Zhuo Zhang

Postdoctoral Fellow in Computer Science, Purdue
(765) 714-2552 · zhan3299@purdue.edu · https://zzhang.xyz · Zhuo Zhang

Education

Purdue University — **West Lafayette, IN, USA**
Ph.D. in Computer Science — *Aug 2018 - Aug 2023*
Committees: *Xiangyu Zhang (advisor)*, *Z. Berkay Celik*, *Suresh Jagannathan*, *Ninghui Li*
Dissertation: *Revamping Binary Analysis with Sampling and Probabilistic Inference*
ACM SIGSAC Doctoral Dissertation Award

Shanghai Jiao Tong University — **Shanghai, China**
B.S. in Computer Science (*Zhiyuan Honor Degree*) — *Aug 2014 - May 2018*

Academic and Industry Appointments

Purdue University — **West Lafayette, IN, USA**
Postdoctoral Fellow — *May 2023 - Present*
Graduate Research Assistant — *Aug 2018 - May 2023*

Honors and Awards

ACM SIGSAC Doctoral Dissertation Award — *2024*
Recognized as the highest honor for a Ph.D. graduate in cybersecurity, awarded for "*groundbreaking contributions in developing a novel probabilistic binary analysis that effectively synergizes learning and reasoning in reverse engineering*".

Distinguished Paper Award
ACM Conference on Computer and Communications Security (CCS) — *2024*
ACM Conference on Systems, Programming, Languages, and Applications (OOPSLA) — *2019*

Distinguished Reviewer Award
International Conference on Automated Software Engineering (ASE) — *2024*

Emil Stefanov Memorial Partial Fellowship — *2021*
Awarded by the Stefanov family for outstanding contributions to cybersecurity research.

CSAW Best Applied Security Paper Award TOP-10 Finalists — *2021*

Selected Achievements

Open Source Contributions (Over 1,800 GitHub Stars) — *By 2024*
Released and open-sourced numerous academic and industrial projects, garnering over 1,800 GitHub stars.

Capture-The-Flag (CTF)
1st Place: Paradigm Blockchain CTF (with Offside Labs) — *2023*
1st Place: DEFCON CTF (with A*0*E) — *2020*
1st Place: IEEE S&P Celebration Scavenger Hunt (solo) — *2019*
4th Place: DEFCON CTF (with A*0*E) — *2018*
3rd Place: DEFCON CTF (with A*0*E) — *2017*

Transitioning Research into Real-World Practice by ONR — *2022*
Successfully transitioned all dissertation work into real-world practice under the Office of Naval Research (ONR), a distinction achieved by fewer than 20% of funded projects.

Grants

PI. "*EDB: The Next-Generation Solidity Debugger for an Enhanced Ethereum Development Experience*". Funded by the ***Ethereum Foundation***.

Co-PI, with Xiangyu Zhang (PI). "*AutoPWN: Generating CTF Challenge Benchmarks to Evaluate Offensive Cybersecurity Capabilities of LLMs with Minimal Risk of Data Leakage*". Funded by ***Anthropic***.

Co-PI, with Xiangyu Zhang (PI). "*Amazon Trusted AI Challenge: An Agentic Red Teaming Framework for Code LLMs*". Funded by ***Amazon*** (acceptance rate: 11%, 10/90).

Co-PI, with Xiangyu Zhang (PI), Lin Tan (Co-PI) and Tianyi Zhang(Co-PI). "*R^3: Rapid and Reliable Repair of Healthcare Software Vulnerabilities by Knowledge Graphs and Multi-modal AI Models*". Submitted to the ***Advanced Research Projects Agency for-Health (ARPA-H)***.

Publications

Highlight: Authored *7 first-author papers* published in top-tier conferences, including **S&P** (×3), **USENIX Security** (×2), **ICSE** (×1), and **OOSPLA** (×1). Additionally, supervised *6 papers* (marked with *) during the postdoctoral fellowship.

NDSS 2025 Xiangzhe Xu, **Zhuo Zhang***, Zian Su, Ziyang Huang, Shiwei Feng, Yapeng Ye, Nan Jiang, Danning Xie, Siyuan Cheng, Lin Tan, Xiangyu Zhang. *Unleashing the Power of Generative Model in Recovering Variable Names from Stripped Binary.* In 32nd Annual Network and Distributed System Security Symposium, NDSS 2025.

ICSE 2025 Yi Sun, **Zhuo Zhang***, Xiangyu Zhang. *FairChecker: Detecting Fund-stealing Bugs in DeFi Protocols via Fairness Validation.* In Proceedings of the 47th IEEE/ACM International Conference on Software Engineering, ICSE 2025.

