Yimin (Ian) Chen

ian_chen@uml.edu | 202-253-9480 | https://cs.uml.edu/ ichen1/ | Lowell, MA, 01854

Education

Arizona State University, Tempe, AZ 12/2018

- Ph.D. in Electrical Engineering, advised by Dr. Yanchao Zhang
- Dissertation: Security and privacy in mobile devices: Novel attacks and countermeasures

The Chinese University of Hong Kong, Hong Kong 04/2013

- M.Phil. in Electrical Engineering, advised by Dr. Hon Ki Tsang
- Thesis: Design and evaluation of high speed silicon waveguide

Peking University, Beijing 07/2010

- B.S. in Electronics and Information Science and Technology

Professional Experience

Tenure-Track Assistant Professor, Miner School of Computer and Information Sciences, University of Massachusetts Lowell, Lowell, MA 09/2021 – Present

Postdoctoral associate in the CNSR Lab, Department of Computer Science, Virginia Tech, Falls Church, VA 12/2019 – 08/2021

- Working on research and grant proposals on security and privacy in deep/meta learning
- Co-supervising three graduate students

Research engineer in the AI Security Lab, Tencent, Shenzhen 12/2018 – 11/2019

- Worked on research and implementation of multitask learning for consumer credit risk evaluation

Research assistant in the CNSG Lab, School of Electrical, Computer, and Energy Engineering, Arizona State University, Tempe 08/2013 – 12/2018

- Worked on security and privacy in mobile computing

Research assistant in the Department of Electrical Engineering, The Chinese University of Hong Kong, Hong Kong 08/2010 – 04/2013

- Worked on design and evaluation of high speed silicon waveguide

Research Interests

Security and privacy in deep/machine learning, Internet of things (IoT), smart health, edge computing, online social networks, and wireless networks

Selected Publications

Under review

1. Jiawei Xu, Ziqian Bi, **Yimin Chen**, and Tao Li. One conference paper on detecting human leaving gesture through mm-wave technology.
2. Pranathi Rayavaram, Santhosh Pothineni, **Yimin Chen**, Mohammad Arif Ul Alam, and Sashank Narain. One conference paper on efficient image retrieval systems.
3. Ning Wang, Shanghao Shi, **Yimin Chen**, Wenjing Lou, and Tomas Hou. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning. Submitted to IEEE Transactions on

Dependable and Secure Computing (TDSC).

Conference proceedings

1. Xin Yao, Yu Zhan, **Yimin Chen**, Fengxiao Tang, Ming Zhao, Enlang Li, and Yanchao Zhang. DUO: Stealthy Adversarial Example Attack on Video Retrieval Systems via Frame-Pixel Search. IEEE International Conference on Distributed Computing Systems (ICDCS), Hong Kong, China, July 2023.
2. Ning Wang, Yang Xiao, **Yimin Chen**, Ning Zhang, Wenjing Lou, and Y. Thomas Hou. Squeezing More Utility via Adaptive Clipping on Deferentially Private Gradients in Federated Meta-Learning. The Annual Computer Security Applications Conference (ACSAC), Austin, TX, Dec. 2022.
3. Jared Widberg, Sashank Narain, and **Yimin Chen**. Clang __usercall: Towards Native Support for User Defined Calling Conventions. ACM Symposium on the Foundations of Software Engineering (FSE), Singapore, Nov. 2022.
4. Yang Hu, Ning Wang, **Yimin Chen**, and Wenjing Lou. Transferability of Adversarial Examples in Machine Learning-based Malware Detection. IEEE Conference on Communications and Network Security (CNS), Austin, TX, Oct. 2022.
5. Ning Wang, Yang Xiao, **Yimin Chen**, Yang Hu, Wenjing Lou, and Y. Thomas Hou. FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations. ACM ASIA Conference on Computer and Communications Security (AsiaCCS), Virtual Conference, May 2022.
6. Ning Wang, **Yimin Chen**, Yang Xiao, Yang Hu, Wenjing Lou, and Y. Thomas Hou. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning. IEEE Conference on Computer Communications (INFOCOM), Virtual Conference, April 2022.
7. Ning Wang, **Yimin Chen**, Yang Hu, Wenjing Lou, and Y. Thomas Hou. MANDA: On adversarial example detection for network intrusion detection system. IEEE Conference on Computer Communications (INFOCOM), Virtual Conference, May 2021 (9 pages, acceptance ratio: 19.9%).
8. Dianqi Han, **Yimin Chen**, Tao Li, Rui Zhang, Yanchao Zhang, and Terri Hedgpeth. Proximity-Proof: Secure and usable two-factor mobile authentication. ACM Annual Conference on Mobile Computing and Networking (MobiCom), New Delhi, India, October 2018 (12 pages, acceptance ratio: 292/1395=20.9%).
9. **Yimin Chen**, Tao Li, Rui Zhang, Yanchao Zhang, and Terri Hedgpeth. EyeTell: Video-assisted touchscreen keystroke inference from eye movements. IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, May 2018 (17 pages, acceptance ratio: 63/549=11.5%).
10. Tao Li, **Yimin Chen**, Rui Zhang, Yanchao Zhang, and Terri Hedgpeth. Secure crowdsourced indoor positioning systems. IEEE Conference on Computer Communications (INFOCOM), Honolulu, HI, April 2018 (9 pages, acceptance ratio: 309/1606=19.2%).
11. **Yimin Chen**, Jingchao Sun, Xiaocong Jin, Tao Li, Rui Zhang, and Yanchao Zhang. Your face your heart: Secure mobile face authentication with photoplethysmograms. IEEE Conference on Computer Communications (INFOCOM), Atlanta, GA, May 2017 (9 pages, acceptance ratio: 292/1395=20.9%).
12. **Yimin Chen**, Xiaocong Jin, Jingchao Sun, Rui Zhang, and Yanchao Zhang. POWERFUL: Mobile app fingerprinting via power analysis. IEEE Conference on Computer Communications (INFOCOM), Atlanta, GA, May 2017 (9 pages, acceptance ratio: 292/1395=20.9%).
13. Xiaocong Jin, Rui Zhang, **Yimin Chen**, Tao Li, and Yanchao Zhang. DPSense: Differentially private crowdsourced spectrum sensing. ACM Conference on Computer and Communications Security (CCS), Vienna, Austria, October 2016 (12 pages, acceptance ratio: 137/831=16.5%).
14. Tao Li, **Yimin Chen**, Jingchao Sun, Xiaocong Jin, and Yanchao Zhang. iLock: Immediate and automatic locking of mobile devices against data theft. ACM Conference on Computer and Communications Security (CCS), Vienna, Austria, October 2016 (12 pages, acceptance ratio: 137/831=16.5%).
15. Jingchao Sun, Xiaocong Jin, **Yimin Chen**, Jinxue Zhang, Rui Zhang, and Yanchao Zhang. VISIBLE: Video-assisted keystroke inference from tablet backside motion. ISOC Network and Distributed

