Xiangyu Zhang

2/24/2024

Samuel Conte Professor
Purdue University
Department of Computer Science
LWSN Building 3154K
305 N. University Street
West Lafayette, IN 47907

Email: xyzhang@cs.purdue.edu
URL: `http://www.cs.purdue.edu/homes/xyzhang`
Telephone: 520-891-7317

Short Bio

I am a computer scientist specializing in AI security, cyber forensics, and software security and analysis. My work involves developing techniques to detect bugs, including security vulnerabilities, in traditional software systems as well as AI models and systems, and to diagnose runtime failures. By February 2024, I have served as the Principal Investigator (PI) for numerous projects funded by organizations such as DARPA, IARPA, ONR, NSF, AirForce, and industry, securing over $13 million in research funding. Many of the techniques developed by my team have successfully transitioned into practical applications. Throughout my career, I have graduated 25 PhD students and mentored 8 post-docs, with fifteen of them securing academic positions in various universities. Many of them have been honored with NSF Career Awards or comparable recognitions. On February 24th, 2024, my Google Scholar page reports 14,478 citations to my papers, with an h-index of 64 and an i10-index of 193. According to csrankings.org, I have a notable record of 89 publications in top-tier venues spanning from 2014 to 2024. Additionally, according to `https://nebelwelt.net/pubstats/top-authors-sys.html`(as of February 24th, 2024), I am ranked eighth worldwide among the most productive scholars in systems research. My research has been recognized with numerous distinguished paper awards at top-tier conferences. Notably, I received the ACM SIGPLAN Distinguished Dissertation Award in 2006, the highest honor for a PhD dissertation in Programming Languages. Furthermore, I co-supervised a PhD dissertation that was honored with the ACM SIGSAC Distinguished Dissertation Award in 2018, the highest recognition in the field of cybersecurity.

RESEARCH INTERESTS

AI Security: identify and fix security vulnerabilities in AI models and systems, such as backdoors and privacy leakage; **Software Engineering and Programming Languages:** static, dynamic, and symbolic program analysis for various kinds of programs, e.g., binary executables and smart contracts; **Software and System Security:** finding software vulnerabilities, analyzing malware, and attack forensics.

EMPLOYMENT HISTORY

11/2016-present, Full Professor	Dept. of Computer Science, Purdue University, West Lafayette, IN
11/2012-10/2016, Associate Professor	Dept. of Computer Science, Purdue University, West Lafayette, IN
10/2006-10/2012, Assistant Professor	Dept. of Computer Science, Purdue University, West Lafayette, IN

EDUCATION

08/00-09/06, Ph.D.	Dept. of Computer Science, University of Arizona, Tucson, AZ Thesis: "Fault Location via Precise Dynamic Slicing" Rajiv Gupta, advisor
09/98-07/00, M.S.	Dept. of Computer Science, University of Sci. & Tech. of China, Hefei, P.R.China Thesis: "Human Face Modeling and Animation from Orthogonal Views" Yiyun Chen, advisor
09/93-07/98, B.S.	Dept. of Computer Science, University of Sci. & Tech. of China, Hefei, P.R.China

AWARDS

(OOPSLA is a top tier Programming Language conference; FSE, ICSE, ASE are top tier Software Engienering conferences; and CCS, NDSS, USENIX Security are top tier Security conferences)

- The Purdue-UMass team, previously the Purdue-Rutgers team (led by Zhang) ranked number 1 in 13 out of the 18 rounds in the **IARPA TrojAI Competition** (for backdoor scanning of deep learning models), 2020-2024.
- **Most Influential Professor** in the Department of Computer Science, Purdue, 2021-2023.
- **CSAW Best Applied Security Paper Award TOP-10 Finalists**, 2019.
- **ACM SIGPLAN Distinguished Paper Award** on OOPSLA, 2019.
- Former Brendan Saltaformmagio's PhD Dissertation co-supervised with Dongyan Xu received **ACM SIGACT Distinguished Dissertation Award**, 2017.
- **Distinguished Paper Award** on USENIX Security, 2017.
- **Distinguished Artifact Award** on FSE, 2016.
- **ACM SIGSOFT Distinguished Paper Award** on FSE, 2016.
- **NDSS Distinguished Paper Award**, 2016.
- **CSAW Best Applied Security Paper Award TOP-10 Finalists**, 2015.
- **CCS Best Paper Award**, 2015.
- **College of Science Graduate Student Mentoring Award**, 2015, Purdue University.
- **Best Student Paper Award** in *the 24th USENIX Security Symposium*, 2014, San Diego, CA (**1 out of 350 submissions**).
- **University Scholar**, 2014-2019, Purdue Univeristy, IN.
- **ACM SIGSOFT Distinguished Paper Award** and **Best Paper Award**, "PIEtrace: Platform Independent Executable Trace," *the 28th IEEE/ACM International Conference on Automated Software Engineering*, 2013, Santa Clara, CA (**1 out of 317 submissions**).
- **2009 NSF Career Award**, "Scalable Dynamic Program Reasoning".
- **2006 ACM SIGPLAN Doctoral Dissertation Award**, "Fault Location via Precise Dynamic Slicing".
- **ACM SIGSOFT Distinguished Paper Award**, "Precise Dynamic Slicing Algorithms," *International Conference on Software Engineering*, May 2003, Portland, Oregon.

JOURNAL PUBLICATIONS

[27] TSE Mohannad Alhanahnah, Shiqing Ma, Ashish Gehani, Gabriela F. Ciocarlie, Vinod Yegneswaran, Somesh Jha, Xiangyu Zhang, "AutoMPI: Automated Multiple Perspective Attack Investigation With Semantics Aware Execution Partitioning", *IEEE Transactions on Software Engineering* , 49(4): 2761-2775, 2023.

[26] SCP Qiang Zhang, Lei Xu, Xiangyu Zhang, Baowen Xu, "Quantifying the interpretation overhead of Python", *Science of Computer Programming* , 215: 102759, 2022.

[25] TCSVT Liqi Yan, Siqi Ma, Qifan Wang, Yingjie Victor Chen, Xiangyu Zhang, Andreas E. Savakis, Dongfang Liu, "Video Captioning Using Global-Local Representation", *IEEE Transactions on Circuits and Systems Video Technology* , 32(10): 6642-6656, 2022.

[24] TC Derui Wang, Chaoran Li, Sheng Wen, Qing-Long Han, Surya Nepal, Xiangyu Zhang, Yang Xiang, "Daedalus: Breaking Nonmaximum Suppression in Object Detection via Adversarial Examples", *IEEE Transactions on Cybernetics* , 52(8): 7427-7440, 2022.

[23] ESE Yongqiang Tian, Shiqing Ma, Ming Wen, Yepang Liu, Shing-Chi Cheung, Xiangyu Zhang, “To what extent do DNN-based image classification models make unreliable inferences?”, *Empirical Software Engineering* , 26(4): 84, 2021.

[22] TIFS Hassaan Irshad, Gabriela F. Ciocarlie, Ashish Gehani, Vinod Yegneswaran, Kyu Hyung Lee, Jignesh M. Patel, Somesh Jha, Yonghwi Kwon, Dongyan Xu, Xiangyu Zhang, “TRACE: Enterprise-Wide Provenance Tracking for Real-Time APT Detection”, *IEEE Transactions on Information Forensics and Security* , 16: 4363-4376, 2021.

[21] JSS Junyu Lin, Lei Xu, Yingqi Liu, Xiangyu Zhang, “Black-box adversarial sample generation based on differential evolution”, *Journal of Systems and Software* , 2020.

[20] TDSC , Wei You, Bin Liang, Wenchang Shi, Peng Wang, Xiangyu Zhang, “TaintMan: An ART-Compatible Dynamic Taint Analysis Framework on Unmodified and Non-Rooted Android Devices”, *IEEE Transactions on Dependable Secure Computing* , 17(1): 209-222, 2020.

[19] ACCESS , Yang Zhang, Shicheng Dong, Xiangyu Zhang, Huan Liu, Dongwen Zhang, “Automated Refactoring for Stampedlock”, *IEEE Access* , 7: 104900-104911, 2019.

[18] FMSD Zachary Benavides, Keval Vora, Rajiv Gupta, Xiangyu Zhang, “Annotation guided collection of context-sensitive parallel execution profiles”, *Formal Methods System Design* , 54(3): 388-415, 2019.

[17] JSS Chang-ai Sun, Yufeng Ran, Caiyun Zheng, Huai Liu, Dave Towey, Xiangyu Zhang, “Fault localisation for WS-BPEL programs based on predicate switching and program slicing”, *Journal of Systems and Software* , 135: 191-204, 2018.

[16] C&S Z Gu, B Saltaformaggio, X Zhang, D Xu, “Gemini: Guest-transparent honey files via hypervisor-level access redirection”, *Computers & Security* , 2018.

[15] TDSC W You, B Liang, W Shi, P Wang, X Zhang, “TaintMan: an ART-Compatible Dynamic Taint Analysis Framework on Unmodified and Non-Rooted Android Devices”, *IEEE Transactions on Dependable and Secure Computing*, 2017.

[14] TSE Enyi Tang, Xiangyu Zhang, Norbert Th. Mller, Zhenyu Chen, and Xuandong Li “Software Numerical Instability Detection and Diagnosis by Combining Stochastic and Infinite-precision Testing”, *IEEE Transactions on Software Engineering*, 2017.

[13] FMSD Yunhui Zheng, Vijay Ganesh, Sanu Subramanian, Omer Tripp, Murphy Berzish, Julian Dolby, Xiangyu Zhang, “Z3str2: An Efficient Solver for Strings, Regular Expressions, and Length Constraints”, *Formal Methods in System Design*, 50(2), p249-288, 2017.

[12] SW P. Eugster, V. Sundaram(*), and Xiangyu Zhang, “Debugging the Internet of Things: The Case of Wireless Sensor Networks”, *IEEE Software*, 32(1), p38-49, 2015.

[11] TOSEM Yueqi Li, S.C. Cheung, Xiangyu Zhang, and Yepang Liu, “ Scaling Up Symbolic Analysis by Removing Z-Equivalent States”, *ACM Transactions on Software Engineering and Methodology*, 23(4), p34:1-34:32, 2014.

[10] TOSN V. Sundaram (*), P. Eugster, X. Zhang and V. Addanki, “Diagnostic Tracing for Wireless Sensor Networks”. *ACM Transactions of Sensor Networks*, 9(4), p38:1-38:41, 2013.