S&P 2024 **Zhuo Zhang**, Guangyu Shen, Guanhong Tao, Siyuan Cheng, Xiangyu Zhang. *On Large Language Models' Resilience to Coercive Interrogation.* In IEEE Symposium on Security and Privacy, SP 2024.

CCS 2024 Danning Xie, **Zhuo Zhang***, Nan Jiang, Xiangzhe Xu, Lin Tan, Xiangyu Zhang. *ReSym: Harnessing LLMs to Recover Variable and Data Structure Symbols from Stripped Binaries.* In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, CCS 2024. **🏆 ACM SIGSAC Distinguished Paper Award.**

S&P 2024 Wuqi Zhang, **Zhuo Zhang***, Qingkai Shi, Lu Liu, Lili Wei, Yepang Liu, Xiangyu Zhang, Shing-Chi Cheung. *Nyx: Detecting Exploitable Front-Running Vulnerabilities in Smart Contracts.* In IEEE Symposium on Security and Privacy, SP 2024.

NeurIPS 2024 Brian Zhang, **Zhuo Zhang***. *Detecting Bugs with Substantial Monetary Consequences by LLM and Rule-based Reasoning.* In Annual Conference on Neural Information Processing Systems 2024, NeurIPS 2024.

PLDI 2024 Guannan Wei, Danning Xie, Wuqi Zhang, Yongwei Yuan, **Zhuo Zhang***. *Consolidating Smart Contracts with Behavioral Contracts.* In Proceedings of the ACM on Programming Languages, volume 8, number PLDI, pages 965–989.

FSE 2024 Zian Su, Xiangzhe Xu, Ziyang Huang, **Zhuo Zhang**, Yapeng Ye, Jianjun Huang, Xiangyu Zhang. *CodeArt: Better Code Models by Attention Regularization When Symbols Are Lacking.* In Proceedings of the ACM on Software Engineering, volume 1, number FSE, pages 562–585.

EACL 2024 Chanwoo Bae, Guanhong Tao, **Zhuo Zhang**, Xiangyu Zhang. *Threat Behavior Textual Search by Attention Graph Isomorphism.* In Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics, EACL 2024 - Volume 1: Long Papers.

ICSE 2024 Xuwei Liu, Wei You, Yapeng Ye, **Zhuo Zhang**, Jianjun Huang, Xiangyu Zhang. *FuzzInMem: Fuzzing Programs via In-memory Structures.* In Proceedings of the 46th IEEE/ACM International Conference on Software Engineering, ICSE 2024.

ISSTA 2024 Dongnan He, Dongchen Xie, Yujie Wang, Wei You, Bin Liang, Jianjun Huang, Wenchang Shi, **Zhuo Zhang**, Xiangyu Zhang. *Define-Use Guided Path Exploration for Better Forced Execution.* In Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, ISSTA 2024.

S&P 2024 Siyuan Cheng, Guangyu Shen, Guanhong Tao, Kaiyuan Zhang, **Zhuo Zhang**, Shengwei An,

Xiangzhe Xu, Yingqi Li, Shiqing Ma, Xiangyu Zhang. *OdScan: Backdoor Scanning for Object Detection Models.* In IEEE Symposium on Security and Privacy, SP 2024.

Security 2024 Le Yu, Yapeng Ye, **Zhuo Zhang**, Xiangyu Zhang. *Cost-effective Attack Forensics by Recording and Correlating File System Changes.* In 33rd USENIX Security Symposium, USENIX Security 2024.

ICSE 2023 **Zhuo Zhang**, Brian Zhang, Wen Xu, Zhiqiang Lin. *Demystifying Exploitable Bugs in Smart Contracts.* In 45th IEEE/ACM International Conference on Software Engineering, ICSE 2023. **🏆 Achieved over 1,500 GitHub stars and 200 forks, gaining widespread adoption within the blockchain community.**

Security 2023 **Zhuo Zhang**, Zhiqiang Lin, Marcelo Morales, Xiangyu Zhang, Kaiyuan Zhang. *Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract.* In 32nd USENIX Security Symposium, USENIX Security 2023. **🏆 Thwarted several live attacks, safeguarding over 2 million US dollars in funds.**

Security 2023 **Zhuo Zhang**, Guanhong Tao, Guangyu Shen, Shengwei An, Qiuling Xu, Yingqi Liu, Yapeng Ye, Yaoxuan Wu, Xiangyu Zhang. *PELICAN: Exploiting Backdoors of Naturally Trained Deep Learning Models In Binary Code Analysis.* In 32nd USENIX Security Symposium, USENIX Security 2023.

