Mengjia Yan

Contact Information

4238 Thomas M. Siebel Center
University of Illinois at Urbana-Champaign
201 N. Goodwin Ave.
Urbana, IL. 61801.

Mobile: 1-217-778-7721
E-mail: myan8@illinois.edu
Website:
http://iacoma.cs.uiuc.edu/students/yan

Research Interest

My research lies in the field of computer architecture, with an emphasis on hardware support for security. My work has focused on developing efficient detection and defense mechanisms against side channel attacks, an important class of security threat. I'm now exploring security issues in the training and inference of machine learning algorithms in the cloud.

Education Background

University of Illinois, Urbana-Champaign **Sep 2013 - present**
PhD Candidate/Research Assistant, Computer Science
Adviser: Professor Josep Torrellas
GPA(curr.): 4.0/4.0, *Qualify Examination Passed*

University of Illinois, Urbana-Champaign **Jul 2016**
Master of Science, Computer Science
Adviser: Professor Josep Torrellas
GPA: 4.0/4.0
Thesis: "Performance Evaluation of VM-level Record-and-Replay Techniques and Applications"

Zhejiang University, China **Jun 2013**
Bachelor, Computer Science
Adviser: Professor Tianzhou Chen, Professor Wenzhi Chen
GPA: 91.36/100(3.98/4.00), Rank: **2/181**

Publications

[1] **Mengjia Yan**, Bhargava Gopireddy, Thomas Shull, Josep Torrellas. *Secure Hierarchy-Aware Replacement Policy (SHARP): Defending Against Cache-Based Side Channel Attacks.* The 44th International Symposium on Computer Architecture(**ISCA**), 2017. Acceptance rate of 16.77%

[2] **Mengjia Yan**, Yasser Shalabi, Josep Torrellas. *ReplayConfusion: Detecting Cache-based Covert Channel Attacks Using Record and Replay.* The 49th Annual IEEE/ACM International Symposium on Microarchitecture(**MICRO**), 2016. Acceptance rate of 21.55%

[3] Yasser Shalabi, **Mengjia Yan**, Nima Honamarand, Ruby Lee, Josep Torrellas. *Record-Replay as a General Framework for Thwarting Attacks and its Application to Return Oriented Programming.* (submitted for publication)

[4] **Mengjia Yan**, Weiwei Fu, Chao Wang, Li Liu, Tianzhou Chen. *Agent-Based Traffic Merging in Network-on-Chip.* The 15th IEEE International Symposium on Parallel & Distributed Processing, Workshops(**APDCM**), 2013.

Selected Honors and Awards

W.J. Poppelbaum Memorial Award	2017
ACM SIGARCH Student Scholarships for Celebration of 50 Years of the ACM Turing Award	2017
National Scholarship in China(**1.8%**)	2010/2011
1th Prize, Excellent Undergraduate Scholarship(**3%**)	2010/2011/2012
1th Grade, Scholarship of Excellent Achievements(**3%**)	2010/2011/2012

Talks

1. Secure Hierarchy-Aware Replacement Policy (SHARP): Defending Against Cache-Based Side Channel Attacks; *ITI Trust and Security Seminar*, University of Illinois at Urbana-Champaign, 01/31/2017.

2. ReplayConfusion: Detecting Cache-based Covert Channel Attacks Using Record and Replay; *The 49th Annual IEEE/ACM International Symposium on Microarchitecture*(**MICRO**), Taipei, 10/18/2016.

Selected Research Projects

Hardware Support for Covert/Side Channel Defense and Detection
Efficient and practical defense and detection approaches against covert/side channel on last-level caches.

A Record-and-Replay Framework to Thwart ROP Attacks
A novel framework using Record and Deterministic Replay (RnR) is used to complement hardware security features to improve its intrusiveness and completeness trade-off.

Sequential Consistency Violation Detection Using RnR
Efficient precise sequential consistency violation detection using chunk-based record and replay.

Agent-Based Traffic Merging in NoC
A novel routing algorithm to improve Network-on-Chip performance.

Selected Course Projects

Block Fusion in FCUDA
A compilation technique to optimize off-chip bandwidth for FCUDA.

Parallel Graph Coloring in Charm++
Apply state space search to do parallel graph coloring using Charm++, a parallel programming framework.

Compiler design and implementation in LLVM
Implement lexer, parser and intermediate code generation in LLVM for an object-oriented language. Besides, implement register allocator and a flow-sensitive pointer analysis pass.

Multi-Chip-Synchronization via Optical Switch
Program on-chip photoelectric transducer to do multi-chip clock synchronization. Implemented in Verilog.

FPGA Pipelined CPU
Design and implement a five-stage pipelined CPU in verilog with branch-prediction and bypassing.

Service

- External review for GLSVLSI'16

Skills

Programming Languages: C/C++, OpenMP, CUDA, Java, Python, Matlab, Javascript
Software Frameworks: Qemu/KVM, MarssX86, Theano, Tensorflow, Simics, LLVM, Pin, Charm++, Gem5, Sniper, BookSim
EDA Tools and HDLs: Verilog/VHDL, Xilinx ISE, ModelSim