System Security Symposium (NDSS), San Diego, CA, February 2016 (14 pages, acceptance ratio: 60/389=15.4%).

16. **Yimin Chen**, Jingchao Sun, Rui Zhang, and Yanchao Zhang. Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. IEEE International Conference on Computer Communications (INFOCOM), Hong Kong, China, April 2015 (9 pages, acceptance ratio: 316/1640= 19.3%).

Journal article

1. Ning Wang, **Yimin Chen**, Yang Xiao, Yang Hu, Wenjing Lou, and Y. Thomas Hou. MANDA: On Adversarial Example Detection for Network Intrusion Detection System, IEEE Transactions on Dependable and Secure Computing, 2022.
2. Xindi Ma, Baopu Li, Qi Jiang, **Yimin Chen**, Sheng Gao, and Jianfeng Ma. NOSnoop: an Effective Collaborative Meta-Learning Scheme against Property Inference Attack. IEEE Internet of Things Journal, September 2021.
3. Tao Li, Dianqi Han, **Yimin Chen**, Rui Zhang, and Yanchao Zhang. IndoorWaze: A crowdsourcing-based context-aware indoor navigation system. IEEE Transactions on Wireless Communication, vol. 19, no. 8, pp. 5461-5472, August 2020.
4. Xin Yao, **Yimin Chen**, Rui Zhang, Yanchao Zhang, and Yaping Lin. Beware of what you share: Inferring user locations in Venmo. IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5109-5118, December 2018.

Book chapter

1. Leon Zeng and **Yimin Chen**. Applying behavioral finance to influence consumer decision-making and behavior via human-automation interaction. In: Duffy, V.G., Lehto, M., Yih, Y., Proctor, R.W. (eds) Human-Automation Interaction. Automation, Collaboration, E-Services, vol 10. Springer, Cham. https://doi.org/10.1007/978-3-031-10780-1_33

Teaching Experience

COMP 2300: Introduction to Computer Security, UML	2021/2022 fall
COMP 4600/5800: Machine Learning Security and Privacy, UML	2022/2023 spring
COMP 3085/5170: Introduction to Linux Kernel Development, UML	2022 fall, 2023 spring
COMP 4010: Software Project I, UML	2022 fall
COMP 4020: Software Project II, UML	2023 spring

Awards and Recognitions

Graduate Student Travel Fund of Dean's Office, School of Electrical, Computer, and Energy Engineering, Arizona State University, Tempe	2018
IEEE INFOCOM Student Travel Grant	2017
IEEE INFOCOM Student Travel Grant	2015
Tutor Commendation Award, Department of Electrical Engineering, The Chinese University of Hong Kong	2011
Lee Wai Wing Scholarship for Outstanding Undergraduate Student, Peking University	2009

Professional Services

Program committee member for:

- IEEE International Conference on Computer Communications and Networks (ICCCN) 2023
- IEEE International Conference on Computer Communications (INFOCOM) 2022
- IEEE International Conference on Communications and Network Security (CNS) 2022, 2023
- IEEE International Conference on Mobile Ad Hoc and Smart Systems (MASS) 2022
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2020

Conference reviewer for:

- IEEE International Conference on Computer Communications and Networks (ICCCN) 2023
- IEEE International Conference on Computer Communications (INFOCOM) 2022
- IEEE International Conference on Communications and Network Security (CNS) 2022, 2023
- IEEE International Conference on Mobile Ad Hoc and Smart Systems (MASS) 2022
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2020
- IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) 2016
- IEEE International Conference on Pervasive Computing and Communications (PerCom) 2016
- ACM Workshop on Privacy-Aware Mobile Computing (PAMCO) 2016
- ACM Symposium on Information, Computer and Communications Security (AsiaCCS) 2015
- IEEE International Conference on Computer Communications (INFOCOM) 2015

Journal reviewer for:

- IEEE/ACM Transactions on Network (ToN)
- IEEE Transactions on Mobile Computing (TMC)
- IEEE Internet of Things
- IEEE Transactions on Vehicular Technology (TVT)
- IEEE ACCESS