Yufei Chen

Postdoc
Department of Computer Science
City University of Hong Kong

(Last updated: March 2025)
Homepage: https://yfchen1994.github.io
Email: yufeichen8@cityu.edu.hk

EDUCATION

09/2019 – 06/2024 **City University of Hong Kong**, Hong Kong SAR, China
Ph.D. in Computer Science
Supervisor: Cong Wang

09/2016 – 12/2024 **Xi'an Jiaotong University**, China
Ph.D. in Control Science and Engineering
Supervisor: Chao Shen

09/2012 – 06/2016 **Xi'an Jiaotong University**, China
B.Eng. in Electrical Engineering

02/2014 – 06/2016 **Xi'an Jiaotong University**, China
B.B.A. in Business Administration

WORKING EXPERIENCES

06/2024 – present **City University of Hong Kong**, Hong Kong SAR, China
Postdoc
Department of Computer Science
Host: Cong Wang

03/2018 – 11/2018 **Qihoo 360**, China
Research Intern
Research Center for Intelligence Security
Supervisor: Kang Li

05/2015 – 08/2016 **Xi'an Jiaotong University**, China
Research Intern
Ministry of Education Key Lab for Intelligent Networks & Network Security
Supervisor: Chao Shen

PUBLICATIONS

(*: co-first authors)

Conference Papers

C15. Longxiang Wang*, Lei Xu*, **Yufei Chen**, Ying Zou, and Cong Wang. "ALERT: Machine Learning-Enhanced Risk Estimation for Databases Supporting Encrypted Queries," in ***Proceedings of 34th USENIX Security Symposium (USENIX Security)***, 2025.

C14. Sen Peng, **Yufei Chen**, Cong Wang, and Xiaohua Jia. "Intellectual Property Protection of Diffusion Models via the Watermark Diffusion Process," in ***Proceedings of 25th International Web Information Systems Engineering Conference (WISE)***, 2024.

C13. Xuanqi Gao, Juan Zhai, Shiqing Ma, Chao Shen, **Yufei Chen**, and Shiwei Wang. "CILIATE: 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.

C12. **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.

C11. **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)***, 2022.

C10. 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.

C9. 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.

C8. 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)***, 2019.

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)***, 2018.
Best Paper Award

C6. 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)***, 2018.

C5. Zhao Wang, Chao Shen, and **Yufei Chen**. "Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics," in ***Proceedings of 2017 Chinese Conference on Biometric Recognition (CCBR)***, 2017.

C4. 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***, 2017.

C3. 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)***, 2017.

C2. **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)***, 2017.

C1. 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)***, 2016.

Journal Articles

J12. Sen Peng, **Yufei Chen**, Jie Xu, Zizhuo Chen, Cong Wang, and Xiaohua Jia. “Intellectual Property Protection of DNN Models,” ***World Wide Web***, vol. 26, pp. 1877-1911, 2023.

J11. 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)***, vol. 20, no. 4, pp. 2867-2881, 2023.

J10. 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.

J9. **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.

J8. 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, pp. 57-63, 2020.

J7. **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)*

J6. 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, 2018.

J5. 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, 2018.

J4. 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.

J3. 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.

J2. 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, 2018.

J1. **Yufei Chen** and Chao Shen. "Performance Analysis of Smartphone-Sensor Behavior for Human Activity Recognition," ***IEEE Access***, vol. 5, pp. 2169-3536, 2017.

TEACHING

2025 Spring	CS6290 (Privacy-enhancing Technologies), PG, **Tutorial Lecturer**, CityUHK(DG)
2025 Spring	CS2310 (Computer Programming), UG, **Tutorial Lecturer**, CityUHK
2024 Fall	CS2311 (Computer Programming), UG, **Tutorial Lecturer**, CityUHK

AWARDS AND HONORS

11/2024	NeurIPS 2024 Top Reviewer (Top 10%)
07/2022	USENIX Security '22 Student Grant
11/2021	Outstanding Presenter Award of the 14th USTC PhD Student Workshop
03/2021	The Shaanxi Provincial Natural Science Award (First Class, 4/4)
12/2020	National Scholarship for Ph.D. Student (Top 0.2%)
06/2020	Outstanding Graduate Student of XJTU
10/2019	Cyber Security Scholarship (awarded annually to 100 graduate students nationwide)
12/2018	National Scholarship for Ph.D. Student (Top 0.2%)
12/2017	National Scholarship for Master's Student (Top 0.2%)
12/2015	National Scholarship for Undergraduate Student (Top 0.2%)
12/2013	National Endeavor Scholarship (Top 3%)
2012 – 2016	Outstanding Undergraduate Student of XJTU

SERVICES

PC Member \Reviewer	NeurIPS 2025, 2024 ICLR 2025 ICML 2025 AAAI 2025 AISTATS 2025 MSN 2024 SecTL-AsiaCCS: 2025, 2024, 2023

External Reviewer	USENIX Security 2024, 2023
	NDSS 2022
	ACM CCS 2023
	ESORICS 2024
	RAID 2022, 2021
	ACSAC 2022
	ACNS 2022
	AsiaCCS 2021
	ICICS 2021
Journal Reviewer	IEEE Transactions on Dependable and Secure Computing
	IEEE Transactions on Information Forensics and Security
	IEEE Transactions on Mobile Computing
	ACM Transactions on Privacy and Security
	IEEE Transactions on Neural Networks and Learning Systems
	IEEE Internet of Things Journal
	ACM Transactions on Sensor Networks
	Transactions on Machine Learning Research
	IEEE Transactions on Automation Science and Engineering
	Neural Networks
	Computers & Security
	Information Sciences