Shuo Yang

yangsh233@mail2.sysu.edu.cn · shuo-young.github.io · GitHub · Google Scholar

Education

Sun Yat-sen University — Zhuhai, China
Ph.D. in Software Engineering, focus on AI for Software Security and Program Analysis — *Sep 2022 – Present*
Advisors: Prof. Zibin Zheng at InPlusLab and Assoc. Prof. Jiachi Chen

Zhongnan University of Economics and Law — Wuhan, China
B.E. in Information Management System, Rank 8/115 (7%) — *Sep 2018 – Jun 2022*

Publications

[1] **Shuo Yang**, Xingwei Lin, Jiachi Chen, Qingyuan Zhong, Lei Xiao, Renke Huang, Yanlin Wang, Zibin Zheng. "Hyperion: Unveiling DApp Inconsistencies using LLM and Dataflow-Guided Symbolic Execution." *ICSE 2025*. **(CCF-A)**

[2] **Shuo Yang**, Jiachi Chen, Lei Xiao, Jinyuan Hu, Dan Lin, Jiajing Wu, Tao Zhang, Zibin Zheng. "Who is Pulling the Strings: Unveiling Smart Contract State Manipulation Attacks through State-Aware Dataflow Analysis." *IEEE TSE*, 2025. **(CCF-A)**

[3] **Shuo Yang**, Jiachi Chen, Mingyuan Huang, Zibin Zheng, Yuan Huang. "Uncover the Premeditated Attacks: Detecting Exploitable Reentrancy Vulnerabilities by Identifying Attacker Contracts." *ICSE 2024*. **(CCF-A)**

[4] **Shuo Yang**, Jiachi Chen, Zibin Zheng. "Definition and Detection of Defects in NFT Smart Contracts." *ISSTA 2023*. **(CCF-A)**

[5] Mingyuan Huang, Han Liu, **Shuo Yang**, Daoyuan Wu, Shuai Wang. "Revealing the Dark Side of Smart Accounts: An Empirical Study of EIP-7702 Incurred Risks in Blockchain Ecosystem." *USENIX Security 2026*. **(CCF-A)**

[6] Jiachi Chen, Zhenzhe Shao, **Shuo Yang**, Yiming Shen, Yanlin Wang, Ting Chen, Zhenyu Shan, Zibin Zheng. "NumScout: Unveiling Numerical Defects in Smart Contracts using LLM-Pruning Symbolic Execution." *IEEE TSE*, 2025. **(CCF-A)**

[7] Mingxi Ye, Yuhong Nan, Hong-Ning Dai, **Shuo Yang**, Zibin Zheng, Xiapu Luo. "FunFuzz: A Function-oriented Fuzzer for Smart Contract Vulnerability Detection with High Effectiveness and Efficiency." *ACM TOSEM*, 2024. **(CCF-A)**

[8] Jiajing Wu, Dan Lin, Qishuang Fu, **Shuo Yang**, Ting Chen, Zibin Zheng, Bowen Song. "Towards Understanding Asset Flows in Crypto Money Laundering Through the Lenses of Ethereum Heist." *IEEE TIFS*, 2023. **(CCF-A)**

[9] Lei Xiao, **Shuo Yang* (corresponding author)**, Wen Chen, Zibin Zheng. "WakeMint: Detecting Sleep-minting Vulnerabilities in NFT Smart Contracts." *SANER 2025*. **(CCF-B)**

Industry Experience

DarkNavy — Shanghai, China
Research Intern — *Jul 2025 – Present*

- Earned **$22,000** in Web3 bug bounty rewards on ImmuneFi, covering smart contract and client projects.
- Founded the **Defi_Nerd_sec** X/Twitter account; published **50+** root-cause analyses of real-world on-chain attacks, accumulating over **160K** views.
- Released the first Web3 security skill suite **web3-skills**, covering smart contract & client vulnerability detection and on-chain incident root cause analysis (**50+** GitHub stars to date).

