Zhuo Zhang

Postdoctoral Research Associate
Department of Computer Science
Purdue University
Room 3133, 305 N. University Street
West Lafayette, IN 47907

Email: zhan3299@purdue.edu (Preferred)
research@zzhang.xyz (Alternative)
web3@zzhang.xyz (Blockchain)
Homepage: https://zzhang.xyz

Research Interests

Software Security and Engineering, Program Analysis (especially for native code without sources), Blockchain Security

Experience

Purdue University, West Lafayette, IN ..... June 2023-present
Postdoctoral Research Associate
Advisor: Dr. Xiangyu Zhang

Purdue University, West Lafayette, IN .....August 2018–June 2023
Research Assistant
Advisor: Dr. Xiangyu Zhang

Tencent KeenLab, Shanghai, China ..... June 2016–July 2017
Security Research Intern

Education

Purdue University, West Lafayette, IN ..... August 2018–August 2023
Ph.D. in Computer Science
Advisor: Dr. Xiangyu Zhang
Thesis: Revamping Binary Analysis with Sampling and Probabilistic Inference

Shanghai Jiao Tong University, Shanghai, China .....September 2014–June 2018
B.Sc. in Computer Science (w/ Zhiyuan Honours)
Thesis: Static Binary Analysis for Decompilation

Publications

Conference Proceedings

[1] **Nyx: Detecting Exploitable Front-Running Vulnerabilities in Smart Contracts**.
Wuqi Zhang, **Zhuo Zhang**, Qingkai Shi, Lu Liu, Lili Wei, Yepang Liu, Xiangyu Zhang, and Shing-Chi Cheung.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2024.

[2] **ODSCAN: Backdoor Scanning for Object Detection Models**.
Siyuan Cheng, Guangyu Shen, Guanhong Tao, Kaiyuan Zhang, **Zhuo Zhang**, Shengwei An, Xiangzhe Xu, Yingqi Liu, Shiqing Ma, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2024.

[3] **ParaFuzz: An Interpretability-Driven Technique for Detecting Poisoned Samples in NLP**.
Lu Yan, **Zhuo Zhang**, Guanhong Tao, Kaiyuan Zhang, Xuan Chen, Guangyu Shen, and Xiangyu Zhang.
In *Proceedings of the Conference on Neural Information Processing Systems (NeurIPS)*, 2023.

[4] **PEM: Representing Binary Program Semantics for Similarity Analysis via A Probabilistic Execution Model**.
Xiangzhe Xu, Zhou Xuan, Shiwei Feng, Siyuan Cheng, Yapeng Ye, Qingkai Shi, Guanhong Tao, Le Yu, **Zhuo Zhang**, and Xiangyu Zhang.
In *Proceedings of the International Symposium on the Foundations of Software Engineering (FSE)*, 2023.

[5] **Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract**.
Zhuo Zhang, Zhiqiang Lin, Marcelo Morales, and Kaiyuan Zhang.
In *Proceedings of the USENIX Security Symposium (Security)*, 2023.

[6] **Pelican: Exploiting Backdoors of Naturally Trained Deep Learning Models In Binary Code Analysis**.
Zhuo Zhang, Guanhong Tao, Guangyu Shen, Shengwei An, Qiuling Xu, Yingqi Liu, Yapeng Ye, Yaoxuan Wu, and Xiangyu Zhang.
In *Proceedings of the USENIX Security Symposium (Security)*, 2023.

[7] **Improving Binary Code Similarity Transformer Models by Semantics-Driven Instruction Deemphasis**.
Xiangzhe Xu, Shiwei Feng, Yapeng Ye, Guangyu Shen, Zian Su, Siyuan Cheng, Guanhong Tao, Qingkai Shi, **Zhuo Zhang**, and Xiangyu Zhang.
In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*, 2023.

[8] **Demystifying Exploitable Bugs in Smart Contracts**.
Zhuo Zhang, Brian Zhang, Wen Xu, and Zhiqiang Lin.
In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE)*, May 2023.

[9] **D-ARM: Disassembling ARM Binaries by Lightweight Superset Instruction Interpretation and Graph Modeling**.
Yapeng Ye, **Zhuo Zhang**, Qingkai Shi, Yousra Aafer, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2023.

[10] **Poirot: Probabilistically Recommending Protections for the Android Framework**.
Zeinab El-Rewini, **Zhuo Zhang**, and Yousra Aafer.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2022.

[11] **Constrained Optimization with Dynamic Bound-scaling for Effective NLP Backdoor Defense**.
Guangyu Shen, Yingqi Liu, Guanhong Tao, Xuwei Liu, **Zhuo Zhang**, Shengwei An, Shiqing Ma, and Xiangyu Zhang.
In *Proceedings of the International Conference on Machine Learning (ICML)*, 2022.

[12] **TensileFuzz: Facilitating Seed Input Generation in Fuzzing via String Constraint Solving**.
Xuwei Liu, Wei You, **Zhuo Zhang**, and Xiangyu Zhang.
In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*, 2022.

[13] **Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security**.
Guanhong Tao, Yingqi Liu, Guangyu Shen, Qiuling Xu, Shengwei An, **Zhuo Zhang**, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2022.

[14] **StochFuzz: Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting**.

Zhuo Zhang, Wei You, Guanhong Tao, Yousra Aafer, Xuwei Liu, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2021.
* **CSAW 2021 Best Applied Security Paper Award TOP-10 Finalists**.