[9] TSE W. N. Sumner (*), X. Zhang, D. Weeratunge (*) and X. Zhang, “Precise Calling Context Encoding”, *IEEE Transactions of Software Engineering*, 38(5), p1160-1177, 2012.

[8] SCP A. Navabi(*), X. Zhang, and S. Jagannanthan, “Dependence Analysis for Safe Futures”, *Science of Computer Programming*, 77(6), p707-726, 2012.

[7] TSE Z. Lin(*), X. Zhang, and D. Xu, “Deriving Input Syntactic Structure from Program Execution and Its Applications”, *IEEE Transactions of Software Engineering*,36(5), p688-703, 2010.

[6] TSE C. Liu, X. Zhang, and J. Han, “A Systematic Study of Failure Proximity”, *IEEE Transactions of Software Engineering*, 34(6), p826-843, 2008.

[5] CRC X. Zhang, N. Gupta, and R. Gupta, “Whole Execution Traces and Their Use in Debugging”, *The Compiler Design Handbook: Optimizations and Machine Code Generation*, Second Edition, Chapter 18, CRC Press, 2008.

[4] SP&E X.Zhang, N. Gupta, and R. Gupta, “Locating Faulty Code By Multiple Points Slicing”, *Software - Practice & Experience*, 37(9), p935-961, 2007.

[3] ESE X. Zhang, N. Gupta, and R. Gupta, “A Study of Effectiveness of Dynamic Slicing in Locating Real Faults”, *Empirical Software Engineering*, 2007.

[2] TACO X. Zhang and R. Gupta, “Whole Execution Traces and their Applications”, *ACM Transactions on Architecture and Code Optimization*, 2005.

[1] TOPLAS X. Zhang, R. Gupta, and Y. Zhang, “Cost and Precision Tradeoffs of Dynamic Data Slicing Algorithms”, *ACM Transactions on Programming Languages and Systems*, 2005.

CONFERENCE PUBLICATIONS

[206] SECURITY Qingkai Shi, Xiangzhe Xu, Xiangyu Zhang, “Extracting Protocol Format as State Machine via Controlled Static Loop Analysis ”, in *Proceedings of USENIX Security*, 2023.

[205] SECURITY 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 *Proceedings of USENIX Security*, 2023.

[204] SECURITY Zhuo Zhang, Zhiqiang Lin, Marcelo Morales, Xiangyu Zhang, Kaiyuan Zhang, “Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract ”, in *Proceedings of USENIX Security*, 2023.

[203] SECURITY Guanhong Tao, Shengwei An, Siyuan Cheng, Guangyu Shen, Xiangyu Zhang, “Hard-label Blackbox Universal Adversarial Patch Attack ”, in *Proceedings of USENIX Security*, 2023.

[202] S&P Yapeng Ye, Zhuo Zhang, Qingkai Shi, Yousra Aafer, Xiangyu Zhang, “D-ARM: Disassembling ARM Binaries by Lightweight Superset Instruction Interpretation and Graph Modeling ”, in *Proceedings of S&P*, 2023.

[201] S&P Shengwei An, Yuan Yao, Qiuling Xu, Shiqing Ma, Guanhong Tao, Siyuan Cheng, Kaiyuan Zhang, Yingqi Liu, Guangyu Shen, Ian Kelk, Xiangyu Zhang, “ImU: Physical Impersonating Attack for Face Recognition System with Natural Style Changes ”, in *Proceedings of S&P*, 2023.

[200] FSE 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 FSE*, 2023.

[199] NDSS Siyuan Cheng, Guanhong Tao, Yingqi Liu, Shengwei An, Xiangzhe Xu, Shiwei Feng, Guangyu Shen, Kaiyuan Zhang, Qiuling Xu, Shiqing Ma, Xiangyu Zhang, “BEAGLE: Forensics of Deep Learning Backdoor Attack for Better Defense ”, in *Proceedings of NDSS*, 2023.

[198] ISSTA Jingyao Zhou, Lei Xu, Gongzheng Lu, Weifeng Zhang, Xiangyu Zhang, “INodeRT: Detecting Races in Node.js Applications Practically ”, in *Proceedings of ISSTA*, 2023.

[197] ISSTA 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 ISSTA*, 2023.

[196] ICSE Nan Jiang, Thibaud Lutellier, Yiling Lou, Lin Tan, Dan Goldwasser, Xiangyu Zhang, “KNOD: Domain Knowledge Distilled Tree Decoder for Automated Program Repair ”, in *Proceedings of ICSE*, 2023.

[195] ICSE I Luk Kim, Weihang Wang, Yonghwi Kwon, Xiangyu Zhang, “BFTDETECTOR: Automatic Detection of Business Flow Tampering for Digital Content Service ”, in *Proceedings of ICSE*, 2023.

[194] ICLR Zhiyuan Cheng, James Liang, Guanhong Tao, Dongfang Liu, Xiangyu Zhang, “Adversarial Training of Self-supervised Monocular Depth Estimation against Physical-World Attacks ”, in *Proceedings of the Eleventh International Conference on Learning Representations (ICLR)*, 2023.

[193] ICLR Kaiyuan Zhang, Guanhong Tao, Qiuling Xu, Siyuan Cheng, Shengwei An, Yingqi Liu, Shiwei Feng, Guangyu Shen, Pin-Yu Chen, Shiqing Ma, Xiangyu Zhang, “FLIP: A Provable Defense Framework for Backdoor Mitigation in Federated Learning ”, in *Proceedings of the Eleventh International Conference on Learning Representations (ICLR)*, 2023, also ECCV 2022 Workshop on Adversarial Robustness in the Real World (AROW 2022) **Best Paper Award**.

[192] CVPR Qiuling Xu, Guanhong Tao, Jean Honorio, Yingqi Liu, Shengwei An, Guangyu Shen, Siyuan Cheng, Xiangyu Zhang, “MEDIC: Remove Model Backdoors via Importance Driven Cloning ”, in *Proceedings of CVPR*, 2023.

[191] CVPR Shiwei Feng, Guanhong Tao, Siyuan Cheng, Guangyu Shen, Xiangzhe Xu, Yingqi Liu, Kaiyuan Zhang, Shiqing Ma, Xiangyu Zhang, “Detecting Backdoors in Pre-trained Encoders ”, in *Proceedings of CVPR*, 2023.

[190] CCS Qingkai Shi, Junyang Shao, Yapeng Ye, Mingwei Zheng, Xiangyu Zhang, “Lifting Network Protocol Implementation to Precise Format Specification with Security Applications ”, in *Proceedings of CCS*, 2023.

[189] ACL Weisong Sun, Yuchen Chen, Guanhong Tao, Chunrong Fang, Xiangyu Zhang, Quanjun Zhang, Bin Luo, “Backdooring Neural Code Search ”, in *Proceedings of ACL*, 2023.

[188] SECURITY Fei Wang, Jianliang Wu, Yuhong Nan, Yousra Aafer, Xiangyu Zhang, Dongyan Xu, Mathias Payer, “ProFactory: Improving IoT Security via Formalized Protocol Customization ”, in *Proceedings of USENIX Security*, 2022.

[187] S&P Yingqi Liu, Guangyu Shen, Guanhong Tao, Shengwei An, Shiqing Ma, Xiangyu Zhang, “PICCOLO: Exposing Complex Backdoors in NLP Transformer Models ”, in *Proceedings of S&P*, 2022.

[186] S&P 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 *Proceedings of S&P*, 2022.

[185] FSE Guanhong Tao, Weisong Sun, Tingxu Han, Chunrong Fang, Xiangyu Zhang, “RULER: discriminative and iterative adversarial training for deep neural network fairness ”, in *Proceedings of FSE*, 2022.

[184] NDSS Shengwei An, Guanhong Tao, Qiuling Xu, Yingqi Liu, Guangyu Shen, Jingwei Xu, Xiangyu Zhang, Yuan Yao, “MIRROR: Model Inversion for Deep LearningNetwork with High Fidelity ”, in *Proceedings of NDSS*, 2022.

[183] NDSS Hongjun Choi, Zhiyuan Cheng, Xiangyu Zhang, “RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning ”, in *Proceedings of NDSS*, 2022.

[182] ASE Max Taylor, Johnathon Aurand, Feng Qin, Xiaorui Wang, Brandon Henry, Xiangyu Zhang, “SA4U: Practical Static Analysis for Unit Type Error Detection ”, in *Proceedings of ASE*, 2022.

[181] ISSTA Xuwei Liu, Wei You, Zhuo Zhang, Xiangyu Zhang, “TensileFuzz: facilitating seed input generation in fuzzing via string constraint solving ”, in *Proceedings of ISSTA*, 2022.

[180] ISSTA Danning Xie, Yitong Li, Mijung Kim, Hung Viet Pham, Lin Tan, Xiangyu Zhang, Michael W. Godfrey, “DocTer: documentation-guided fuzzing for testing deep learning API functions ”, in *Proceedings of ISSTA*, 2022.

[179] IJCAI Liqi Yan, Qifan Wang, Yiming Cui, Fuli Feng, Xiaojun Quan, Xiangyu Zhang, Dongfang Liu, “GL-RG: Global-Local Representation Granularity for Video Captioning ”, in *Proceedings of IJCAI*, 2022.

[178] ICML 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 *Proceedings of ICML*, 2022.

[177] ECCV Zhiyuan Cheng, James Liang, Hongjun Choi, Guanhong Tao, Zhiwen Cao, Dongfang Liu, Xiangyu Zhang, “Physical Attack on Monocular Depth Estimation with Optimal Adversarial Patches ”, in *Proceedings of ECCV*, 2022.

[176] CVPR Qiuling Xu, Guanhong Tao, Xiangyu Zhang, “Bounded Adversarial Attack on Deep Content Features ”, in *Proceedings of CVPR*, 2022.

[175] CVPR Guanhong Tao, Guangyu Shen, Yingqi Liu, Shengwei An, Qiuling Xu, Shiqing Ma, Pan Li, Xiangyu Zhang , “Better Trigger Inversion Optimization in Backdoor Scanning ”, in *Proceedings of CVPR* (oral), 2022.

[174] CVPR Yingqi Liu, Guangyu Shen, Guanhong Tao, Zhenting Wang, Shiqing Ma, Xiangyu Zhang, “Complex Backdoor Detection by Symmetric Feature Differencing ”, in *Proceedings of CVPR*, 2022.

[173] CCS Muslum Ozgur Ozmen, Xuansong Li, Andrew Chu, Z. Berkay Celik, Bardh Hoxha, Xiangyu Zhang, , “Discovering IoT Physical Channel Vulnerabilities ”, in *Proceedings of CCS*, 2022.

