

ZHUO ZHANG

Ph.D. student
Department of Computer Science
Purdue University
Room 3133, 305 N. University Street
West Lafayette, IN 47907

Email: zhan3299@purdue.edu (Preferred)
academia@izhuer.me (Alternative)
Homepage: <http://izhuer.me>

RESEARCH INTERESTS

Software Security and Engineering, Program Analysis (especially for native code without sources), Web 3.0 Security (\$100,000 bug bounty awarded)

EDUCATION

- Purdue University**, West Lafayette, IN August 2018–Present
Ph.D. in Computer Science
Advisor: Dr. Xiangyu Zhang
- Shanghai Jiao Tong University**, Shanghai, China September 2014–June 2018
B.Sc. in Computer Science (w/ Zhiyuan Honours)
Theses: Static Binary Analysis for Decompilation

PUBLICATIONS

Conference Proceedings

- [1] **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.
- [2] **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.
- [3] **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)*, 2022.
- [4] **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.
- [5] **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.

- [6] **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.**
- [7] **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.
- [8] **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.
- [9] **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.
- [10] **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.
- [11] **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.**
- [12] **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 at the 40th IEEE S&P Celebration Scavenger Hunt 2019
- 4th place (w/ A*0*E) at DEFCON CTF 2018 2018
- 3rd place (w/ A*0*E) at DEFCON CTF 2017 2017

Selected Web 3.0 Bug Bounties

- Critical bug report for *Anonymous Project*\$3,000
- Critical bug report for **Duet Protocol** (w/ Wen Xu) \$50,000
- Critical bug report for **Grizzly.fi** \$10,000
- Critical bug report for **ApeX Protocol** NFT + \$15,000
- Critical bug report for **Infinity NFT Marketplace** \$20,000

SERVICES

Program Committee Member

- Workshop on Binary Analysis Research (BAR), NDSS 2022

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

Advanced Binary Analysis via Probabilistic Inference and Distribution Analysis

Northwestern University, Evanston, ILMay 2022

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

S&P 2021, VirtuallyMay 2020

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

S&P 2021, VirtuallyMay 2020

PMP: Cost-effective Forced Execution with Probabilistic Memory Pre-planning

S&P 2020, VirtuallyMay 2020

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

SPLASH 2019, Athens, GreeceOctober 2019

Renmin University of China, Beijing, ChinaNovember 2019

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

Renmin University of China, Beijing, ChinaNovember 2019

EXPERIENCE

Purdue University, West Lafayette, IN August 2018–Present

Research Assistant

Advisor: Dr. Xiangyu Zhang

Tencent KeenLab, Shanghai, China June 2016–July 2017

Security Research Intern

Last updated: August 27, 2022