Tao Zhang

Email: tzhang06@email.wm.edu **or** tzhang06@wm.edu
Last updated on: Oct. 15, 2021 **Latest version**: http://www.cs.wm.edu/~taozhang/

EDUCATION

William & Mary — Williamsburg, VA, USA
Ph.D. candidate in Computer Science. **Advisor:** Dr. Dmitry Evtyushkin — Expected May 2022

Central Michigan University — Mount Pleasant, MI, USA
M.Sc. in Computer Science. **Advisor:** Dr. Qi Liao — May 2014

North China University of Technology — Beijing, China
B.Eng. in Computer Science and Technology. — July 2012

RESEARCH EXPERIENCE

William & Mary — Williamsburg, VA, USA
Research Assistant. **Advisor:** Dr. Dmitry Evtyushkin — May 2018 - present

- Implemented microbenchmarks to investigate security implications in the CPU front-end, including BPU, DSB, etc.
- Reverse-engineered multiple branch predictors and found HW vulnerabilities for speculative execution attacks.
- Demonstrated transient execution trojans with (or without) modified Linux Kernel and optimized the attacks.
- Designed secure branch predictors to defend against transient execution attacks and BPU side-channels.
- Built a branch prediction simulator (BPUsim) for fast and in-depth performance analysis on Intel PT traces.
- Implemented various BPU models and their secure counterparts with address encryptions, remapping schemes, and security microcode updates (e.g., IBPB, IBRS, STIBP) in BPUsim and gem5 to study the performance impacts.
- Wrote LLVM analysis passes for extracting branch instruction data dependency on real-world applications.
- Designed prefetching schemes for accelerating branch resolution and prediction verification to mitigate spectre-v1.

Central Michigan University — Mount Pleasant, MI, USA
Research Assistant. **Advisor:** Dr. Qi Liao — Aug. 2012 - Jun. 2014

- Applied unsupervised learning for network link anomaly detection and basketball offense tactic analysis with link prediction algorithms, Jaccard coefficient, and Katz Index, etc.
- Implemented a real-time network visualization platform for network anomaly monitoring, analysis, and detection.
- Designed multiple visual analytics for data mining in vast volume, metadata, interconnectivity, and high dynamics.

State Key Laboratory of Computer Science, Chinese Academy of Science — Beijing, China
Research Intern. **Advisor:** Dr. Lei Shi — May 2012 - Aug. 2012

- Designed and implemented spatiotemporal visual analytics for big data and network security.
- Build automated tools to parse, analyze, and transform large datasets to insights for KML visualization tools.

SELECTED PUBLICATION

- **T Zhang**, T Lesch, K Koltermann, D Evtyushkin. STBPU: A Reasonably Safe Branch Predictor Unit. arXiv preprint arXiv:2108.02156. (under review)
- **T Zhang**, K Koltermann, D Evtyushkin. Exploring Branch Predictors for Constructing Transient Execution Trojans. **ASPLOS**, 2020

Prior to the PhD study:

- **T Zhang**, Q Liao. Dynamic link anomaly analysis for network security management. **Springer Journal of Network and Systems Management,** 2019
- **T Zhang**, Q Liao, L Shi. Bridging the Gap of Network Management and Anomaly Detection through Interactive Visualization. **PacificVis**, 2014.
- **T Zhang**, Q Liao, L Shi, W Dong. Analyzing Spatiotemporal Anomalies through Interactive Visualization. **Informatics**, 2014

AWARD

- **Graduate Studies and Research Recruitment Fellowship**, William & Mary, 2016-2018
- **Student Travel Grant**, ASPLOS 2019, ASPLOS 2020

PROFESSIONAL MEMBERSHIP

- ACM: Student Membership (#4794330)

SKILL

- **Main Programming Languages:** C/C++, Assembly, Python, Java
- **Other Technologies:** gem5, LLVM, Intel PT, Intel Pin, Intel SDE, Caffe, LAMP, JavaScript, AJAX, PHP, SQL
- **Language Skills**: Chinese (native), English (fluent)