[172] CAIN Xiangzhe Xu, Hongyu Liu, Guanhong Tao, Zhou Xuan, Xiangyu Zhang , “Checkpointing and deterministic training for deep learning ”, in *Proceedings of the 1st International Conference on AI Engineering: Software Engineering for AI*, 2022.

[171] FSE Ming Yan, Junjie Chen, Xiangyu Zhang, Lin Tan, Gan Wang, Zan Wang , “Exposing numerical bugs in deep learning via gradient back-propagation ”, in *Proceedings of Foundations of Software Engineering*, 2021.

[170] FSE Sayali Kate, Michael Chinn, Hongjun Choi, Xiangyu Zhang, Sebastian G. Elbaum , “PHYSFRAME: type checking physical frames of reference for robotic systems ”, in *Proceedings of Foundations of Software Engineering*, 2021.

[169] ICML Guangyu Shen, Yingqi Liu, Guanhong Tao, Shengwei An, Qiuling Xu, Siyuan Cheng, Shiqing Ma, Xiangyu Zhang, , “Backdoor Scanning for Deep Neural Networks through K-Arm Optimization ”, in *Proceedings of ICML*, 2021.

[168] ICSE Xincheng He, Lei Xu, Xiangyu Zhang, Rui Hao, Yang Feng, Baowen Xu , “PyART: Python API Recommendation in Real-Time ”, in *Proceedings of the International Conference on Software Engineering*, 2021.

[167] AAAI Siyuan Cheng, Yingqi Liu, Shiqing Ma, Xiangyu Zhang, “Deep Feature Space Trojan Attack of Neural Networks by Controlled Detoxification”, in *Proceedings of the 35th AAAI Conference on Artificial Intelligence*, 2021.

[166] AAAI Qiuling Xu , Guanhong Tao , Siyuan Cheng and Xiangyu Zhang, “Towards Feature Space Adversarial Attack”, in *Proceedings of the 35th AAAI Conference on Artificial Intelligence*, 2021.

[165] SECURITY Abdulellah Alsaheel, Yuhong Nan, Shiqing Ma, Le Yu, Greg Walkup, Celik Berkay, Xiangyu Zhang, Dongyan Xu, “ATLAS: A Sequence-based Learning Approach for Attack Investigation”, in *the 30th USENIX Security Symposium*, 2021.

[164] SECURITY Y. Aafer, W. You, Y. Sun, Y. Shi, X. Zhang, and H. Yin, “Android SmartTVs Vulnerability Discovery via Log-Guided Fuzzing”, in *the 30th USENIX Security Symposium*, 2021.

[163] S&P 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 *Proceedings of the 42th IEEE Symposiums on Security and Privacy*, 2021.

[162] S&P 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 *Proceedings of the 42th IEEE Symposiums on Security and Privacy*, 2021.

[161] NDSS Yapeng Ye, Zhuo Zhang, Fei Wang, Xiangyu Zhang, Dongyan Xu, “NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces”, in *Proceedings of the 28th Network and Distributed System Security Symposium*, 2021.

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

[159] OOPSLA Hongyu Liu, Sam Silvestro, Xiangyu Zhang, Jian Huang, Tongping Liu, “WATCHER: In-Situ Failure Diagnosis”, in *Proceedings of Object Oriented Programming, Systems, Languages and Applications*, 2020.

[158] FSE Juan Zhai, Yu Shi, Minxue Pan, Guian Zhou, Yongxiang Liu, Chunrong Fang, Shiqing Ma, Lin Tan, Xiangyu Zhang, “C2S: translating natural language comments to formal program specifications”, in *Proceedings of the 2020 ACM SIGSOFT International Symposium on the Foundations of Software Engineering*, 2020.

[157] FSE Shenao Yan, Guanhong Tao, Xuwei Liu, Juan Zhai, Shiqing Ma, Lei Xu, Xiangyu Zhang, “Correlations Between Deep Neural Network Model Coverage Criteria and Model Quality”, in *Proceedings of the 2020 ACM SIGSOFT International Symposium on the Foundations of Software Engineering*, 2020.

[156] SECURITY Taegyu Kim, Chung Hwan Kim, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dongyan Xu, Dave (Jing) Tian, “From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with Mayday”, in *The 29th USENIX Security Symposium*, 2020 (conditional accept).

[155] CCS : Junyu Lin, Lei Xu, Yingqi Liu, Xiangyu Zhang, “Composite Backdoor Attack for Deep Neural Network by Mixing Existing Benign Features ”, in *Proceedings of the 27th ACM Conference on Computer and Communications Security*, 2020.

[154] CCS Hongjun Choi, Saylai Kate, Yousra Aafer, Xiangyu Zhang, Dongyan Xu, “Cyber-Physical Inconsistency Vulnerability Idnetification for Safety Checks in Robotic Vehicles”, in *Proceedings of the 27th ACM Conference on Computer and Communications Security*, 2020.

[153] NDSS Runqing Yang, Shiqing Ma, Haitao Xu, Xiangyu Zhang, Yan Chen, “UISCOPE: Accurate, Instrumentation-free and Visible Attack Investigation for GUI Applications”, in *Proceedings of the 27th Network and Distributed System Security Symposium*, 2020.

[152] ICSE Hao Xia, Yuan Zhang, Yingtian Zhou, Xiaoting Chen, Yang Wang, Xiangyu Zhang, Shuaishuai Cui, Geng Hong, Xiaohan Zhang, Min Yang, Zhemin Yang, “How Android Developers Handle Evolution-induced API Compatibility Issues: A Large-scale Study ”, in *Proceedings of the International Conference on Software Engineering*, 2020.

[151] ICSE Guanhong Tao, Shiqing Ma, Yingqi Liu, Qiuling Xu, Xiangyu Zhang, “TRADER: Trace Divergence Analysis and Embedding Regulation for Debugging Recurrent Neural Networks”, in *Proceedings of the International Conference on Software Engineering*, 2020.

[150] ICSE Juan Zhai, Xiangzhe Xu, Yu Shi, Guanhong Tao, Minxue Pan, Shiqing Ma, Lei Xu, Weifeng Zhang, Lin Tan, Xiangyu Zhang, “CPC: Automatically Classifying and Propagating Natural Language Comments via Program Analysis ”, in *Proceedings of the International Conference on Software Engineering*, 2020.

[149] ICSE Wanwangying Ma, Lin Chen, Xiangyu Zhang, Yang Feng, Zhaogui Xu, Zhifei Chen, Yuming Zhou, Baowen Xu, “Impact Analysis of Cross-Project Bugs on Software Ecosystems”, in *Proceedings of the International Conference on Software Engineering*, 2020.

[148] ICSE I Luk Kim, Yunhui Zheng, Hogun Park, Weihang Wang, Wei You, Yousra Aafer, Xiangyu Zhang, “Finding Client-side Business Flow Tampering Vulnerabilities”, in *Proceedings of the International Conference on Software Engineering*, 2020.

[147] S&P Wei You, Zhuo Zhang, Yonghwi Kwon, Yousra Aafer, Fei Peng, Yu Shi, Carson Makena Harmon, Xiangyu Zhang, “PMP: Cost-Effective Forced Execution with Probabilistic Memory Pre-Planning”, in *Proceedings of the 41th IEEE Symposiums on Security and Privacy*, 2020.

[146] CCS Yingqi Liu, Wen-Chuan Lee, Guanhong Tao, Shiqing Ma, Yousra Aafer, Xiangyu Zhang, “ABS: Scanning Neural Networks for Back-doors by Artificial Brain Stimulation”, in *Proceedings of the 26th ACM Conference on Computer and Communications Security*, 2019.

[145] OOPSLA 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 Object Oriented Programming, Systems, Languages and Applications*, 2019 (**ACM SIGPLAN Distinguished Paper Award**).

[144] SECURITY T Kim, C. H. Kim, F. Fei, Z. Tu, G. Walkup, X. Zhang, X. Deng, D. Xu, “RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing”, in *USENIX Security* , 2019.

[143] PLDI David M. Perry, Dohyeong Kim, Roopsha Samanta, and Xiangyu Zhang, “SemCluster: Clustering of Imperative Programming Assignments Based on Quantitative”, in *Proceedings of ACM SIGPLAN Conference on Programming Languages Design and Implementation*, 2019.

[142] PLDI Wen-Chuan Lee, Peng Liu, Yingqi Liu, Shiqing Ma, and Xiangyu Zhang, “Programming Support for Autonomizing Software”, in *Proceedings of ACM SIGPLAN Conference on Programming Languages Design and Implementation*, 2019.

[141] ICSE Wei You, Xuwei Liu, Shiqing Ma, David Perry, Xiangyu Zhang, Bin Liang, “SLF: Fuzzing without Valid Seed Inputs”, in *Proceedings of the 41st ACM/IEEE Internatinoal Conference on Software Engineering (ICSE)*, 2019.

[140] ICSE Kenneth Miller, Yonghwi Kwon, Xiangyu Zhang, Zhiqiang Lin, “Probabilistic Disassembly”, in *Proceedings of the 41st ACM/IEEE Internatinoal Conference on Software Engineering (ICSE)*, 2019.

[139] S&P Wei You, Xueqiang Wang, Shiqing Ma, Jianjun Huang, Xiangyu Zhang, XiaoFeng Wang, Bin Liang, “ProFuzzer: On-the-fly Input Type Probing for Better Zero-day Vulnerability Discovery”, in *Proceedings of the 40th IEEE Symposiums on Security and Privacy (Oakland)*, 2019.

[138] NDSS Shiqing Ma, Yingqi Liu, Guanhong Tao, Wen-Chuan Lee, Xiangyu Zhang, ,“NIC: Detecting Adversarial Samples with Neural Network Invariant Checking ”, in *Proceedings of the 26th Network and Distributed System Security Symposium*, 2019.

[137] CGO Wen-Chuan Lee, Yingqi Liu, Peng Liu, Shiqing Ma, Hongjun Choi, Xiangyu Zhang, Rajiv Gupta, ,“White-Box Program Tuning ”, in *Proceedings of the International Symposium on Code Generation and Optimization*, 2019.

[136] NIPS G Tao, S Ma, Y Liu, X Zhang, ,“Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples ”, in *Advances in Neural Information Processing Systems*, 2018.

[135] ACSAC F Wang, Y Kwon, S Ma, X Zhang, D Xu, ,“Lprov: Practical Library-aware Provenance Tracing ”, in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2018.

