication via Sensor-Behavior Analysis,” *Information Sciences*, vol. 430-431, pp. 538-553, Mar. 2018.
- [J9] Chao Shen, **Yufei Chen**, Xiaohong Guan, and Roy Maxion. “Pattern-Growth based Mining Mouse-Interaction Behavior for an Active User Authentication System,” *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 17, no. 2, pp. 335-349, 2018.
- [J10] Chao Shen, **Yufei Chen**, Gengshan Yang, and Xiaohong Guan. “Toward Hand-Dominated Activity Recognition Systems With Wristband-Interaction Behavior Analysis,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 7, pp. 2501-2511, 2018.
- [J11] Chao Shen, Yuanxun Li, **Yufei Chen**, Xiaohong Guan, and Roy Maxion. “Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication,” *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 13, no. 1, Jan. 2018.
- [J12] **Yufei Chen** and Chao Shen. “Performance Analysis of Smartphone-Sensor Behavior for Human Activity Recognition,” *IEEE Access*, vol. 5, pp. 2169-3536, Mar. 2017.

Conferences:

- [C1] Xuanqi Gao, Juan Zhai, Shiqing Ma, Chao Shen, **Yufei Chen**, and Shiwei Wang. “CILITE: Towards Fairer Class-based Incremental Learning by Dataset and Training Refinement,” in *Proceedings of 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*, 2023.
- [C2] **Yufei Chen**, Chao Shen, Yun Shen, Cong Wang, and Yang Zhang. “Amplifying Membership Exposure via Data Poisoning,” in *Proceedings of 36th Conference on Neural Information Processing Systems (NeurIPS 2022)*, 2022.
- [C3] **Yufei Chen**, Chao Shen, Cong Wang, and Yang Zhang. “Teacher Model Fingerprinting Attacks Against Transfer Learning,” in *Proceedings of 31st USENIX Security Symposium (USENIX Security ’22)*, Boston, MA, USA, Aug. 10-12, 2022.
- [C4] Xuanqi Gao, Juan Zhai, Shiqing Ma, Chao Shen, **Yufei Chen**, and Qian Wang. “FairNeuron: Improving Deep Neural Network Fairness with Adversary Games on Selective Neurons,” in *Proceedings of 44th International Conference on Software Engineering (ICSE 2022)*, 2022.
- [C5] Junhao Zhou*, **Yufei Chen***, Chao Shen, and Yang Zhang. “Property Inference Attacks Against GANs,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS 2022)*, 2022. (*:co-first authors)
- [C6] Qixue Xiao*, **Yufei Chen***, Chao Shen, Yu Chen, and Kang Li. “Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms,” in *Proceedings of 28th USENIX Security Symposium (USENIX Security ’19)*, Santa Clara, CA, USA, Aug. 14-16, 2019. (*:co-first authors)
- [C7] Chao Shen, Qi Lv, Zhao Wang, **Yufei Chen**, and Xiaohong Guan. “Hand-Interactive Behavior Analysis for User Authentication Systems with Wrist-Worn Devices,” in *Proceedings of 2018 International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS)*, Hangzhou, China, Aug. 16-19, 2018. (Best Paper Award)
- [C8] Xiaozi Liu, Chao Shen, and **Yufei Chen**. “Multi-source Interactive Behavior Analysis for Continuous User Authentication on Smartphones,” in *Proceedings of 2018 Chinese Conference on Biometric Recognition (CCBR)*, Urumqi, China, Aug. 11-12, 2018.
- [C9] Zhao Wang, Chao Shen, and **Yufei Chen**. “Handwaving Authentication: Unlocking Your Smart-watch Through Handwaving Biometrics,” in *Proceedings of 2017 Chinese Conference on Biometric Recognition (CCBR)*, Shenzhen, China, Oct. 28-29, 2017.
- [C10] Chao Shen, Ziqiang Ren, **Yufei Chen**, and Zhao Wang. “On Using Wearable Devices to Steal Your Passwords: A Fuzzy Inference Approach,” in *Proceedings of 2017 International Symposium*

on Cyberspace Safety and Security, Xi'an, China, Oct. 22-25, 2017.

