Zitao Chen • *zitaoc@ece.ubc.ca* • *+1-778-316-8835*

Education

China University of Geosciences (Wuhan)   Wuhan, China
Bachelor degree in Information Security   *Sept. 2014 – Jun. 2018*
GPA: 87.67/100;
GRE: V158 Q168 AW:3.5

University of British Columbia   Vancouver, Canada
Master of Applied Science in Electrical and Computer Engineering *Sept. 2018 - May 2020* (Expected)
Supervisor: Karthik Pattabiraman
Research interest: Fault tolerance, security and privacy of machine learning

Research Experience

Reliability of Machine Learning Systems   Graduate Research
Understanding the error resilience of ML systems   *Presented in SC'19*

- *Research question:* How to identify the critical bits in ML systems due to hardware transient faults (i.e., bit-flip), to guide the design of error-resilient ML systems.
- *Key insight:* We analyze the mathematical properties of common ML computations, and find many of them exhibit monotone property, which constrains the fault propagation behavior.
- We design a binary-search like fault injector to identify critical bits in the system.
- *Results:* Our approach can efficiently identify 99%+ of critical bits with 99%+ precision.
- Code: https://github.com/DependableSystemsLab/TensorFI-BinaryFI

Boosting the error resilience of ML systems   *Manuscript under review*

- *Research question:* How to efficiently enhance the error resilience of ML systems.
- *Key insight:* We propose to apply range restriction on a subset of ML computations, to dampen the fault amplification effect, thus preventing the faults leading to erroneous outputs.
- Our approach can be integrated into existing models without retraining.
- *Results:* Our approach enabled *significant resilience boosting* and *would not* degrade the accuracy of the model.

Wearable Computing Security   Undergraduate Research

- Lightweight and real-time key establishment scheme for wearable embedded devices.
- Sensing user real-time motion to secure communication between on-body devices.
- Selectively exploiting the sensory data (due to device vibration or hardware imprecision) for random key generation, without any data processing.

Publications

- [**DAC'20**] <u>Zitao Chen</u>, Guanpeng Li, Karthik Pattabiraman"Boosting Error-Resilience of Deep Neural Networks through Range Restriction", ACM/ESDA/IEEE Design Automation Conference (DAC) **Under review. Manuscript available upon request.**

- [**SC'19**] <u>Zitao Chen</u>, 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*, **AR: 20.9% (72/344) direct acceptance rate for regular papers.**

- [**FGCS**] <u>Zitao Chen</u>, 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) [Impact Factor: 5.768]

Others

Open-source project: https://github.com/DependableSystemsLab/TensorFI   Sept. 2018 - present
Programming languages: Python, Java, C, C++
Teaching Experience: CPEN400A   2019
Award: Graduate Student Initiative: $4000   2019