Zhuojia Shen

Department of Computer Science
University of Rochester
Rochester, NY, USA 14627

+1 (585) 629-2327
zshen10@cs.rochester.edu
https://www.cs.rochester.edu/u/zshen10

Education

Sept. 2016 – Present	**University of Rochester**, Rochester, NY, USA Ph.D. in Computer Science *Advisor:* Prof. John Criswell
Sept. 2016 – Jan. 2019	**University of Rochester**, Rochester, NY, USA M.S. in Computer Science
Sept. 2012 – June 2016	**Beijing Institute of Technology**, Beijing, China B.S. in Computer Science & Technology

Research Interests

Systems:	Operating Systems, Compiler Transformations
Security:	Operating System Security, Embedded System Security, Memory Safety, Control-Flow Integrity, Compiler Transformations for Security

Selected Publications

1. Zhuojia Shen and John Criswell.
   InversOS: Efficient Control-Flow Protection for AArch64 Applications with Privilege Inversion.
   arXiv e-Print 2304.08717.
   April 2023.
2. Zhuojia Shen, Komail Dharsee, and John Criswell.
   Randezvous: Making Randomization Effective on MCUs.
   In *Proceedings of the 38th Annual Computer Security Applications Conference* (ACSAC '22).
   Austin, TX, USA. December 2022.
3. Yufei Du, Zhuojia Shen, Komail Dharsee, Jie Zhou, Robert J. Walls, and John Criswell.
   Holistic Control-Flow Protection on Real-Time Embedded Systems with Kage.
   In *Proceedings of the 31st USENIX Security Symposium* (Security '22).
   Boston, MA, USA. August 2022.
4. Zhuojia Shen, Komail Dharsee, and John Criswell.
   Fast Execute-Only Memory for Embedded Systems.
   In *Proceedings of the 2020 IEEE Secure Development Conference* (SecDev '20).
   ~~Atlanta, GA, USA~~ (Virtual). September 2020.
5. Jie Zhou, Yufei Du, Zhuojia Shen, Lele Ma, John Criswell, and Robert J. Walls.
   Silhouette: Efficient Protected Shadow Stacks for Embedded Systems.
   In *Proceedings of the 29th USENIX Security Symposium* (Security '20).
   ~~Boston, MA, USA~~ (Virtual). August 2020.
6. Zhuojia Shen, Jie Zhou, Divya Ojha, and John Criswell.
   Restricting Control Flow During Speculative Execution with Venkman.
   arXiv e-Print 1903.10651.
   March 2019.
7. Zhuojia Shen, Jie Zhou, Divya Ojha, and John Criswell.
   POSTER: Restricting Control Flow During Speculative Execution.
   In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (CCS '18).
   Toronto, ON, Canada. October 2018.
8. Xiaowan Dong, Zhuojia Shen, John Criswell, Alan L. Cox, and Sandhya Dwarkadas.
   Shielding Software from Privileged Side-Channel Attacks.
   In *Proceedings of the 27th USENIX Security Symposium* (Security '18).
   Baltimore, MD, USA. August 2018.
9. Xiaowan Dong, Zhuojia Shen, John Criswell, Alan Cox, and Sandhya Dwarkadas.
   Spectres, Virtual Ghosts, and Hardware Support.
   In *Proceedings of the 7th Int'l Workshop on Hardware and Architectural Support for Security and Privacy* (HASP '18).
   Los Angeles, CA, USA. June 2018.

Work Experience

June 2020 – Aug. 2020

Intern - Member of Technical Staff - VM Monitor
VMware, ~~Palo Alto, CA, USA~~ (Virtual)
Mentor: Dr. Zheng Cui

- Designed and implemented a live patch generation tool for VMKernel
- Implemented a live patch applying mechanism to verify patch correctness

May 2019 – Aug. 2019

Intern - Member of Technical Staff - VM Monitor
VMware, Boston, MA, USA
Mentor: Dr. Jiajun Cao

- Designed and implemented a generic interface for sharing Page-Modification Logging (PML), an Intel processor feature, among modules in the VM monitor
- Evaluated the performance of vMotion utilizing the PML interface

May 2014 – Feb. 2015

Co-Founder & CTO (part-time)
Taoxue Information Technology Co., Ltd, Beijing, China

- Member of Taoxue Backend Team, main developer and maintainer of Taoxue web server
- Provided technical support to Taoxue iOS and Android Client Teams

Research Experience

Mar. 2022 – Present

InversOS: Protecting AArch64 Applications with Privilege Inversion
Advisor: Prof. John Criswell

- Designed Privilege Inversion, a low-cost intra-address space isolation mechanism for AArch64
- Designed and implemented InversOS, a Linux-based OS utilizing Privilege Inversion to protect applications from control-flow hijacking attacks
- Evaluated the performance of InversOS with various benchmarks and applications