GoPlus Security — Remote
Research Intern — *Sep 2024 – Dec 2024*

- Contributed to the development of a static analysis tool for detecting fraudulent behaviors in smart contracts, designing the underlying dataflow analysis algorithms and identification patterns.

- Fine-tuned a **Llama 3**-based model to identify obfuscated/garbled variable naming patterns in Solidity contracts, surfacing malicious contracts that attempt to disguise their true intent.

LightYear Security Lab, Ant Group Hangzhou, China
Research Intern *Aug 2023 – Jan 2024*

- Researched DApp front-end/back-end inconsistency detection, identifying **7** distinct patterns where the functionality or profit advertised by the DApp front-end deviates from the actual contract implementation.
- Built a hybrid analysis framework: instruction-tuned a **Llama 2** model to summarize front-end semantics, and combined it with a symbolic execution engine over IR lifted from EVM bytecode, using dataflow analysis to guide directed exploration and recover contract-level behaviors (work published at **ICSE 2025**).
- Large-scale evaluation revealed over **25%** of flagged inconsistent DApps had already gone offline.

Blockchain Infrastructure R&D Department, WeBank Shenzhen, China
Research Intern *Oct 2021 – Jan 2022*

- Developed the Java SDK for the **FISCO-BCOS** interactive blockchain console and on-chain contract compilation, supporting the v3.0 product iteration.
- Added Chinese national cryptographic standard (**SM**) support to the **Liquid** smart contract compiler, contributing to the Liquid contract language ecosystem.

Security&Community Contributions

- 10 uncovered real-world attack analyses confirmed by **DeFiHackLabs**.
- 2 GPTs prompt-leak bugs confirmed by developers; 1 developer adopted our prompt protection suggestion.
- 2 confirmed issues in **Uniswap V4 Periphery** and Stop Loss Orders with Uniswap V4 Hooks repos.

Awards & Honors

- **National Scholarship**, China 2024
- President Scholarship for Doctoral Students, Sun Yat-sen University 2023
- 1st Prize, China Service Computing Innovation Contest 2023
- 8th Place, Numen Cyber CTF 2023
- 3rd Prize, Competition of Service Outsourcing and Entrepreneurship Innovation 2021
- 3rd Prize, Chinese Undergraduate Internet Software Design Competition 2021
- 3rd Prize, Competition of Service Outsourcing and Entrepreneurship Innovation 2020
- 2nd Prize, Chinese Undergraduate Computer Design Contest 2019

Open-source Software

- **web3-skills** – First Web3 security skill suite for contract/client audit and on-chain incident analysis.
- **SMAsher** – State manipulation attack detector via state-aware dataflow analysis.
- **Hyperion** – DApp inconsistency detector using LLM and symbolic execution.
- **BlockWatchdog** / **Lydia** – Reentrancy attacker contract identification (Python / Rust).
- **NFTGuard** – NFT smart contract defect definition and detection.

Patents

[1] Zibin Zheng, **Shuo Yang**, Peilin Zheng. "A Smart Contract Testing Method, Apparatus, Electronic Device, and Storage Medium." *CN Patent* ZL 2025 1 0010201.8, 2025.

[2] Zibin Zheng, Lei Xiao, **Shuo Yang**, et al. "A Method, Apparatus, Device, and Storage Medium for NFT Smart Contract Defect Detection." *CN Patent* CN119830307A, 2026.

[3] Zibin Zheng, Huizhong Li, **Shuo Yang**, Kaixiang Zhang, Ruibin Fan, Xingqiang Bai, Chengbo Li. "A Method and Apparatus for Determining Test Seeds." *CN Patent* CN115017048A, 2022.

Skills

- **Programming:** Python, Rust, Solidity, Java, C/C++, JavaScript/TypeScript
- **Languages:** English (IELTS 7.0, GRE 321+4.0), Chinese (Native)