ZIYI ZHAO

Department of Cyber Science
Nankai University, P.R. China
Homepage: https://tr0py.github.io/ | Email: troppingz@gmail.com

EDUCATION

Nankai University Tianjin, China
B.Eng. Information Security, Major GPA: 90.9/100 (rank 4/54) Aug 2016 – June 2020

- Academic Excellence Scholarship, Innovation Scholarship, Distinguished Thesis Award
- Selected as a visiting scholar to University of Minnesota, Twin Cities from June - September 2019
- Selected Core Courses: Operating System(93), Principles of Compilers(93), Computer Networks(96), Vulnerability Exploitation and Penetration Test(99), Computer Virus(94.2), High Level Language Program Design 2-1(100), Computer Graphics(99), Big Data Analytics and Application(97.4), Digital Logic(94)

RESEARCH EXPERIENCE

Nankai University Tianjin, China
Research Assistant, Information Security & Embedded System Lab June 2020 – Present

- Initiated an independent project exploiting vulnerabilities in state-of-the-art JavaScript Engines
- Initiated and designed a project to find efficient solutions for ABA problems in Dynamic Binary Translation (DBT) systems; Implemented and analyzed performance bottlenecks of existing solutions toward ABA problems; Proposed new correct, efficient, and portable solutions
- Analyzed research trends in computer systems such as Processor-In-Memory, Non-Volatile Memory, RDMA
- Mentored and trained two undergraduate students during the completion of their research projects

University of Georgia (Remote) Georgia, USA
Research Assistant to Prof. Wenwen Wang February 2020 – May 2020

- Initiated a project and proposed effective and unconventional exploitation of SIMD hardware extensions
- Analyzed register usage behavior in JavaScript Engine, PARSEC, SPEC Benchmark and real world applications; Designed and developed a scientific register allocation scheme in a DBT system for Cross-ISA Virtualization; Developed a code generation optimizer that supports AArch64, RISC-V and X86 for QEMU

University of Minnesota at Twin Cities Minnesota, USA
Visiting student to Prof. Pen-Chung Yew's group June 2019 – September 2019

- Discovered a flaw in atomic instruction emulation for Cross-ISA emulation, which may lead to ABA problems
- Designed a novel Arm-lock-free-stack that crashes on an ABA problem to address the issue
- Optimized a distributed DBT framework to improve its scalability by paralleling the emulation

Nankai University Tianjin, China
Undergraduate Research Assistant, Information Security & Embedded System Lab January 2019 – June 2019

- Designed and implemented a distributed shared memory coherence protocol, efficient distributed locking algorithm and system call delegation scheme to extend DBT's scalability from single node to cluster
- Analyzed performance bottleneck issues in distributed DBT systems and proposed three corresponding solutions
- Helped design an SGX page preloading algorithm
- Assisted in lab maintenance and organization

PUBLICATIONS

- **Enhancing Atomic Instruction Emulation for Cross-ISA Dynamic Binary Translation**
  Ziyi Zhao, Zhang Jiang, Xiaoli Gong, Ying Chen, Wenwen Wang, Pen-Chung Yew
  *International Symposium on Code Generation and Optimization (**CGO 2021, Rank A2 in Qualis**), Virtual Conference, February 27th - March 3rd, 2021*
- **DQEMU: A Scalable Emulator with Retargetable DBT on Distributed Platforms**
  Ziyi Zhao, Zhang Jiang, Ximing Liu, Xiaoli Gong, Wenwen Wang, Pen-Chung Yew
  *The 49th International Conference on Parallel Processing (**ICPP 2020, Rank A2 in Qualis**), Edmonton, AB, Canada, August 2020*
- **Regaining Lost Seconds: Efficient Page Preloading for SGX Enclaves**
  Ximing Liu, Xiaoli Gong, Wenwen Wang, ***Ziyi Zhao***, Pen-Chung Yew
  *The ACM/IFIP Middleware Conference 2020 (**Middleware 2020, Rank A2 in Qualis**), Delft, Netherlands, December 2020*
- **SELWasm: A Code Protection Mechanism for WebAssembly**
  Jian Sun, Dingyuan Cao, Ximing Liu, ***Ziyi Zhao***, Wenwen Wang, Xiaoli Gong, Jin Zhang
  *The 17th IEEE International Symposium on Parallel and Distributed Processing with Applications (**ISPA 2019, Rank B3 in Qualis**), Xiamen, China, December 2019*