[134] FSE Shiqing Ma, Yingqi Liu, Wen-Chuan Lee, Xiangyu Zhang, Ananth Grama, ,“MODE: automated neural network model debugging via state differential analysis and input selection”, in *Proceedings of the Foundations of Software Engineering*, 2018.

[133] FSE Sayali Kate, John-Paul Ore, Xiangyu Zhang, Sebastian G. Elbaum, Zhaogui Xu, ,“Phys: probabilistic physical unit assignment and inconsistency detection”, in *Proceedings of the Foundations of Software Engineering*, 2018.

[132] CCS Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, Xinyan Deng, ,“Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach”, in *Proceedings of the ACM Conference on Computer and Communications Security*, 2018.

[131] CCS Yousra Aafer, Guanhong Tao, Jianjun Huang, Xiangyu Zhang, Ninghui Li, ,“Precise Android API Protection Mapping Derivation and Reasoning”, in *Proceedings of the ACM Conference on Computer and Communications Security*, 2018.

[130] WWW IL Kim, W Wang, Y Kwon, Y Zheng, Y Aafer, W Meng, X Zhang, ,“AdBudgetKiller: Online Advertising Budget Draining Attack”, in *Proceedings of the 2018 World Wide Web Conference*, 2018.

[129] ATC S Ma, J Zhai, Y Kwon, KH Lee, X Zhang, G Ciocarlie, A Gehani, Vinod Yegneswaran, Dongyan Xu, Somesh Jha, “Kernel-Supported Cost-Effective Audit Logging for Causality Tracking”, in *Proceedings of the USENIX Annual Technical Conference*, 2018.

[128] ASE Z Tang, J Zhai, M Pan, Y Aafer, S Ma, X Zhang, J Zhao, “Dual-force: understanding WebView malware via cross-language forced execution”, in *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, 2018.

[127] ICSE Z Xu, S Ma, X Zhang, S Zhu, B Xu, “Debugging with intelligence via probabilistic inference”, in *Proceedings of the 40th International Conference on Software Engineering*, 2018.

[126] COMPSAC C Sun, J Jia, H Liu, X Zhang, “A Lightweight Program Dependence Based Approach to Concurrent Mutation Analysis”, in *Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference*, 2018.

[125] ICRA Fan Fei, Zhan Tu, Ruikun Yu, Taegyu Kim, Xiangyu Zhang, Dongyan Xu, Xinyan Deng, “Cross-Layer Retrofitting of UAVs Against Cybe r-Physical Attacks”, in *Proceedings of the IEEE International Conference on Robotics and Automation*, 2018.

[124] NDSS Yonghwi Kwon, Fei Wang, Weihang Wang, Kyu Hyung Lee, Wen-Chuan Lee, Shiqing Ma, Xiangyu Zhang, Dongyan Xu, Somesh Jha, Gabriela F. Ciocarlie, Ashish Gehani, Vinod Yegneswaran, ,“MCI : Modeling-based Causality Inference in Audit Logging for Attack Investigation ”, in *Proceedings of NDSS*, 2018.

[123] NDSS Rohit Bhatia, Brendan Saltaformaggio, Seung Jei Yang, Aisha I. Ali-Gombe, Xiangyu Zhang, Dongyan Xu, Golden G. Richard III, ,“Tipped Off by Your Memory Allocator: Device-Wide User Activity Sequencing from Android Memory Images ”, in *Proceedings of NDSS*, 2018.

[122] NDSS Yousra Aafer, Jianjun Huang, Yi Sun, Xiangyu Zhang, Ninghui Li, Chen Tian, ,“AceDroid: Normalizing Diverse Android Access Control Checks for Inconsistency Detection ”, in *Proceedings of NDSS*, 2018.

[121] NDSS CH Kim, T Kim, H Choi, Z Gu, B Lee, X Zhang, D Xu, ,“Securing real-time microcontroller systems through customized memory view switching ”, in *Proceedings of NDSS*, 2018.

[120] NDSS Y Liu, S Ma, Y Aafer, WC Lee, J Zhai, W Wang, X Zhang, “Trojaning attack on neural networks”, in *Proceedings of NDSS* , 2018.

[119] ACSAC H Chen, N Li, W Enck, Y Aafer, X Zhang, ,“Analysis of SEAndroid Policies: Combining MAC and DAC in Android ”, in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017.

[118] ACSAC Taegyu Kim, Chung Hwan Kim, Hongjun Choi, Yonghwi Kwon, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu ,“RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications”, in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017.

[117] ASE W Wang, Y Kwon, Y Zheng, Y Aafer, I Kim, WC Lee, Y Liu, W Meng,“PAD: Programming third-party web advertisement censorship”, in *Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering*, 2017.

[116] ASE J Huang, Y Aafer, D Perry, X Zhang, C Tian,“UI driven Android application reduction”, in *Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering*, 2017.

[115] SECCOMM Chonghua Wang, Shiqing Ma, Xiangyu Zhang, Junghwan Rhee, Xiaochun Yun, Zhiyu Hao,“A Hypervisor Level Provenance System to Reconstruct Attack Story Caused by Kernel Malware”, in *Proceedings of International Conference on Security and Privacy in Communication Systems*, 2017.

[114] FSE S Ma, Y Aafer, Z Xu, WC Lee, J Zhai, Y Liu, X Zhang,“LAMP: data provenance for graph based machine learning algorithms through derivative computation”, in *Proceedings of Foundations of Software Engineering*, 2017.

[113] SECURITY S Ma, J Zhai, F Wang, KH Lee, X Zhang, D Xu, “MPI: Multiple perspective attack investigation with semantics aware execution partitioning”, in *Proceedings of USENIX Security*, 2017 (**Distinguished Paper Award**).

[112] ISSTA Y Kwon, W Wang, Y Zheng, X Zhang, D Xu, “CPR: cross platform binary code reuse via platform independent trace program”, in *Proceedings of the 26th ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2017.

[111] ISSTA DM Perry, A Mattavelli, X Zhang, C Cadar, “Accelerating array constraints in symbolic execution”, in *Proceedings of the 26th ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2017.

[110] ICSE P Liu, X Zhang, M Pistoia, Y Zheng, M Marques, L Zeng, “Automatic text input generation for mobile testing”, in *Proceedings of the 26th International Conference on IEEE/ACM 39th International Conference on Software Engineering*, 2017.

[109] ICSE W Ma, L Chen, X Zhang, Y Zhou, B Xu, “How Do Developers Fix Cross-Project Correlated Bugs? A Case Study on the GitHub Scientific Python Ecosystem”, in *Proceedings of the 26th International Conference on IEEE/ACM 39th International Conference on Software Engineering*, 2017.

[108] WWW K Kim, IL Kim, CH Kim, Y Kwon, Y Zheng, X Zhang, D Xu, “J-force: Forced execution on javascript”, in *Proceedings of the 26th International Conference on World Wide Web* , 2017.

[107] RV Zachary Benavides, Rajiv Gupta, Xiangyu Zhang, “Annotation Guided Collection of Context-Sensitive Parallel Execution Profiles”, in *Proceedings of Runtime Verification* , 2017.

[106] NDSS Y Kwon, B Saltaformaggio, IL Kim, KH Lee, X Zhang, D Xu, “A2c: Self destructing exploit executions via input perturbation”, in *Proceedings of NDSS* , 2017.

[105] ACSAC Kexin Pei, Zhongshu Gu, Brendan Saltaformaggio, Shiqing Ma, Fei Wang, Zhiwei Zhang, Luo Si, Xiangyu Zhang, Dongyan Xu, “Hercule: Attack story reconstruction via community discovery on correlated log graph ”, in *Proceedings of the 32Nd Annual Conference on Computer Security Applications* , 2016.

[104] OOPSLA Dohyeong Kim, Yonghwi Kwon, Peng Liu, I Luk Kim, David Mitchel Perry, Xiangyu Zhang, Gustavo Rodriguez-Rivera, “Apex: automatic programming assignment error explanation”, in *Proceedings of Object Oriented Programming, Systems, Languages and Applications*, 2016.

[103] HPDC Zachary Benavides, Rajiv Gupta, Xiangyu Zhang, “Parallel execution profiles”, in *Proceedings of the 25th ACM International Symposium on High-Performance Parallel and Distributed Computing*, 2016.

[102] WOOT Brendan Saltaformaggio, Hongjun Choi, Kristen Johnson, Yonghwi Kwon, Qi Zhang, Xiangyu Zhang, Dongyan Xu, John Qian, “Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic”, in *WOOT* , 2016.

[101] IST Chang-ai Sun, Feifei Xue, Huai Liu, Xiangyu Zhang, “A path-aware approach to mutant reduction in mutation testing”, in *Information and Software Technology* , 2016.

[100] FSE Chung Hwan Kim, Junghwan Rhee, Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu, “PerfGuard: Binary-Centric Application Performance Monitoring in Production Environments”, in *Proceedings of the 2016 ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2016.

[99] FSE Weihang Wang, Yunhui Zheng, Xinyu Xing, Xiangyu Zhang, Patrick Eugster, “WebRanz: Web Page Randomization For Better Advertisement Delivery and Web-Bot Prevention”, in *Proceedings of the 2016 ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2016.

[98] FSE Jianjun Huang, Xiangyu Zhang, Lin Tan, “Detecting Sensitive Data Disclosure via Bi-directional Text Correlation Analysis”, in *Proceedings of the 2016 ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2016 (**ACM SIGSOFT Distinguished Paper Award**).

[97] FSE Zhaogui Xu, Xiangyu Zhang, Lin Chen, Kexin Pei, Baowen Xu, “Python Probabilistic Type Inference with Natural Language Support”, in *Proceedings of the 2016 ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2016 (**Distinguished Artifact Award**).

[96] FSE Zhaogui Xu, Peng Liu, Xiangyu Zhang, Baowen Xu, “Python Predictive Analysis for Bug Detection”, in *Proceedings of the 2016 ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2016.

[95] ISSTA Peng Liu, Omer Tripp, Xiangyu Zhang, “IPA: Improving Predictive Analysis with Pointer Analysis”, in *Proceedings of the 2016 ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2016.

[94] ISSTA Weihang Wang, Yunhui Zheng, Peng Liu, Lei Xu, Xiangyu Zhang, Patrick Eugster, “ARROW: Automated Repair of Races on Client-Side Web Pages”, in *Proceedings of the 2016 ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2016.