[15] **OSPREY: Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary**.
Zhuo Zhang, Yapeng Ye, Wei You, Guanhong Tao, Wen-chuan Lee, Yonghwi Kwon, Yousra Aafer, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2021.

[16] **NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces**.
Yapeng Ye, **Zhuo Zhang**, Fei Wang, Xiangyu Zhang, and Dongyan Xu.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February 2021.

[17] **ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without Instrumentation**.
Le Yu, Shiqing Ma, **Zhuo Zhang**, Guanhong Tao, Xiangyu Zhang, Dongyan Xu, Vincent E. Urias, Han Wei Lin, Gabriela Ciocarlie, Vinod Yegneswaran, and Ashish Gehani.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February 2021.

[18] **PMP: Cost-Effective Forced Execution with Probabilistic Memory Pre-Planning**.
Wei You, **Zhuo Zhang**, Yonghwi Kwon, Yousra Aafer, Fei Peng, Yu Shi, Carson Makena Harmon, and Xiangyu Zhang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2020.

[19] **BDA: Practical Dependence Analysis for Binary Executables by Unbiased Whole-Program Path Sampling and Per-Path Abstract Interpretation**.
Zhuo Zhang, Wei You, Guanhong Tao, Guannan Wei, Yonghwi Kwon, and Xiangyu Zhang.
In *Proceedings of the ACM on Programming Languages Volume 3 Issue OOPSLA (OOPSLA)*, October 2019.
* **ACM SIGPLAN Distinguished Paper Award**.

[20] **Probabilistic Disassembly**.
Kenneth Miller, Yonghwi Kwon, Yi Sun, **Zhuo Zhang**, Xiangyu Zhang, and Zhiqiang Lin.
In *Proceedings of the ACM/IEEE International Conference on Software Engineering (ICSE)*, May 2019.

Honors and Awards

Academic Awards

- **CSAW Best Applied Security Paper Award TOP-10 Finalists**, NYU CCS 2021
- **Emil Stefanov Memorial Partial Fellowship**, Purdue University 2021
- **OOPSLA 2019 Distinguished Paper Award**, ACM SIGPLAN 2019
- Zhiyuan Honor Degree of B.Sc. in Computer Science, SJTU 2018
- Natinoal Scholarship, Ministry of Education of China (Top 2%) 2016

Selected Capture-The-Flag (CTF)

- 1st place (w/ Offside Labs) at Paradigm CTF 2023
- 1st place at the 40th IEEE S&P Celebration Scavenger Hunt 2019
- 4th place (w/ A*0*E) at DEFCON CTF 2018
- 3rd place (w/ A*0*E) at DEFCON CTF 2017

Selected Web3 Bug Bounties

- Critical bug report for *Anonymous Project* $3,000
- Critical bug report for Duet Protocol $50,000
- Critical bug report for Grizzly.fi $10,000
- Critical bug report for ApeX Protocol $25,000
- Critical bug report for Infinity NFT Marketplace $20,000
- Critical bug reports for ENS $40,000

Services

Program Committee Member

- The ACM Conference on Computer and Communications Security (CCS), 2024
- International Conference on Software Engineering (ICSE), 2025
- International Conference on Automated Software Engineering (ASE), 2024
- International Symposium on Software Testing and Analysis (ISSTA), 2024
- The ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2024
- Workshop on Binary Analysis Research (BAR), 2022

Reviewer

- IEEE Transactions on Software Engineering
- IEEE/ACM Transactions on Networking
- The Association for Computational Linguistics (ACL) Rolling Review, 2023

Sub-reviewer

- USENIX Security Symposium
- IEEE Symposium on Security and Privacy (Oakland)
- The Network and Distributed System Security Symposium (NDSS)
- International Conference on Dependable Systems and Networks (DSN)
- International Conference on Automated Software Engineering (ASE)
- International Symposium on Software Testing and Analysis (ISSTA)
- International Symposium on the Foundations of Software Engineering (FSE)
- The ACM Conference on Computer and Communications Security (CCS)
- The ACM Conference on Systems, Programming, Languages, and Applications (OOPSLA)

Invited Talks

Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract
Usenix Security 2023, Anaheim, CA ..... August 2023

Exploiting Backdoors of Naturally Trained Deep Learning Models In Binary Code Analysis
Usenix Security 2023, Anaheim, CA ..... August 2023

Demystifying Exploitable Bugs in Smart Contracts
Georgia Institute of Technology, Virtually ..... May 2023

Blockchain 101

Rutgers University, Virtually ..... February 2022

A Systematic Study of Recent Smart Contract Security Vulnerabilities

Crypto Economics Security Conference (CESC) 2022, Berkeley, CA ..... November 2022

Advanced Binary Analysis via Probabilistic Inference and Distribution Analysis

Northwestern University, Evanston, IL ..... May 2022

Renmin University of China, Virtually ..... November 2022

Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting

S&P 2021, Virtually ..... May 2020

Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary

S&P 2021, Virtually ..... May 2020

Cost-effective Forced Execution with Probabilistic Memory Pre-planning

S&P 2020, Virtually ..... May 2020

Practical Dependence Analysis for Binary Executables by Unbiased Whole-Program Path Sampling and Per-Path Abstract Interpretation

SPLASH 2019, Athens, Greece ..... October 2019

Renmin University of China, Beijing, China ..... November 2019

Hello World: A Brief Introduction to Capture-The-Flag

Renmin University of China, Beijing, China ..... November 2019

Last updated: June 3, 2024