SELECTED RESEARCH PROJECTS

Distributed Dynamic Binary Translator (DBT) Minnesota, USA & Tianjin, China
Supervised by Prof. Xiaoli Gong, Prof. Pen-Chung Yew and Prof. Wenwen Wang Nov 2018 – Jan 2020

- Collaboration between the University of Georgia, Nankai University and University of Minnesota, Twin Cities
- Proposed the distributed DBT framework DQEMU which goes beyond a single-node multicore processor and can scale up to a cluster of multi-node servers
- Designed and implemented a page-level directory-based data coherence protocol, a hierarchical locking mechanism, and a delegation scheme for system calls to maintain coherence and consistency
- Proposed several performance optimization strategies including page splitting to mitigate false data sharing among nodes, data forwarding for latency hiding, and a hint-based locality-aware scheduling scheme
- Results showed that DQEMU scaled well beyond a single-node machine with reasonable overheads (e.g. ~5x speedup using 7-nodes); Source code available at GitHub and research published at *ICPP 2020*

Enhancing Atomic Instruction Emulation for Cross-ISA Emulation Tianjin, China
Supervised by Prof. Xiaoli Gong, Nankai University Sept 2019 – Oct 2020

- State-of-the-art DBT tools do not provide a fully correct translation of atomic instructions, particularly RISC atomic instructions (i.e. LL/SC) to CISC atomic instructions (i.e. CAS), due to performance concerns. This introduces ABA problems that lead to wrong results and program crashes
- Proposed several schemes to address these issues and implemented them on a popular DBT,QEMU to evaluate their performance overheads: Designed a non-blocking hash table to lower the synchronization overhead and simplified memory checking algorithms in the critical path; Exploited Intel Protection Key to reduce privilege confliction and virtual page remapping to reduce false sharing
- Results published in *CGO 2021* showed that all of my proposed schemes can provide correct emulation and the best solution achieved 2.03x speedup over the best existing software-based scheme

Effective and Unconventional Exploitation of SIMD Extensions in Cross-ISA Virtualization Remote Collaboration
Supervised by Prof. Wenwen Wang, University of Georgia Feb 2020 – June 2020

- Proposed an effective and unconventional exploitation of hardware SIMD extensions in cross-ISA virtualization systems to bridge the utilization gap of SIMD extensions when there is little data parallelism
- Measured different register behaviors from different benchmarks and compilers to find the best register allocate scheme to map the hottest register to SIMD registers
- Exploited powerful SIMD instructions to automatically replace certain general instructions to accelerate the emulation process and wrote x86-based SIMD instruction converters, targeting AArch64 and RISC-V, respectively
- Prototype achieved an average of 2.2x speedup, and is compatible with various SIMD extensions including SSE, AVX, AVX2, and AVX512, and can be applied to different ISAs (e.g. AArch64, RISC-V, x86)

Binary Vulnerabilities Exploiting Tianjin, China
Nankai CTF team member; Supervised by Prof. Zhi Wang, Nankai University Apr 2018 – June 2019

- Focused on binary vulnerabilities exploitation; Exploited vulnerabilities in binaries like overflows to bypass security protections such as canary and ASLR to execute malicious codes
- Won several Capture-The-Flag (CTF) cybersecurity competition awards

SELECTED COURSEWORK

Simple Operating System Kernel Operating Systems
Music Recommendation System Big Data Analytics and Application
Simple C Compiler Principles of Compilers
Network Packet Sniffer, Email Server & Client Computer Networks

SELECTED AWARDS AND HONORS

- Academic Excellence Scholarship (top 2 out of 54), Nankai University 2019
- Innovative Scholarship, Nankai University 2019
- College Students Information Security Competition, Second Prize (top 10%) 2018
- Qiang Wang Cup Cyber Security Competition, Excellence Prize (ranked 2nd in Tianjin) 2018
- The Mathematical Contest in Modeling, Honorable Mention (37%) 2017
- Nation Olympiad of Informatics (Advanced), Second Prize in Province 2015

ADDITIONAL INFORMATION

- Programming languages: C/C++, Assembly (x86, ARM, RISC-V), Pascal, Python, JavaScript
- Familiar Tools: QEMU, Valgrind, Intel PIN
- Familiar Hardware: Non-volatile Memory, RDMA, Processor-In-Memory (PIM), Hardware Transactional Memory (HTM), Intel Memory Protection Key (MPK)
- Leader of the Cyber Tech Department, New Youth News Agency, Nankai University