[93] ICSE Hao Sun, Xiangyu Zhang, Yunhui Zheng, Qingkai Zeng, “IntEQ: Recognizing Benign Integer Overflows via Equivalence Checking Across Multiple Precisions”, in *Proceedings of the International Conference on Software Engineering*, 2016.

[92] ICSE Wei You, Bin Liang, Wenchang Shi, Shuyang Zhu, Peng Wang, Sikefu Xie, Xiangyu Zhang, “Reference Hijacking: Patching, Protecting and Analyzing on Unmodified and Non-Rooted Android Devices ”, in *Proceedings of the International Conference on Software Engineering*, 2016.

[91] ICSE Juan Zhai, Jianjun Huang, Shiqing Ma, Xiangyu Zhang, Lin Tan, Jianhua Zhao, Feng Qin, “Automatic Model Generation from Documentation for Java API Functions”, in *Proceedings of the International Conference on Software Engineering*, 2016.

[90] ASPLOS Yonghwi Kwon, Dohyeong Kim, William Nick Sumner, Kyungtae Kim, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu, “LDX: Causality Inference by Lightweight Dual Execution”, in *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems*, 2016.

[89] NDSS Shiqing Ma, Xiangyu Zhang, Dongyan Xu, “ProTracer: Towards Practical Provenance Tracing by Alternating Between Logging and Tainting ”, in *Proceedings of NDSS*, 2015 **Distinguished Paper**.

[88] ACSAC Shiqing Ma, K.H. Lee, C.H. Kim, J. Rhee, X. Zhang, D. Xu, “Accurate, Low Cost and Instrumentation-Free Security Audit Logging for Windows”, in *Proceedings of the 31st Annual Computer Security Applications Conference*, 2015.

[87] CCS Zhui Deng(*), Brendan Saltaformaggio(*), Xiangyu Zhang, Dongyan Xu, “iRiS: Vetting Private API Abuse in iOS Applications”, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015 **Contributed to the confirmation and removal of hundreds of privacy-violating apps from Apple’s App Store**.

[86] CCS Brendan Saltaformaggio (*), Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, Dongyan Xu, “GUITAR: Piecing together android app GUIs from memory images”, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015 **Best Paper Award**.

[85] CCS Brendan Saltaformaggio (*), Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, Dongyan Xu,, “VCR: App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images ”, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[84] OOPSLA W. Lee (*), T. Bao(*), Y. Zheng(*), X. Zhang, K. Vora, R. Gupta, “RAIVE: Runtime Assessment of Floating-Point Instability by Vectorization”, in *Proceedings of Object Oriented Programming, Systems, Languages and Applications*, 15 pages, 2015.

[83] CAV Yunhui Zheng(*), Vijay Ganesh, Sanu Subramanian, Omer Tripp, Julian Dolby, Xiangyu Zhang, “Effective Search-space Pruning for Solvers of String Equations, Regular Expressions and Length Constraints”, in *Proceedings of the 27th International Conference on Computer Aided Verification*, 12 pages, 2015.

[82] SECURITY Jianjun Huang(*), Zhichun Li, Xusheng Xiao, Zhenyu Wu, Kangjie Lu, Xiangyu Zhang, Guofei Jiang, “Detect Sensitive User Input from Massive Android Apps”, in *Proceedings of USENIX Security*, 12 pages, 2015, **CSAW 2015 Best Applied Security Paper Award TOP-10 Finalists**.

[81] PLDI Peng Liu(*), Xiangyu Zhang, Omer Tripp, Yunhui Zheng(*), “Light: Replay via Tightly Bounded Recording”, in *Proceedings of Programming Language Design and Implementation*, 12 pages, 2015.

[80] DSN Zhongshu Gu(*), Kexin Pei(*), Qifan Wang(*), Luo Si, Xiangyu Zhang, Dongyan Xu, “Detecting Camouflaged Attacks with Statistical Learning Guided by Program Analysis”, in *Proceedings of the 45th IEEE/IFIP International Conference on Dependable Systems and Networks*, 12 pages, 2015.

[79] ASPLOS Dohyeong Kim(*), Yonghwi Kwon(*), William N. Sumner, Xiangyu Zhang, Dongyan Xu, “Dual Execution for On the Fly Fine Grained Execution Comparison”, in *Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems*, p325-338, 2015.

[78]ASIACCS Hao Sun(*), Xiangyu Zhang, Chao Su, Qingkai Zeng, “Efficient Dynamic Tracking Technique for Detecting Integer-Overflow-to-Buffer-Overflow Vulnerability”, in *Proceedings of ACM Symposium on Information, Computer and Communications Security*, p483-494, 2015.

[77]ASIACCS Wei You, Bin Liang, Jingzhe Li, Wenchang Shi, Xiangyu Zhang, “Android Implicit Information Flow Demystified”, in *Proceedings of ACM Symposium on Information, Computer and Communications Security*, p585-590, 2015.

[76] NDSS Yonghwi Kwon(*), Fei Peng(*), Dohyeong Kim(*), Kyungtae Kim(*), Xiangyu Zhang, Dongyan Xu, Vinod Yegneswaran, John Qian, “P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions”, in *Proceedings of the ISOC Network and Distributed System Security Symposium*, 12pages, 2015.

[75] OOPSLA Peng Liu(*), Omer Tripp, Xiangyu Zhang, “Flint: Fixing Linearizability Violations”, in *Proceedings of Object Oriented Programming, Systems, Languages and Applications*, p543-560, 2014.

[74] SECURITY Brendan Saltaformaggio(*), Zhongshu Gu, Xiangyu Zhang, Dongyan Xu, “DESCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse”, in *Proceedings of USENIX Security*, p255-269 **Recipient of the Best Student Paper**, 2014.

[73] SECURITY Fei Peng(*), Zhui Deng(*), Xiangyu Zhang, Dongyan Xu, Zhiqiang Lin, Zhendong Su, “X-Force: Force-Executing Binary Programs for Security Applications ”, in *Proceedings of USENIX Security*, p829-844, 2014.

[72] ECOOP Kyu Hyung Lee(*), Dohyeong Kim(*) and Xiangyu Zhang, “Infrastructure-Free Logging and Replay of Concurrent Execution on Multiple Cores”, in *Proceedings of European Conference on Object-Oriented Programming*, p232-256, 2014.

[71] ISSTA Yunxiao Zou(*), Zhenyu Chen, Yunhui Zheng(*), Xiangyu Zhang, and Zebao Gao, “Virtual DOM Coverage: Drive an Effective Testing for Dynamic Web Applications”, in *Proceedings of International Symposium on Software Testing and Analysis*, p60-70, 2014.

[70] DSN Zhongshu Gu(*), Brendan Saltaformaggio(*), Xiangyu Zhang, Dongyan Xu, “FACE-CHANGE: Application-Driven Dynamic Kernel View Switching in a Virtual Machine”, in *Proceedings of the 44th IEEE/IFIP International Conference on Dependable Systems and Networks*, p491-502, 2014.

[69] SIGMETRICS Chung Hwan Kim (*), Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, Xiangyu Zhang, Dongyan Xu, “IntroPerf: Transparent Context-Sensitive Multi-Layer Performance Inference using System Stack Traces”, in *Proceedings of ACM SIGMETRICS*, p235-247, 2014.

[68] ICSE Dohyeong Kim(*), William N. Sumner(*), Xiangyu Zhang, Dongyan Xu, Hira Agrawal, “Reuse-Oriented Reverse Engineering of Functional Components from X86 Binaries ”, in *Proceedings of the 36th International Conference on Software Engineering*, p1128-1139, 2014.

[67] ICSE Jianjun Huang(*), Xiangyu Zhang, Lin Tan, Peng Wang, Bin Liang, “AsDroid: Detecting Stealthy Behaviors in Android Applications by User Interface and Program Behavior Contradiction ”, in *Proceedings of the 36th International Conference on Software Engineering*, p1036-1046, 2014.

[66] OOPSLA T. Bao(*), X. Zhang, “On-the-fly Detection of Instability Problems in Floating-Point Program Execution”, in *Object Oriented Programming, Systems, Languages and Applications*, p817-832, 2013.

[65] ACSAC Z. Deng(*), X. Zhang, D. Xu, “SPIDER: Stealthy Binary Program Instrumentation and Debugging via Hardware Virtualization,” *Proceedings of the Annual Computer Security Applications Conference*, p289-298, 2013.

[64] ASE W. N. Sumner(*), X. Zhang, “Identifying Execution Points For Dynamic Analyses, ” *Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering*, p81-91, 2013.

[63] ASE Y. Kwon(*), X. Zhang, D. Xu, “PIEtrace: Platform Independent Executable Trace,” *Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering*, **Recipient of ACM SIGSOFT Distinguished Paper Award and Best Paper Award**, p48-58, 2013.

[62] CCS J. Zeng, Y. Fu, K. Miller, Z. Lin, X. Zhang, D. Xu, “Obfuscation Resilient Binary Code Reuse through Trace-oriented Programming,” *Proceedings of the 20th ACM Conference on Computer and Communications Security* , p487-498, 2013.

[61] CCS K. H. Lee(*), X. Zhang, D. Xu, “LogGC: Garbage Collecting Audit Log,” *Proceedings of the 20th ACM Conference on Computer and Communications Security* , p1005-1016, 2013.

[60] ESORICS Z. Deng(*), X. Zhang, D. Xu, “BISTRO: Binary Component Extraction and Embedding for Software Security Applications,” *Proceedings of the 18th European Symposium on Research in Computer Security*, p200-218, 2013.

[59] FSE Y. Zheng(*), X. Zhang, V. Ganesh, “Z3-str: A Z3-Based String Solver for Web Application Analysis,”, in *the 9th joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering*, p114-124, 2013.

[58] DSN-PDS Z. Gu(*), W. N. Sumner(*), Z. Deng(*), X. Zhang, D. Xu, “DRIP: A Framework for Purifying Trojaned Kernel Drivers,” *the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks*, p1-12, 2013.

[57] EuroSec B. Saltaformaggio(*), D. Xu, X. Zhang, “BusMonitor: A Hypervisor-Based Solution for Memory Bus Covert Channels,” *the 6th European Workshop on Systems Security*, 5 pages, 2013.

[56] ICSE Y. Zheng(*), X. Zhang, “Path Sensitive Static Analysis of Web Applications for Remote Code Execution Vulnerability Detection,” *the 35th International Conference on Software Engineering*, p652-661, 2013.

[55] ICSE W. N. Sumner(*), X. Zhang, “Comparative Causality: Explaining the Differences Between Executions,” *the 35th International Conference on Software Engineering*, p272-281, 2013.