- [C11] Zhanpei Jia, Chao Shen, Xiao Yi, **Yufei Chen**, Tianwen Yu, and Xiaohong Guan. "Big-data analysis of multi-source logs for anomaly detection on network-based system," in *Proceedings of 13th IEEE Conference on Automation Science and Engineering (CASE)*, Xi'an, China, Aug. 20-23, 2017.
- [C12] **Yufei Chen**, Chao Shen, Zhao Wang, and Tianwen Yu. "Modeling Interactive Sensor-Behavior with Smartphones for Implicit and Active User Authentication," in *Proceedings of 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, New Delhi, India, Feb. 22-24, 2017.
- [C13] Chao Shen, **Yufei Chen**, and Gengshan Yang. "On Motion-Sensor Behavior Analysis for Human-Activity Recognition via Smartphones," in *Proceedings of 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, Sendai, Japan, Feb. 29 - Mar. 2, 2016.

Patents:

- [P1] Chao Shen, **Yufei Chen**, Zhao Wang, Qi Lv, and Xiaohong Guan. An authentication method based on handwriting behavior via wearable devices, *Chinese Patent*. (CN107153780B).
- [P2] Chao Shen, **Yufei Chen**, Zhao Wang, Gengshan Yang, and Xiaohong Guan. An unlocking and authentication approach based on motion-sensor behavior of smartwatches, *Chinese Patent, Pending*. (CN107273728B).
- [P3] Yujuan Fang, Quan Zhou, **Yufei Chen**, Qihang Huang, Shuhong Wang, and Yikai Wang. Moving-static compatible wireless electric energy transmission system for electric automobile, *Chinese Patent*. (CN104816646B).

AWARDS & HONORS

- | | |
|---|-------------|
| • USENIX Security '22 Student Grant | Jul. 2022 |
| • Outstanding Presenter Award of the 14th USTC PhD Student Workshop | Nov. 2021 |
| • The Shaanxi Provincial Natural Science Award (First Class, 4/4) | Mar. 2021 |
| • National Scholarship for Ph.D. Student (Top 2%) | Dec. 2020 |
| • Outstanding Graduate of XJTU | 2019 - 2020 |
| • Cyber Security Scholarship | Oct. 2019 |
| • National Scholarship for Ph.D. Student (Top 2%) | Dec. 2018 |
| • National Scholarship for Master's Student (Top 2%) | Dec. 2017 |
| • Outstanding Graduate of XJTU | 2016 - 2017 |
| • Third Prize of China Graduate Mathematical Contest in Modeling | Dec. 2017 |
| • Third Prize of the 4th National Mobile Internet Application Development Innovation Contest | Nov. 2017 |
| • National Scholarship for Undergraduate Student (Top 2%) | Dec. 2015 |
| • Second Prize of 8th National University Student Social Practice and Science Contest on Energy Saving Emission Reduction | Aug. 2015 |
| • First Prize in 10th Xi'an High-tech "Challenge Cup" (Students Extracurricular Scientific Contest) in Shaanxi Province | Jun. 2015 |
| • First Prize of Physics Contest of XJTU | Mar. 2014 |
| • National Endeavor Scholarship (Top 5%) | Dec. 2013 |
| • Outstanding Undergraduate of XJTU | 2012 - 2016 |

ACADEMIC SERVICES

Journal Reviewer

- IEEE Transactions on Dependable and Secure Computing

- IEEE Transactions on Information Forensics and Security
- ACM Transactions on Privacy and Security
- IEEE Transactions on Mobile Computing
- IEEE Transactions on Neural Networks and Learning Systems
- IEEE Internet of Things Journal
- ACM Transactions on Sensor Networks
- Computers & Security
- Information Sciences

External Conference Reviewer

- 2024: USENIX Security, ESORICS
- 2023: USENIX Security, NDSS, CCS
- 2022: NDSS, ACSAC, RAID, AsiaCCS, ACNS
- 2021: ICICS, RAID, AsiaCCS