

Tao Zhang

Email: tzhang06@email.wm.edu or tzhang06@wm.edu

Last updated on: Oct. 6, 2020 Latest version: <http://www.cs.wm.edu/~taozhang/>

EDUCATION

William & Mary

Ph.D. candidate in Computer Science. **Advisor:** Dr. Dmitry Evtvushkin

Williamsburg, VA, USA

Expected May 2022

Central Michigan University

M.Sc. in Computer Science. **Advisor:** Dr. Qi Liao

Mount Pleasant, MI, USA

May 2014

North China University of Technology

B.Eng. in Computer Science and Technology.

Beijing, China

July 2012

RESEARCH EXPERIENCE

William & Mary

Research Assistant. **Advisor:** Dr. Dmitry Evtvushkin

Williamsburg, VA, USA

May 2018 - present

- Implemented automated microbenchmarks to investigate potential hardware (HW) vulnerabilities in CPU.
- Reverse-engineered multiple CPU branch predictors and found HW vulnerabilities for speculative execution attacks.
- Demonstrated new transient execution trojans with modified Linux Kernel and automated attack optimizations.
- Designed secure branch predictors to defense against transient execution attacks and side-channel attacks.
- Built a branch prediction simulator (BPUsim) to process Intel PT traces for in-depth performance analysis.
- Implemented various BPU models and security microcode updates (e.g., IBRS, STIBP) in BPUsim and gem5 to study the performance impacts.
- Analyzing branch instruction data dependency and timing using static analyses e.g., Angr and pintools e.g., DrDebug.

Central Michigan University

Research Assistant. **Advisor:** Dr. Qi Liao

Mount Pleasant, MI, USA

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

Research Intern. **Advisor:** Dr. Lei Shi

Beijing, China

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**, K Koltermann, D Evtvushkin. 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, Intel PT, Intel Pin, Intel SDE, Caffe, LAMP, JavaScript, AJAX, PHP, SQL
- **Language Skills:** Chinese (native), English (fluent)