Mengjia Yan

Contact Information

4238 Thomas M. Siebel Center
201 N. Goodwin Ave. Urbana, IL. 61801.

E-mail: myan8@illinois.edu
Website: http://myan8.web.engr.illinois.edu

Research Interest

My research lies in the field of computer architecture, with an emphasis on hardware support for security. My work has focused on cache-based side channel attacks, an important class of security threat. I designed new types of attacks targeting evolving applications and architectures to help the community to identify unexploited security vulnerabilities. Moreover, I worked on designing practical detection and defense mechanisms to combat cache-based side channels by leveraging architecture innovations, to attain much better trade-offs between performance, effectiveness and implementation complexity.

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, *Qualifying 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**, Read Sprabery, Bhargava Gopireddy, Christopher Fletcher, Roy Campbell, Josep Torrellas. "Attack Directories, Not Caches: Side Channel Attacks in a Non-Inclusive World". To appear in IEEE International Symposium on Security and Privacy (**SP**), 2019.

[2] Kartik Hegde, Jiyong Yu, Rohit Agrawal, **Mengjia Yan**, Michael Pellauer, Christopher Fletcher. "UCNN: Exploiting Computational Reuse in Deep Neural Networks via Weight Repetition". The 45th International Symposium on Computer Architecture (**ISCA**), 2018. Acceptance rate of 16.93%.

[3] Yasser Shalabi, **Mengjia Yan**, Nima Honarmand, Ruby B Lee, Josep Torrellas. "Record-Replay Architecture as a General Security Framework". The 24th International Symposium on High-Performance Computer Architecture (**HPCA**), 2018. Acceptance rate of 19.23%.

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

[5] **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%.

[6] **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

Mavis Future Faculty Fellow	2018
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/ Posters

Attack Directories, Not Caches: Side Channel Attacks in a Non-Inclusive World
- Midwest Security Workshop, University of Illinois at Urbana-Champaign, 04/14/2018.
- Hardware and Architectural Support for Security and Privacy (HASP), Los Angeles, CA, 06/02/2018.

Stealing Neural Network Architectures Using Cache-based Side Channel Attacks
- Compiler Seminar, University of Illinois at Urbana-Champaign, 10/11/2017.

Secure Hierarchy-Aware Cache Replacement Policy (SHARP)
- Career Workshop for Women and Minorities in Computer Architecture (CWWMCA), Boston, MA, 10/15/2017.
- ITI Trust and Security Seminar, University of Illinois at Urbana-Champaign, 01/31/2017.
- Intel, 01/19/2018.

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

Teaching Experience

Secure Processor Design Fall 2017, UIUC
- With Professor Christopher W. Fletcher.
- Gave guest lecture on defending against cache-based side channel attacks.
- Involved in designing lab assignment: Dead Drop lab.

Parallel Computer Architectures Spring 2018, UIUC
- With Professor Josep Torrellas.
- Teaching assistant.
- Lead lecture-discussion on CMP, multi-scalar processors, dataflow architectures.

Advanced Memory and Storage Systems Spring 2018, UIUC
- With Professor Jian Huang.
- Gave guest lecture on secure cache hierarchies.

Service

- External review for GLSVLSI'16

Membership

- IEEE, ACM, CRA-W (Computing Research Association-Women), GradSWE (the UIUC chapter of Society of Women Engineers), WCS (Women in Computer Science)

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