Ganxiang Yang

800 Dongchuan Road, Minhang District, Shanghai 200240
(+86) 185-6395-9307 yangganxiang@gmail.com github.com

Education

Zhiyuan College, Shanghai Jiao Tong University **Sep.2020 - Present**
*BEng in Computer Science and Technology, member of **ACM Honor Class** (top 5% students in SJTU)* *Shanghai, China*

- Excellent professional and mathematical courses performance (to list a few):
  Operating System: 95/100, Machine Learning: 93/100, Model Checking: 94/100, Lab Research Practice: A+
  Mathematical Analysis: 92/100, Linear Algebra: 90/100, Mathematical Logic: 91/100, Probability Theory: 92/100

Research Interests

Security and Privacy, System in general, Programming Language, Compiler.

Publications

ShadowBound: Efficient Memory Protection through Metadata Management and Compiler Optimization
*Authors: Zheng. Y, **Ganxiang. Y**, Xinyu. X*

- Submitted to *Usenix Security'24*, under review.
- Propose ShadowBound, a novel approach for detecting heap out-of-bound by static analysis and pointer tagging.
- Implement ShadowBound onto LLVM 15 and integrate state-of-the-art use-after-free defense approaches.
- Evaluation shows ShadowBound maintains robustness and safety with minimal time and memory overhead in all off-the-shelf techniques.

Palantír: Formally Verified Privileged Enclave as a Lightweight and Efficient Framework Extension
*Authors: **Ganxiang. Y**, Chenyang. L, Zhen. H, Guoxing. C, Hongfei. F, Yuanyuan. Z, Haojin. Z*

- Preprint, under review.
- Propose Palantír, a novel Privileged Enclave (PE) framework for bringing back customizable services to enclaves.
- Build TAP^2, an extended formal model of TEE platform for verifying Palantír security properties.
- Implement Palantír onto Penglai-TVM and conducted three various case studies to show service flexibility.

Academic Experiences

Research Intern **Feb.2023 – Present**
Northwestern University, U.S.A. *Mentor: Xinyu Xing*

- Designing new methods to exploit blockchain platform vulnerabilities and to improve web API fuzzing efficiency.
- Proposing an efficient memory protection approach though metadata management and compiler optimization.
- Exploring LLM-aided static analysis approaches for various open-sourced projects.

Undergraduate Research Assistant **Jul.2022 – Present**
Network Security and Privacy Protection (NSEC) Lab, SJTU *Mentor: Guoxing Chen*

- Focusing on cross-platform Trusted Execution Environment (TEE) primitive designs.
- Providing a lightweight and secure service framework to Penglai-TVM, a RISC-V trusted computing platform.
- Utilizing formal verification to describe TEE platform and verify security properties based on TAP.

Honors & Awards

Freshmen Scholarship **Shanghai Jiao Tong University**
Awards to students with outstanding performance on admission *Sep.2020*

Zhiyuan Honorary Scholarship **Shanghai Jiao Tong University**
Top 2% in SJTU *2020, 2021, 2022*

Projects

Isaiah: A compiler for Mx* language **[Github Link]**

*A **compiler** written in Java for compiling a C-and-Java-like Language named Mx**

- Use **ANTLR4** as frontend generator, subset of LLVM as Intermediate Representation (IR), rv32im as assembly.
- Support **λ-function** and **more complex class grammar** than others.
- With **7k+ LoC** and several test cases' performance **close to GCC-O1**.

YPU: An Speculative Executed CPU on FPGA **[Github Link]**

*A **rv32i CPU** written in Verilog HDL and working fine on FPGA at 100 MHz.*

- Design a single-issued **Speculative Execution** based on **Tomasulo Algorithm**.
- Support various features: precise interruption, BPU, icache, Load Buffer, prefetching.
- With **3k+ LoC**, low circuit path delay design, and outstanding performance on FPGA.

Specialized Skills

Programming Languages: C, C++, Java, Python, Verilog, RISC-V Assembly, Bash, Boogie, Go, SQL
Frameworks & Tools: LLVM, qemu, OpenSBI, Docker, Vivado, LibAFL, AFL++, Fuzzbench
Mandarin: Native Speaker
English: Fully Professional
TOEFL (Feb 2023): 107 (R29/L30/S23/W25)