NeurIPS 2023 Lu Yan, **Zhuo Zhang**, Guanhong Tao, Kaiyuan Zhang, Xuan Chen, Guangyu Shen, Xiangyu Zhang. *ParaFuzz: An Interpretability-Driven Technique for Detecting Poisoned Samples in NLP.* In Annual Conference on Neural Information Processing Systems 2023, NeurIPS 2023.

ISSTA 2023 Xiangzhe Xu, Shiwei Feng, Yapeng Ye, Guangyu Shen, Zian Su, Siyuan Cheng, Guanhong Tao, Qingkai Shi, **Zhuo Zhang**, Xiangyu Zhang. *Improving Binary Code Similarity Transformer Models by Semantics-Driven Instruction Deemphasis.* In Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis, ISSTA 2023.

FSE 2023 Xiangzhe Xu, Zhou Xuan, Shiwei Feng, Siyuan Cheng, Yapeng Ye, Qingkai Shi, Guanhong Tao, Le Yu, **Zhuo Zhang**, Xiangyu Zhang. *PEM: Representing Binary Program Semantics for Similarity Analysis via a Probabilistic Execution Model.* In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2023.

S&P 2023 Yapeng Ye, **Zhuo Zhang**, Qingkai Shi, Yousra Aafer, Xiangyu Zhang. *D-ARM: Disassembling ARM Binaries by Lightweight Superset Instruction Interpretation and Graph Modeling.* In 44th IEEE Symposium on Security and Privacy, SP 2023.

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

ICML 2022 Guangyu Shen, Yingqi Liu, Guanhong Tao, Qiuling Xu, **Zhuo Zhang**, Shengwei An, Shiqing Ma, Xiangyu Zhang. *Constrained Optimization with Dynamic Bound-scaling for Effective NLP Backdoor Defense.* In International Conference on Machine Learning, ICML 2022.

ISSTA 2022 Xuwei Liu, Wei You, **Zhuo Zhang**, Xiangyu Zhang. *TensileFuzz: facilitating seed input generation in fuzzing via string constraint solving.* In ISSTA '22: 31st ACM SIGSOFT International Symposium on Software Testing and Analysis.

S&P 2022 Guanhong Tao, Yingqi Liu, Guangyu Shen, Qiuling Xu, Shengwei An, **Zhuo Zhang**, Xiangyu Zhang. *Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security.* In 43rd IEEE Symposium on Security and Privacy, SP 2022.

S&P 2021 **Zhuo Zhang**, Wei You, Guanhong Tao, Yousra Aafer, Xuwei Liu, Xiangyu Zhang. *StochFuzz: Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting.* In 42nd IEEE Symposium on Security and Privacy, SP 2021. **🏆 CSAW 2021 Best Applied Security Paper Award TOP-10 Finalists.**

S&P 2021 **Zhuo Zhang**, Yapeng Ye, Wei You, Guanhong Tao, Wen-Chuan Lee, Yonghwi Kwon, Yousra Aafer, Xiangyu Zhang. *OSPREY: Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary.* In 42nd IEEE Symposium on Security and Privacy, SP 2021.

NDSS 2021 Yapeng Ye, **Zhuo Zhang**, Fei Wang, Xiangyu Zhang, Dongyan Xu. *NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces.* In 28th Annual Network and Distributed System Security Symposium, NDSS 2021.

NDSS 2021 Le Yu, Shiqing Ma, **Zhuo Zhang**, Guanhong Tao, Xiangyu Zhang, Dongyan Xu, Vincent E. Urias, Han Wei Lin, Gabriela F. Ciocarlie, Vinod Yegneswaran, Ashish Gehani. *ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without Instrumentation.* In 28th Annual Network and Distributed System Security Symposium, NDSS 2021.

S&P 2020 Wei You, **Zhuo Zhang**, Yonghwi Kwon, Yousra Aafer, Fei Peng, Yu Shi, Carson Harmon, Xiangyu Zhang. *PMP: Cost-effective Forced Execution with Probabilistic Memory Pre-planning.* In 2020 IEEE Symposium on Security and Privacy, SP 2020.

OOPSLA 2019 **Zhuo Zhang**, Wei You, Guanhong Tao, Guannan Wei, Yonghwi Kwon, Xiangyu Zhang. *BDA: practical dependence analysis for binary executables by unbiased whole-program path sampling and per-path abstract interpretation.* In Proceedings of the ACM on Programming Languages, volume 3, number OOPSLA, pages 137:1–137:31. 🏆 **ACM SIGPLAN Distinguished Paper Award.**

ICSE 2019 Kenneth A. Miller, Yonghwi Kwon, Yi Sun, **Zhuo Zhang**, Xiangyu Zhang, Zhiqiang Lin. *Probabilistic disassembly.* In Proceedings of the 41st International Conference on Software Engineering, ICSE 2019.

