Zitao Chen

zitaoc@ece.ubc.ca | https://people.ece.ubc.ca/zitaoc/

Education

University of British Columbia

Ph.D. in Electrical and Computer Engineering — 2022 - 2025 (expected)
M.A.Sc. in Electrical and Computer Engineering — 2018 - 2020
Advisor: Karthik Pattabiraman

China University of Geosciences (Wuhan)

B.Eng. in Information Security — 2014 - 2018

Research Interests

Trustworthy Machine Learning: Privacy, Accountability, Safety

Publications [Google Scholar]

[ArXiv'24] **Zitao Chen**, Karthik Pattabiraman "Catch Me if You Can: Detecting Unauthorized Data Use in Deep Learning Models" arXiv preprint arXiv:2409.06280, 2024.

[NDSS'25] **Zitao Chen**, Karthik Pattabiraman "A Method to Facilitate Membership Inference Attacks in Deep Learning Models" *To appear in the ISOC Network and Distributed Systems Security (NDSS) Symposium*, 2025. Direct acceptance without revision. Acceptance rate: TBD [Code]

Artifact Available, Functional and Reproduced

[NDSS'24] **Zitao Chen**, Karthik Pattabiraman "Overconfidence is a Dangerous Thing: Mitigating Membership Inference Attacks by Enforcing Less Confident Prediction " *The ISOC Network and Distributed Systems Security Symposium*, 2024. **Acceptance rate: 15%** [Code]

Artifact Available, Functional and Reproduced

[DSN'21] **Zitao Chen**, Guanpeng Li, Karthik Pattabiraman "A Low-cost Fault Corrector for Deep Neural Networks through Range Restriction" *The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2021. **Acceptance rate: 16.3%** [Code]

Best paper award runner up (2/295)
IEEE Top Picks in Test and Reliability
Adopted by Intel OpenVINO [Details]

[SC'19] **Zitao Chen**, Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben "BinFI: An Efficient Fault Injector for Safety-Critical Machine Learning Systems" *In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, 2019. **Acceptance rate: 20.9%** [Code]

Finalist for SC reproducibility challenge (3/344)

[AsiaCCS'23] **Zitao Chen**, Pritam Dash, Karthik Pattabiraman " Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks " *The 18th ACM ASIA Conference on Computer and Communications Security* 2023. **Acceptance rate: 16%** [Code]

[ISSRE'20] **Zitao Chen***, Niranjhana Narayanan*, Bo Fang, Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben, "TensorFI: A Flexible Fault Injection Framework for TensorFlow Applications" *The 31st IEEE International Symposium on Software Reliability Engineering*, 2020. **Acceptance rate: 25.7%** [Code]

[DSN'21] Pritam Dash, Guanpeng Li, **Zitao Chen**, Mehdi Karimi, Karthik Pattabiraman "PID-Piper: A Framework for Recovering Robotic Vehicles From Physical Attacks" *The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2021. **Acceptance rate: 16.3%** [Code]

Best paper award (1/295)

Journals and short papers

[CCS'24 Doctoral Symposium] **Zitao Chen** "Catch Me if You Can: Detecting Unauthorized Data Use in Training Deep Learning Models" *In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS'24)*. 3 pages. 2024

[TDSC] Niranjhana Narayanan, **Zitao Chen**, Bo Fang, Guanpeng Li, Karthik Pattabiraman, and Nathan DeBardeleben, "Fault Injection for TensorFlow Applications" *IEEE Transactions on Dependable and Secure Computing*. 2022 [Code]

[IOLTS'20] Karthik Pattabiraman, Guanpeng Li, **Zitao Chen**, "Error Resilient Machine Learning for Safety-Critical Systems: Position Paper" *IEEE 26th International Symposium on On-Line Testing and Robust System Design*, 4 pages, 2020. *Invited paper*

[FGCS] **Zitao Chen**, Wei Ren, Yi Ren and Kim-Kwang Raymond Choo, "LiReK: A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions" *Future Generation Computer Systems* (2018) Undergrad research

Honors and Awards

- **IEEE Top Picks in Test and Reliability** (1 of 7 papers) 2024
  - Recognizing the most impactful publications in the computer systems reliability area from 2018-2024
- **DAAD AInet Fellowship** (awarded to 50 fellows worldwide) 2024
- **Brandwajn Graduate Fellowship (twice)** (given to the top-ranked student in the ECE dept) 2023, 2024
- **ACM CCS Doctoral Symposium Travel Grant** 2024
- **UBC Public Scholar Award** (awarded to 45 scholars university-wide) 2022
- **UBC Four Year Doctoral Fellowship** 2022
- **Best paper award at DSN** (1 out of 295 submissions) 2021
- **Best paper award runner up at DSN** (1 of 2 in 295 submissions) 2021
- **UBC Faculty of Applied Science Graduate Award** 2019-2024

Teaching Experiences

Teaching assistant	Building Modern Web Applications (University of British Columbia)	2019
Guest lecturer	Adversarial Machine Learning (Texas State University)	2024
Co-instructor	Introduction to Computer Security (China University of Geosciences)	2017

Work Experiences

Research technician Jul 2020 - Feb 2021

University of British Columbia Advisor: Karthik Pattabiraman

Invited Talks

Technical University of Berlin, Germany	Host: Prof. Konrad Rieck	October 2024
Technical University of Darmstadt, Germany	Host: Prof. Thomas Schneider	October 2024

SERVICES

Reviewer:

- IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems 2023, 2024
- Elsvier Computer & Security 2024
- Elsvier Computer Standards & Interfaces 2024
- IEEE Multimedia 2023

Sub-reviewer:

- Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2020, 2022
- ACM/SIGAPP Symposium On Applied Computing (SAC) 2024
- International Symposium on Reliable Distributed Systems (SRDS) 2023
- Inaugural Symposium on Vehicle Security and Privacy (VehicleSec) 2023
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2022
- IEEE International Conference on Software Security and Reliability (QRS) 2019