Zhi Chen

Thomas M. Siebel Center, 201 North Goodwin Avenue, Urbana, IL 61801-2302
zhic4@illinois.edu ⋄ (+1) 510-345-7211 ⋄ https://zhichen98.github.io

EDUCATION

University of Illinois at Urbana-Champaign *Aug 2020 - Present*
Ph.D. in Computer Science
Advisor: Professor Gang Wang

University of California, Berkeley *Aug 2019 - May 2020*
M.S. in Electrical Engineering and Computer Sciences
Advisor: Professor Dawn Song

University of California, Berkeley *Aug 2016 - May 2019*
B.S. Honors in Electrical Engineering and Computer Sciences

Duke University *Jul 2015 - Aug 2015*
Summer Session Student, Economics: Game Theory

EXPERIENCE

Conference Subreviewer: *CCS* 2024. *May 2024*

CS 463: Computer Security II, UIUC, Urbana, IL. *Fall 2023*
Teaching Assistant

Security and Privacy Research at Illinois, UIUC, Urbana, IL. *Spring 2021 - Present*
Research Assistant

CS 445: Computational Photography, UIUC, Urbana, IL. *Fall 2020*
Teaching Assistant

Center for Long-Term Cybersecurity, UC Berkeley, Berkeley, CA. *Jan 2019 - Aug 2020*
Research Assistant

Alibaba DAMO Academy, Hangzhou, China. *Dec 2018 - Jan 2019*
Research Intern

Berkeley Artificial Intelligence Research Lab, UC Berkeley, Berkeley, CA. *May 2018 - Nov 2018*
Research Assistant

PUBLICATIONS

(* indicates equal contribution)

- Limin Yang*, **Zhi Chen***, Chenkai Wang, Zhenning Zhang, Sushruth Booma, Phuong Cao, Constantin Adam, Alex Withers, Zbigniew Kalbarczyk, Ravishankar K. Iyer, Gang Wang.**True Attacks, Attack Attempts, or Benign Triggers? An Empirical Measurement of Network Alerts in a Security Operations Center**. Proceedings of *The 33rd USENIX Security Symposium (USENIX Security)*, Philadelphia, PA, August 2024.
- Limin Yang, **Zhi Chen**, Jacopo Cortellazzi, Feargus Pendlebury, Kevin Tu, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang. **Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers**. Proceedings of *The 44th IEEE Symposium on Security and Privacy (IEEE SP)*, San Francisco, CA, May 2023.
- **Zhi Chen**, Zhenning Zhang, Zeliang Kan, Limin Yang, Jacopo Cortellazzi, Feargus Pendlebury, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang. **Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors**. Proceedings of *The 6th Deep Learning Security and Privacy Workshop (DLSP)*, in conjunction with IEEE Symposium on Security and Privacy (IEEE SP), San Francisco, CA, May 2023.
- Jinyin Chen, Jian Zhang, **Zhi Chen**, Min Du, Qi Xuan. **Time-aware Gradient Attack on Dynamic Network Link Prediction**. Proceedings of *The IEEE Transactions on Knowledge and Data Engineering (TKDE)*, February 2023.
- Jiajun Zhou*, **Zhi Chen***, Min Du, Lihong Chen, Shanqing Yu, Guanrong Chen, Qi Xuan. **RobustECD: Enhancement of Network Structure for Robust Community Detection**. Proceedings of *The IEEE Transactions on Knowledge and Data Engineering (TKDE)*, January 2023.

- **Zhi Chen**. **NDSGD: A Practical Method to Improve Robustness of Deep Learning Model on Noisy Dataset**. *Technical Report No. UCB/EECS-2020-55*, EECS Department, University of California, Berkeley, May 2020.
- Min Du, **Zhi Chen**, Chang Liu, Rajvardhan Oak, Dawn Song. **Lifelong Anomaly Detection Through Unlearning**. Proceedings of *The 26th ACM Conference on Computer and Communications Security (CCS)*, London, UK, November 2019.

HONORS & AWARDS

- **B.S. Honors**, UC Berkeley *May 2019*
- **Dean's List**, College of Engineering, UC Berkeley *Spring 2017* & *Spring 2018*
- **Finalist**, the 67th Intel International Science and Engineering Fair, Phoenix *May 2016*

RESEARCH INTERESTS

- **Security; Machine Learning**