Academic Services

Program Committee Member 🏆 (×1): **ACM SIGSOFT Distinguished Reviewer Award (ASE 2024)**

USENIX Security Symposium	*2025*
The ACM Conference on Computer and Communications Security (CCS)	*2024, 2025*
International Conference on Software Engineering (ICSE)	*2025*
International Symposium on Software Testing and Analysis (ISSTA)	*2024, 2025*
International Conference on Automated Software Engineering (ASE)	*2024*
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	*2024*
The ACM ASIA Conference on Computer and Communications Security (ASIACCS)	*2024*
Workshop on Binary Analysis Research (BAR)	*2022*

Journal Reviewer

IEEE Transactions on Information Forensics and Security (TIFS)	*2024*
IEEE Transactions on Software Engineering (TSE)	*2023*
IEEE/ACM Transactions on Networking (TON)	*2023*
The Association for Computational Linguistics (ACL) Rolling Review	*2023*

External 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)

Teaching

Teaching Assistant, Purdue University — *Fall 2024*
CS 592: AI and Security

Guest Lecturer, University of Massachusetts Amherst — *Fall 2024*
CS 520: Theory and Practice of Software Engineering

Guest Lecturer, Rutgers University — *Fall 2023*

COMPSCI 360: Introduction to Computer and Network Security

Guest Lecturer, Rutgers University *Spring 2023*
CS 546: Computer System Security

Guest Lecturer, Northwestern University *Spring 2022*
COMPSCI 496: Advanced System Security

Advising and Mentoring

Brian Zhang (High School Student, William Henry Harrison High School) *2022 - 2024*
Currently an undergraduate student at the University of Texas at Austin
Worked on detecting high monetary issue vulnerabilities in smart contracts and coauthored two publications in ICSE 2023 and NeurIPS 2024.

Fangyan Shi (Undergraduate Student at Yao Class, Tsinghua University) *2024*
Currently an undergraduate student at Tsinghua University
Worked on developing an efficient and effective Solidity debugger for Ethereum smart contracts.

Yaoxuan Wu (Undergraduate Student at Turing Class, Peking University) *2022*
Currently a Ph.D. student at the University of California Los Angeles
Worked on red-teaming and adversarial attacks on binary analysis deep learning models and coauthored a publication in USENIX Security 2023.

Xiangzhe Xu (Undraduate Student, Nanjing University) *2019 - 2020*
Currently a Ph.D. student at Purdue University
Worked on developing binary similarity analysis tools and coauthored two publications in ISSTA 2023 and FSE 2023 for projects conducted under my guidance at that time.

Wuqi Zhang (Graduate Student, Hong Kong University of Science and Technology) *2023 - 2024*
Currently a research scientist at MegaETH working on next-generation blockchain technology
Worked on developing automatic detection and remediation of vulnerabilities in smart contracts and coauthored a publication in S&P 2024.

Lu Yan (Graduate Student, Purdue University) *2023 - 2024*
Currently a Ph.D. student at Purdue University
Worked on introducing fuzzing techniques to find adversarial samples in deep learning language models and coauthored a publication in NeurIPS 2023.

Danning Xie (Graduate Student, Purdue University) *2023 - 2024*
Currently a Ph.D. student at Purdue University
Worked on using the power of large language models for binary decompilation and coauthored a publication in CCS 2024 that received the Distinguished Paper Award.

Invited Talks and Presentations

Beyond C/C++: Probabilistic and LLM Methods for Rust Binary Reverse Engineering
CCS FEAST 2024. Salt Lake City, UT, USA *Oct 2024*

When Binary Analysis Meets Web3: Automating Threat Detection and Prevention
UCSB Gigabrains Blockchain Seminar. Virtual *Oct 2024*

On Large Language Models' Resilience to Coercive Interrogation
S&P 2024. San Francisco, CA, USA *May 2024*

Demystifying Exploitable Bugs in Smart Contracts
Georgia Institute of Technology SSLab's Security Seminar. Virtual *May 2023*
CESC, Berkeley, CA, USA *Oct 2022*

Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract
USENIX Security 2023. Anaheim, CA, USA *Aug 2023*

PELICAN: Exploiting Backdoors of Naturally Trained Deep Learning Models in Binary Code Analysis
USENIX Security 2023. Anaheim, CA, USA *Aug 2023*

STOCHFUZZ: Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting
S&P 2021. Virtual *May 2021*

OSPREY: Recovery of Variable and Data Structure via Probabilistic Analysis for Stripped Binary
S&P 2021. Virtual *May 2021*

BDA: Practical Dependence Analysis for Binary Executables by Unbiased Whole-Program Path Sampling and Per-Path Abstract Interpretation
OOPSLA 2019. Athens, Greece *Oct 2019*