[54] NDSS K. H. Lee(*), X. Zhang, D. Xu, “High Accuracy Attack Provenance via Binary-based Execution Partition,” *the 20th Network and Distributed System Security Symposium*, 12 pages, 2013.

[53] WCRE D. Qi(*), W. N. Sumner(*), F. Qin, M. Zheng, X. Zhang and A. Roychoudhury, “Modeling Software Execution Environment”, in *the 19th Working Conference on Reverse Engineering*, p415-424, 2012.

[52] SenSys V. Sundaram(*), P. Eugster, and Xiangyu Zhang, “Prius: Generic Hybrid Trace Compression for Wireless Sensor Networks”, in *the 10th ACM International Conference on Embedded Networked Sensor Systems*, p183-196, 2012.

[51] OOPSLA T. Bao(*), Y. Zheng(*), and X. Zhang, “White Box Sampling in Uncertain Data Processing Enabled by Program Analysis”, in *Object Oriented Programming, Systems, Languages and Applications*, p897-914, 2012.

[50] DFRWS Z. Deng(*), D. Xu, X. Zhang, and X. Jiang, “IntroLib: Efficient and Transparent Library Call Introspection for Malware Forensics”, *the 12th Annual DFRWS Digital Forensics Conference*, 10 pages, 2012.

[49] ICSE Y. Zheng(*) and X. Zhang, "Static Detection of Resource Contention Problems in Server-Side Scripts", *the 34th International Conference on Software Engineering*, p652-661, 2012.

[48]ESoSS R. Potharaju, A. Newell, C. Nita-Rotaru, and X. Zhang, "Plagiarizing Smartphone Applications: Attack Strategies and Defense Techniques", *International Symposium on Engineering Secure Software and Systems*, p106-120, 2012.

[47] NDSS Z. Lin(*), J. Rhee, C. Wu, X. Zhang, and Dongyan Xu, "DIMSUM: Discovering Semantic Data of Interest from Un-mappable Memory with Confidence", *the 19th ISOC Network and Distributed System Security Symposium*, 12 pages, 2012.

[46] OOPSLA D. Weeratunge(*), X. Zhang, and S. Jagannathan, "Accentuating the Positive: Atomicity Inference and Enforcement Using Correct Executions", in *Object Oriented Programming, Systems, Languages and Applications*, p19-34, 2011.

[45] ISSTA W. N. Sumner(*) and X. Zhang, "Selecting Peers for Execution Comparison", *International Symposium on Software Testing and Analysis*, p309-319, 2011.

[44] DSN K. Lee(*), W. N. Sumner(*), P. Eugster and X. Zhang, "Unified Debugging of Distributed Systems with Recon", *the 41th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, p85-96, 2011.

[43] PLDI K. Lee(*), Y. Zheng(*), W. N. Sumner(*) and X. Zhang, "Toward Generating Reducible Replay Log", *ACM SIGPLAN Conference on Programming Language Design and Implementation*, p246-257, 2011.

[42] WWW Y. Zheng(*), T. Bao(*) and X. Zhang, "Statically Locating Web Application Bugs Caused by Asynchronous Calls", *The 20th International World Wide Web Conference*, p805-814, 2011.

[41] ICSE W. N. Sumer(*), T. Bao(*), X. Zhang, and S. Prabhakar, "Coalescing Executions for Fast Uncertainty Analysis", *the International Conference on Software Engineering*, p581-590, 2011.

[40] NDSS Z. Lin(*), J. Rhee, X. Zhang, D. Xu, and X. Jiang, "SigGraph: Brute Force Scanning of Kernel Data Structure Instances Using Graph-based Signatures", *the 17th Network and Distributed System Security Symposium*, 12 pages, 2011.

[39] SENSYS V. Sundaram(*), P. Eugster and X. Zhang, "Efficient Diagnostic Tracing Support for Wireless Sensor Networks", *the 8th ACM Conference on Embedded Networked Sensor Systems*, p169-182, 2010.

[38] SRDS B. Xin(*), P. Eugster, X. Zhang, and J. Yang, "Lightweight Task Graph Inference for Distributed Applications", *the 29th IEEE International Symposium on Reliable Distributed Systems*, p100-110, 2010.

[37] FSE W. N. Sumner(*) and X. Zhang, "Memory Indexing: Canonicalizing Addresses Across Executions", *the 18th ACM SIGSOFT Symposium on Foundations of Software*, p217-226, 2010.

[36] ISSTA D. Weeratunge(*), X. Zhang, W. N. Sumner(*), and S. Jagannathan, "Analyzing Concurrency Bugs using Dual Slicing", *International Symposium on Software Testing and Analysis*, p253-264, 2010.

[35] ISSTA T. Bao(*), Y. Zheng(*), Z. Lin(*), X. Zhang and D. Xu, "Strict Control Dependence and Its Effect on Dynamic Information Flow Analyses", *International Symposium on Software Testing and Analysis*, p13-24, 2010.

[34] DSN Z. Lin(*), X. Zhang and D. Xu, "Reuse-Oriented Camouflaging Trojan: Vulnerability Detection and Attack Construction", *the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, p281-290, 2010.

[33] ICSE W. N. Sumner(*), Y. Zheng(*), D. Weeratunge(*), and X. Zhang, "Precise Calling Context Encoding", *the International Conference on Software Engineering*, p525-534 2010.

[32] ASPLOS D. Weeratunge(*), X. Zhang and S. Jagannathan, "Analyzing Multicore Dumps to Facilitate Concurrency Bug Reproduction", *the 15th International Conference on Architectural Support for Programming Languages and Operating Systems*, p155-166, 2010.

[31] NDSS Z. Lin(*), X. Zhang and D. Xu, "Automatic Reverse Engineering of Data Structures from Binary Execution", *the 17th Network and Distributed System Security Symposium*, 12 pages, 2010.

[30] ISSTA B. Xin(*) and X. Zhang, "Memory Slicing", *International Symposium on Software Testing and Analysis*, p165-176, 2009.

[29] FASE W. N. Sumner(*) and Xiangyu Zhang, “Algorithms for Automatically Computing the Causal Paths of Failures”, *Fundamental Approaches to Software Engineering*, p355-369, 2009.

[28] CGO X. Zhang, A. Navabi(*), and S. Jagannathan, “Alchemist: A Transparent Dependence Distance Profiling Infrastructure”, *International Symposium on Code Generation and Optimization*, p47-58, 2009.

[27] FSE Z. Lin(*) and X. Zhang. “Deriving Program Input Syntactic Structure from Execution”, *the 16th ACM SIGSOFT Symposium on Foundations of Software*, p83-93, 2008.

[26] COMPSAC S. Tallam, C. Tian, X. Zhang, and R. Gupta, “Perturbing Program Execution For Avoiding Environmental Faults”, *the 32nd Annual IEEE International Computer Software and Applications Conference*, p152-159, 2008.

[25] DSN Z. Lin(*), X. Zhang, and D. Xu. “Convicting Remote Exploitable Vulnerabilities: An Efficient Input Provenance Based Approach”, *IEEE/IFIP International Conference on Dependable Systems and Networks*, p247-256, 2008.

[24] PLDI B. Xin(*), W. N. Sumner(*), and X. Zhang, “Efficient Program Execution Indexing,” *ACM SIGPLAN Conference on Programming Language Design and Implementation*, p238-248, 2008.

[23] NDSS Z. Lin(*), X. Jiang, D. Xu, and X. Zhang, “Automatic Protocol Format Reverse Engineering Through Context-Aware Monitored Execution”, *the 15th Network and Distributed System Security Symposium*, 12 pages, 2008.

[22] PPOPP A. Navabi(*), X. Zhang, and S. Jagannathan, “Quasi-Static Scheduling for Safe Futures”, *the 13th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, p23-32, 2008.

[21] VLDB M. Zhang(*), X. Zhang, S. Prabhakar, “Tracing Lineage Beyond Relational Operators”, *International Conference on Very Large Data Bases*, p1116-1127, 2007.

[20] ICSM V. Nagarajan, R. Gupta, X. Zhang, M. Madou, B. De Sutter, and K. De Bosschere, “Matching Control Flow of Program Versions”, *International Conference on Software Maintenance*, p84-93, 2007.

[19] ICSM C. Liu, X. Zhang, J. Han, Y. Zhang, B. Bhargava, “Failure Indexing: A Dynamic Slicing Based Approach”, *International Conference on Software Maintenance*, 2007.

[18] ISSTA B. Xin and X. Zhang, “Efficient Online Detection of Dynamic Control Dependence”, *International Symposium on Software Testing and Analysis*, 2007.

[17] ISSTA S. Tallam, C. Tian, X. Zhang, and R. Gupta, “Debugging Long-Running Multithreaded Programs via Dynamic Execution Reduction,” *International Symposium on Software Testing and Analysis*, 2007.

[16] PLDI X. Zhang, S. Tallam, N. Gupta, and R. Gupta, “Towards Locating Execution Omission Errors,” *ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2007.

[15] FSE X. Zhang, S. Tallam, and R. Gupta, “Dynamic Slicing Long Running Programs through Execution Fast Forwarding,” *the 14th ACM SIGSOFT Symposium on Foundations of Software Engineering*, 2006.

[14] PLDI X. Zhang, N. Gupta, and R. Gupta, “Pruning Dynamic Slices with Confidence,” *ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2006.

[13] ICSE X. Zhang, N. Gupta, and R. Gupta, “Locating Faults through Automated Predicate Switching,” *IEEE/ACM International Conference on Software Engineering*, 2006.

[12] ASE N. Gupta, H. He, X. Zhang, and R. Gupta, “Locating Faulty Code Using Failure-Inducing Chops,” *IEEE/ACM International Conference on Automated Software Engineering*, 2005.

[11] PACT S. Tallam, R. Gupta, X. Zhang, “Extended Whole Program Paths,” *International Conference on Parallel Architectures and Compilation Techniques*, 2005.

[10] AADEBUG X. Zhang, H. He, N. Gupta, and R. Gupta, “Experimental Evaluation of Using Dynamic Slices for Fault Location,” *the 6th International Symposium on Automated and Analysis-Driven Debugging*, 2005.

[9] ESEC-FSE X. Zhang and R. Gupta, “Matching Execution Histories of Program Versions,” *Joint the 10th European Software Engineering Conference and the 13th ACM SIGSOFT Symposium on the Foundations of Software Engineering*, 2005.