Sept. 2020 – Oct. 2022

Randezvous: Leakage-Resistant Randomization for Microcontrollers (MCUs)
Advisor: Prof. John Criswell

- Designed and implemented Randezvous, a randomization-based defense scheme against leakage-equipped brute-forcing control-flow hijacking attacks on ARMv7/8-M MCUs
- Evaluated the security of Randezvous via statistical modeling and PoC/CVE exploits
- Evaluated the performance of Randezvous via benchmarks and applications on a real MCU

May 2021 – May 2022

Kage: Holistic Control-Flow Protection for Embedded Real-Time Operating Systems
Advisors: Prof. John Criswell and Robert J. Walls

- Co-designed and implemented control-flow integrity with unique labels for ARMv7-M
- Co-designed and implemented a code scanner for privileged instructions
- Evaluated the performance of Kage using CoreMark benchmark

Mar. 2020 – Aug. 2020

PicoXOM: Fast Execute-Only Memory for Embedded Systems using Debug Support
Advisor: Prof. John Criswell

- Designed and implemented PicoXOM, fast XOM for ARMv7/8-M using debug registers
- Evaluated PicoXOM on performance, code size, and security

May 2019 – June 2020

Silhouette: Efficient Protected Shadow Stacks for Embedded Systems
Advisors: Prof. John Criswell and Robert J. Walls

- Designed and implemented label-based control-flow integrity for ARMv7-M
- Designed a solution for handling `setjmp`/`longjmp` that keeps the integrity of return addresses
- Evaluated Silhouette's performance and code size on multiple benchmarks and applications

July 2018 – May 2019

Venkman: Software-Based Defenses against Spectre Attacks
Advisor: Prof. John Criswell

- Co-designed and implemented a software-based defense to defeat existing and potential Spectre attacks that poison CPU's branch target buffer/return stack buffer and leak information via branches
- Co-designed and implemented a software fault isolation technique that resists Store-to-Fetch Forwarding attacks on programs' code segment
- Evaluated performance and code size overhead of Venkman on POWER architecture

July 2017 – June 2018

Defenses against Privileged Side-Channel Attacks

Advisors: Prof. John Criswell, Sandhya Dwarkadas, and Alan L. Cox

- Co-designed and implemented a physical frame buffer queue in Apparition, a shielding system that protects applications from untrusted OSes, to obfuscate applications' memory allocation patterns
- Modified the FreeBSD C library to allow applications to transparently utilize a secure memory allocator interface
- Optimized the bit-masking software fault isolation to resist Spectre and Meltdown attacks

Jan. 2017 – July 2017 **Structure Field Software Fault Isolation**
Advisor: Prof. John Criswell

- Designed and implemented several FreeBSD kernel-level rootkits
- Implemented the Padding Area MetaData (PAMD) shadow table in FreeBSD kernel space for heap objects

Feb. 2014 – June 2014 **The Circular Wirelength Problem for 4-Dimensional Hypercubes**
Advisor: Prof. Qinghui Liu

- Designed and implemented a distributed enumeration system to find out the minimum wirelength of hypercubes
- Developed a GUI tool helping discover the characteristics of a hypercube with minimum wirelength

Dec. 2013 – Apr. 2014 **Data Race Detector for Multi-Threaded Programs**
Advisor: Prof. Weixing Ji

- Designed and implemented the segment AVL tree as an efficient realization of set ADT, used to record memory addresses dereferenced by a thread in a process
- Conducted performance evaluation and profiling on several different implementations

Teaching Experience

Sept. 2018 – Dec. 2018 **Graduate Teaching Assistant**
Course: CSC 256/456 Operating Systems
Instructor: Prof. Sandhya Dwarkadas

Jan. 2018 – May 2018 **Graduate Teaching Assistant**
Course: CSC 261/461 Database Systems
Instructor: Dr. Tamal Biswas

Sept. 2017 – Dec. 2017 **Graduate Teaching Assistant**
Course: CSC 256/456 Operating Systems
Instructor: Prof. John Criswell

Mar. 2016 – June 2016 **Undergraduate Teaching Assistant**
Course: Computational Theory & Algorithm Analysis Design
Course: Combinatorial Mathematics
Instructor: Prof. Qinghui Liu

Honors & Awards

- Senior honors thesis, Beijing Institute of Technology, 2016
- Third-class People's Scholarship (four times), Beijing Institute of Technology, 2012 – 2015

Skills

Programming languages:	C/C++, Java, C#, Bash, Python, Ruby, JavaScript, x86/ARM/PowerPC/MIPS Assembly, SQL
Software & tools:	Vim, Git, LLVM, Docker, Mutt, Eclipse, Sublime Text, Microsoft Office, LaTeX
Platforms:	Linux, Windows, FreeBSD, VMware ESXi