[8] HPCA Y. Zhang, L. Gao, J. Yang, X. Zhang and R. Gupta, “SENSS: Security Enhancement to Symmetric Shared Memory Multiprocessors,” *the 11th IEEE International Symposium on High Performance Computer Architecture*, 2005.

[7] MICRO X. Zhang and R. Gupta, “Whole Execution Traces,” *the 37th IEEE/ACM International Symposium on Microarchitecture*, 2004.

[6] PLDI X. Zhang and R. Gupta, “Cost Effective Dynamic Program Slicing,” *ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2004.

[5] ICSE X. Zhang, R. Gupta, and Y. Zhang, “Efficient Forward Computation of Dynamic Slices Using Reduced Ordered Binary Decision Diagrams,” *IEEE/ACM International Conference on Software Engineering*, 2004.

[4] CGO S. Tallam, X. Zhang, and R. Gupta, “Extending Path Profiling across Loop Backedges and Procedure Boundaries,” *the 2nd IEEE/ACM International Symposium on Code Generation and Optimization*, 2004.

[3] ICSE X. Zhang, R. Gupta, and Y. Zhang, “Precise Dynamic Slicing Algorithms,” *IEEE/ACM International Conference on Software Engineering*, **Recipient of ACM SIGSOFT Distinguished Paper Award**, 2003.

[2] CGO X. Zhang and R. Gupta, “Hiding Program Slices for Software Security,” *the 1st IEEE/ACM International Symposium on Code Generation and Optimization*, 2003.

[1] ICACI D. Zhang, L. Zhou, and X. Zhang, “Enhancing Information Retrieval With Natural Language Processing Technology,” *IASTED International Conference on Artificial and Computational Intelligence*, 2002.

GRANTS

By Feb 2024, I have raised **13 million dollars** of research funding (my share only).

- **NSF**, Proto-OKN Theme 1: Knowledge Graph Construction for Resilient, Trustworthy, and Secure Software Supply Chain, co-PI (5%), 2023-2025, regular, $1,500,000.
- **DARPA**, Algorithms and Architectures for Robust Attack Detection Using Multi-Modal Controller Logs, co-PI (50%), 2023-2024, seedling, $370,000.
- **ONR**, On-the-fly Cyber Crime Scene Transcribing, PI (100%), 2023-2025, regular, $500,000.
- **Good Ventures Foundation** , Attacks Meet Interpretibility: Detecting Deception in Natural Language Processing Applications by Model Interpretation, Good Ventures Foundation, 2023-, gift, $170,000.
- **DARPA**, Binary Analysis For Domain Specific Language Extraction of Legacy Software, PI (100%), 2021-2025, regular, $1,025,000.
- **IARPA**, PI (75%), ABS: An Analytic Approach to Scanning Neural Networks for Back-doors by Artificial Brain Stimulation, 2020-2024, regular, $3,150,000.
- **Cisco**, co-PI (25%), Learn-to-Investigate: Intelligent, Instrumentation-Free Approach to Multi-Stage Cyber Attack Investigation 2020-2021, gift, $100,000.
- **ONR**, PI (100%), Learn-to-Reason: A Probabilistic Binary Analysis Infrastructure and Its Application in Binary Reduction (Phase Two), 2019-2024, regular, $750,000.
- **IAI**, PI (50%), Athena: Binary Code Randomization for Attack Sensitive Software (BRASS), 2019-2020, regular, $125,000.
- **NSF**, PI (100%), AI Model Debugging by Analyzing Model Internals with Python Program Analysis, 2019-2025, regular, $500,000.
- **NSF**, co-PI (50%), SHF: Medium: Principled Co-Reasoning of Software and Natural-Language Artifacts, 2019-2025, regular, $900,000.
- **ONR**, co-PI (25%),IoT-D: Towards Internets of Dialect-Speaking Things , 2018-2021, regular, $6,000,000.
- **NSF EAGER**, PI (100%), EAGER: A Python Program Analysis Infrastructure to Facilitate Better Data Processing, 2017-2019, regular, $147,000.
- **Sandia National Labs**, co-PI (50%), Automated Threat Modeling for Cyber Security Analytics and Emulation, 2017-2019, regular, $300,000.
- **ONR**, PI (60%), Learn-to-Reason: A Probabilistic Binary Analysis Infrastructure and Its Application in Binary Reduction, 2017-2020, regular, $1,200,000.
- **ONR**, co-PI (33%), A Cross-Layer Framework for Retrofitting Robotic Vehicle Controllers, 2017-2020, regular, $3,000,000.
- **Futurewei Technologies**, PI (100%), 2016-, gift, $100,000.
- **DARPA**, PI (50%), TC: Collaborative: TRACE: Tracking and Analysis of Causality at Enterprise Level, 2015-2019, regular, $1,190,000.
- **ONR**, co-PI (33%), A Tale of Two Systems; Bridging Statistical Learning and Formal Reasoning for Cyber Attack Detection, 2014-2016, regular, $750,000.
- **Cisco**, co-PI (50%),Advanced Targeted Attack Detection via Malware Protocol Reverse Engineering and Log Analytics 2014-2015, gift, $100,000.

- **NSF**, co-PI (50%),TWC: Medium: Collaborative: Towards a Binary-Centric Framework for Cyber Forensics in Enterprise Environments, 2014-2016, regular, $800,000.
- **NSF**, PI (100%), SHF: Small: Reliable Data Processing by Dynamic Program Analysis, 2013-2015, regular, $400,000.
- **NSF**, PI (100%), Collaborative Research: Automated Model Synthesis of Library and System Functions for Program-Environment Co-Analysis, 2013-2015, regular, $150,000.
- **NSF**, PI (100%), Collaborative Research: Automated Model Synthesis of Library and System Functions for Program-Environment Co-Analysis, 2012-2013, regular, $45,000.
- **Telcordia**, PI (50%), Extracting Functional Components from x86 Binaries, 2011-2014, regular, $606,000.
- **DARPA**, PI (33.3%), Safe, Reuse-Oriented Reverse Engineering of Functional Components from x86 Binaries, 2011-2014, regular, $1,470,000.
- **Northrop Grumman**, co-PI (50%), Binary-based Data Structure Reverse Engineering for Memory Forensics and Application Vulnerability Discovery, 2010-2011, regular, $120,000.
- **Air Force Research Lab**, co-PI (33%), Secure End-to-end Service Oriented Architecture, 2010-2011, regular, $232,000.
- **NSF CNS**, co-PI (50%), TC: EAGER: Binary-based Data Structure Revelation for Memory Forensics , 2010-2012, regular, $200,000.
- **NSF CRI**, PI (100%), An Advanced Infrastructure for Generation, Storage, and Analysis of Program Execution Traces, 2009-2010, continued grant, $33,000.
- **NSF IIS**, 2009-2012, co-PI (50%), Towards Scalable and Comprehensive Uncertain Data Management, $474,000.
- **NSF CCF**, 2009-2012, PI (100%), Automated Software Failure Causal Path Computation, $493,000.
- **NSF Career**, 2009-2014, PI (100%), Scalable Dynamic Program Reasoning, $420,000.
- **NSF CSR**, 2008-2011, co-PI (50%), A Holistic Approach to Reliable Pervasive Systems, $400,000.
- **NSF CSR**, 2007-2009, PI (100%), Scalable and Efficient Dynamic Information Flow Tracking in Multithreaded Programs, $100,000.
- **NSF CRI**, PI (100%), An Advanced Infrastructure for Generation, Storage, and Analysis of Program Execution Traces, 2007-2008, $50,000.

STUDENTS

Former PhD Students

Yapeng Ye	**Google**, 2024 PhD.
I Luk Kim	**Senior Computational Scientist at Purdue**, 2023 PhD.
Qiuling Xu	**Netflix**, 2023 PhD.
Yingqi Liu	**Research Scientist at Microsoft**, 2023 PhD.
Hongjun Choi	**Assistant Professor at Daegu Gyeongbuk Institute of Science and Technology**, 2022 PhD.
Fei Wang	**Meta**, 2021 PhD.
Dohyeong Kim	**Google**, 2020 PhD.
Wen-chuan Lee	**Senior Scientist at Apple**, 2019 PhD.
Shiqing Ma	**Assistant Professor at University Massachusetts Amherst**, **NSF Career Awardee**, previously Assistant Professor at Rutgers University, 2019 PhD.
Yonghwi Kwon	**Assistant Professor at University of Maryland, College Park**, **NSF Career Awardee**, previously Assistant Professor at University of Virginia, 2018.
Weihang Wang	**Assistant Professor at University of Southern California**, **NSF Career Awardee**, previously Assistant Professor at SUNY Buffalo, 2018.

Jianjun Huang	**Assistant Professor at Renmin University (China)**, 2017.
Brendan Saltaformmagio	**Associate Professor at Georgia Tech**, **Recipient of ACM SIGACT Distinguished Dissertation Award and NSF Career Award**, co-advised with Dongyan Xu, 2017.
Chung Hwan Kim	**Assistant Professor at UT Dallas**, previously **NEC Labs**, 2016 (co-advised with Dongyan Xu)
Fei Peng	**Senior Manager at Apple**, 2015.
Zhui Deng	**Apple**, 2015 (co-advised with Dongyan Xu).
Kyuhyung Lee	**Associate Professor at University of Georgia**, 2014 (co-advised with Dongyan Xu).
Yunhui Zheng	**Co-founder and CTO of Sec3**, previously Research Staff at IBM TJ Watson, 2014.
Bao Tao	**Lead of Engineering** at Sec3, previously Google, 2014.
William N. Sumner	**Associate Professor at Simon Fraser University**, 2013.
Vinai Sundaram	**Founded SensorHound Innovations LLC**, 2013 (co-advised with Patrick Eugster).
Dasarath Weeratunge	**Intel Lab**, 2012 (co-advised with Suresh Jagannathan).
Zhiqiang Lin	**Distinguished Professor at Ohio State University, previously UT Dallas, NSF Career Awardee, Airforce Young Investigator Awardee**, 2011 (co-advised with Dongyan Xu).
Bin Xin	**Google**, 2010.
Mingwu Zhang	**Microsoft**, 2008 (co-advised with Sunil Prabhakar).

Current PhD Students

Jiasheng Jiang	(start spring 2024)
Syed Yusuf Ahmed	(start fall 2023)
Xiaolong Jin	(start fall 2023)
Hanxi Guo	(start fall 2023)
Zian Su	(start fall 2022)
Xuan Zhou	(start fall 2022)
Mingwei Zheng	(start fall 2022)
Lu Yan	(start fall 2022)
Xuan Chen	(start fall 2021)
Kaiyuan Zhang	(start fall 2021), co-advised with Ninghui Li
Xiangzhe Xu	(start fall 2021)
Shiwei Feng	(start fall 2021)
Siyuan Cheng	(start fall 2021)
Yunshu Mao	(start fall 2020)
Xuwei Liu	(start fall 2019)
Zhiyuan Cheng	(start fall 2019)
Guangyu Shen	(start fall 2019)
Yu Shi	(start fall 2018)
Shengwei An	(start fall 2018)
Guanhong Tao	(start fall 2017)
Le Yu	(start fall 2017)
Yi Sun	(start fall 2016)
Sayali Kate	(start fall 2015).

Current Post-Doc

Chengpeng Wang	(start spring 2024)
Zhuo Zhang	(start fall 2023), previously a PhD student in the group (started fall 2018

Former Post-Doc

Qingkai Shi	**Assistant Professor at Nanjing University, China**, 2022-2023.
Hongyu Liu	**Gifted Young Researcher at HuaWei**, 2021-2022.
Mijung Kim	**Assistant Professor at Ulsan National Institute of Science and Technology (Korea)**, 2020-2021.
Yousra Aafer	**Assistant Professor at University of Waterloo Canada**, **Awardee of Discovery Grant by NSERC**, similar to NSF Career in the US, 2019-2021.

Juan Zhai	**Assistant Professor at University Massachusetts Amherst**, previously Professor of Practice at Rugters University, 2018-2019.
Wei You	**Associate Professor at Renmin University, China**, recipient of **Excellent Young Scientists Overseas**, 2019-2022.
Peng Liu	**Research Staff at IBM TJ Watson**, 2014-2015.
Zhiyong Shan	**Univeristy of California, San Diego**, 2012-2013.
Former Undergraduate Students	
Carson Harmon	**Trail of Bits**, 2019.
William Rowan	**Intel**, 2011.
Former Minority Student	
Angello Astorga	through the Summer Research Opportunities Program (SROP), 2013 (**nominated for the National Exemplary Summer Research Citation**)

TALKS

- *Learn-2-Reason: Bridging the Gap of Machine Learning and Formal Reasoning for Better Security*, **keynote speaker** for the 31st International Conference on Tools with Artificial Intelligence (ICTAI), Portland, October 2019.
- *Analyzing AI Model Internals for Debugging and Adversarial Sample Attack Detection*, **invited speaker** for NSF Workshop for Software Engineering and Deep Learning, San Diego, November 2019.
- *Analyzing AI Model Internals for Debugging and Adversarial Sample Attack Detection*, **invited speaker** on ICSE 2019 Workshop on Deep Neural Network Testing (DEEPTEST), Montreal, Canda, May, 2019.
- *Analyzing AI Model Internals for Debugging and Adversarial Sample Attack Detection*, **invited speaker**, ETH, October 2018.
- *Dynamic Program Analyses and Their Security Applications*, **invited speaker**, University of NorthWestern, April, 2018.
- *Dynamic Program Analyses and Their Security Applications*, **Distinguished Speaker** UCI, April, 2018.
- *X-Force: Force-Executing Binary Programs for Security Applications*, **Distinguished Speaker** Virginia Tech, September 2015.
- *Handling Instability in Data Processing Through Runtime Program Analysis*, Northeastern University, August 2015.
- *Handling Instability in Data Processing Through Runtime Program Analysis*, Wuhan University, June 2015, China.
- *Handling Instability in Data Processing Through Runtime Program Analysis*, University of Science and Technology of China, June 2015, China.
- *Handling Instability in Data Processing Through Runtime Program Analysis*, Nanjing University, June 2015, China.
- *Debugging, Instrumentation, and Security*, Huawei US, September 2013, US.
- *Analyzing Floating Point Programs for Instabitility Detection*, invited talk on the 3rd International Symposium on High Confidence Software (ISHCS), Peking University, China, 2013.
- *Avoiding Confoundings in Delta Debugging type of Causality Inference*, Dagstuhl, Germany, 2013.
- *Reverse Engineering of Data Structures from Binary*, IUPUI, 2012.
- *Reproducing, Understanding, and Suppressing Non-deterministic Bugs in Concurrent Programs*, IBM China, 2012.

- *Canonicalizing Execution for Automated Debugging*, Nanjing University, 2011.
- *Canonicalizing Execution for Automated Debugging*, invited talk on the 1st International Symposium on High Confidence Software (ISHCS), Peking University, China, 2011.
- *Canonicalizing Execution for Automated Debugging*, UIUC, 2011.
- *Canonicalizing Execution for Automated Debugging*, Coverity Inc., 2011.
- *Binary-Based Data Structure Reverse Engineering for Memory Forensics and Application Vulnerability Discovery*, Northrop Grumman Cybersecurity Research Consortium, 2010.
- *Automated Software Failure Explanation*, the 45th Software Engineering Research Center (SERC) Showcase, 2008.
- *Dynamic Slicing Long Running Programs through Execution Fast Forwarding,* ACM SIGSOFT Symposium on Foundations of Software Engineering (FSE), 2006.
- *Locating Faults through Automated Predicate Switching,* IEEE/ACM International Conference on Software Engineering (ICSE), 2006.
- *Efficient and Effective Dynamic Slicing,* University of Colorado, Boulder, 2006.
- *Efficient and Effective Dynamic Slicing,* Penn State University, 2006.
- *Efficient and Effective Dynamic Slicing,* IBM T. J. Watson, 2006.
- *Efficient and Effective Dynamic Slicing,* Microsoft, 2006.
- *Experimental Evaluation of Using Dynamic Slices for Fault Location,* the 6th International Symposium on Automated and Analysis-Driven Debugging (AADEBUG), 2005.
- *Whole Execution Traces, the 37th IEEE/ACM International Symposium on Microarchitecture* (MICRO), 2004.
- *Cost Effective Dynamic Program Slicing,* ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), 2004.
- *Efficient Forward Computation of Dynamic Slices Using Reduced Ordered Binary Decision Diagrams,* IEEE/ACM International Conference on Software Engineering (ICSE), 2004.
- *Precise Dynamic Slicing Algorithms,* IEEE/ACM International Conference on Software Engineering (ICSE), 2003
- *Hiding Program Slices for Software Security,* IEEE/ACM International Symposium on Code Generation and Optimization (CGO), 2003.

TEACHING EXPERIENCE

Fall 19, Instructor	**Purdue University**, West Lafayette, IN CS 590PAD, *Program Analysis for Deep Learning*.
Spring 19, Instructor	**Purdue University**, West Lafayette, IN CS 408, *Software Testing*.
Fall 18, Instructor	**Purdue University**, West Lafayette, IN CS 408, *Software Testing*.
Spring 18, Instructor	**Purdue University**, West Lafayette, IN CS 240, *C Programming*.
Fall 17, Instructor	**Purdue University**, West Lafayette, IN CS 408, *Software Testing*.
Spring 17, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Fall 16, Instructor	**Purdue University**, West Lafayette, IN CS 407, *Software Testing*.
Spring 16, Instructor	**Purdue University**, West Lafayette, IN CS 407, *Software Testing*.
Fall 15, Instructor	**Purdue University**, West Lafayette, IN CS 407, *Software Testing*.
Spring 15, Instructor	**Purdue University**, West Lafayette, IN CS 407, *Software Testing*.
Fall 14, Instructor	**Purdue University**, West Lafayette, IN CS 353, *Principles of Concurrency and Parallelism*.
Spring 14, Instructor	**Purdue University**, West Lafayette, IN CS 407, *Software Testing*.
Spring 13, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Fall 12, Instructor	**Purdue University**, West Lafayette, IN CS 490, *Software Testing*.
Spring 12, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Fall 11, Instructor	**Purdue University**, West Lafayette, IN CS 490, *Software Testing*.
Spring 11, Instructor	**Purdue University**, West Lafayette, IN CS 352, *Compilers: Principles and Practice*.
Fall 10, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Spring 10, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Fall 09, Instructor	**Purdue University**, West Lafayette, IN CS 590, *Advanced Testing and Debugging*.
Spring 09, Instructor	**Purdue University**, West Lafayette, IN CS 352, *Compilers: Principles and Practice*.
Fall 08, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Spring 08, Instructor	**Purdue University**, West Lafayette, IN CS 510, *Software Engineering*.
Fall 07, Instructor	**Purdue University**, West Lafayette, IN CS 590Z, *Software Defect Analysis*.
Spring 07, Instructor	**Purdue University**, West Lafayette, IN CS 590F, *Software Reliability*.

PROFESSIONAL ACTIVITIES

- (PC Chair): ISSTA, 2021

- (PC member): CCS, 2020, 2019, 2018, 2014-2016
- (PC member): ISSTA, 2020, 2017, 2016, 2015, 2014, 2012, 2010, 2009
- (PC member): ASE, 2020, 2019, 2018
- (PC member): ICSE, 2020, 2019, 2018, 2017.
- (PC member): FSE, 2020, 2019, 2018, 2016.
- (PC member): ICST, 2015, 2014, 2012
- (Workshop chair): *ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI), 2014-2016.
- (Demo Chair): ISSTA, 2015.
- (Doctoral Symposium co-chair): *ACM SIGSOFT Symposium on Foundations of Software Engineering* (FSE), 2014.
- (PC member): ICSE Doctoral Symposium, 2014.
- (PC member): ASIACCS, 2013.
- (PC member): RV, 2013, 2011
- (PC member): *10th Asian Symposium on Programming Languages and Systems* (APLAS), 2012.
- (PC member): *Object-Oriented Programming, Systems, Languages & Applications* (OOPSLA), 2012.
- (Workshop co-chair): *ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI), 2012.
- (ERC member): *ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI), 2019, 2012.
- (PC co-Chair): *Workshop on Dynamic Analysis* (WODA), 2011.
- (PC member): *International Symposium on Software Reliability Engineering* (ISSRE), 2009.
- (PC member): *International Conference on Software Maintenance* (ICSM), 2009.
- (PC member): *ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI), 2009.
- (PC member): *The 2nd International Conference of Software Testing* (ICST), 2009, 2008

EDITOR/REVIEWER FOR JOURNALS

- (Associate Editor): IEEE Transcations on Software Engineering, 2017-present.
- (Guest Editor): Journal of Computer Science and Technology, 2015.
- **Distinguished Reviewer of 2012** for TOSEM.
- Reviewers for TOPLAS, TOSEM, TSE, TACO, Computer Security, Software Practice and Experience, Empirical Software Engineering, International Journal of Information Security.