Wei Yang

Web: http://youngwei.com/
Email: wei.yang@utdallas.edu

800 W. Campbell Road
Richardson, TX 75080, USA

Education

2013–2018	**Ph.D. Computer Science**, *University of Illinois at Urbana-Champaign.* Advisors: Tao Xie and Carl A. Gunter
2011–2013	**M.S. Computer Science**, *North Carolina State University.*
2007–2011	**B.E. Software Engineering**, *Shanghai Jiao Tong University.*
2007–2011	**B.S. Accounting**, *Shanghai Jiao Tong University.*

Positions held

Fall 2018 - Now	**Assistant Professor**, University of Texas at Dallas, USA.
Summer 2017	**Visiting Researcher**, University of California Berkeley, USA. Advisor: Prof. Dawn Song
Summer 2016	**Research Intern**, IBM T.J Watson Research Center, USA.
Summer 2015	**Research Intern**, Samsung Research America, USA.
Summer 2012-2014	**Research Intern**, Fujitsu Lab of America, USA. Manager: Dr. Mukul Prasad
2010-2011	**Software Engineering Intern**, eBay, Inc., China.

Conference Publications

* indicating students advised by me

[C1] Simin Chen*, Xiaoning Feng, Xiaohong Han, Cong Liu, Wei Yang. PPM: Automated Generation of Diverse Programming Problems for Benchmarking Code Generation Models *In the ACM International Conference on the Foundations of Software Engineering.(**FSE**)*, 2024.

[C2] Xinyue Liu, Zihe Song*, Weike Fang, Wei Yang, Weihang Wang. WEFix: Intelligent Automatic Generation of Explicit Waits for Efficient Web End-to-End Flaky Tests. *In The ACM TheWebConf 2024 Conference (**WWW**)*, 2024.

[C3] Hanlin Chen, Simin Chen*, Wenyu Li*, Wei Yang, Yiheng Feng. Impact Analysis of Inference Time Attack of Perception Sensors on Autonomous Vehicles. *In the 103rd Transportation Research Board Annual Meeting (**TRBAM**)*, 2024.

[C4] Simin Chen*, Shiyi Wei, Cong Liu, Wei Yang. DyCL: Dynamic Neural Network Compilation Via Program Rewriting and Graph Optimization. *In the ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA**)*, 2023.

[C5] Simin Chen*, Hanlin Chen, Mirazul Haque*, Cong Liu, Wei Yang. The Dark Side of Dynamic Routing Neural Networks: Towards Efficiency Backdoor Injection. *In The IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**)*, 2023.

[C6] Yiming Chen, Simin Chen*, Zexin Li, Wei Yang, Cong Liu, Robby T. Tan, Haizhou Li. Dynamic Transformers Provide a False Sense of Efficiency. *In Annual Meeting of the Association for Computational Linguistics (**ACL**)*, 2023.

[C7]   Yufei Li*, Zexin Li, Wei Yang, Cong Liu. RT-LM: Uncertainty-Aware Resource Management for Real-Time Inference of Language Models. *In IEEE Real-Time Systems Symposium (**RTSS**)*, 2023.

[C8]   Mirazul Haque*, Rutvij Shah*, Simin Chen*, Berrak Sisman, Cong Liu, Wei Yang. SlothSpeech: Denial-of-service Attack Against Speech Recognition Models. *In the 24th Interspeech Conference (**INTERSPEECH**)*, 2023.

[W9]   Mirazul Haque*, Wei Yang Dynamic Neural Network is All You Need: Understanding the Robustness of Dynamic Mechanisms in Neural Networks. *In the ICCV 2023 Workshop on Resource Efficient Deep Learning for Computer Vision (**ICCV-W**)*, 2023.

[W10] Mirazul Haque*, Simin Chen*, Wasif Haque*, Cong Liu, Wei Yang AntiNODE: Evaluating Efficiency Robustness of Neural ODEs. *In the ICCV 2023 Workshop on Resource Efficient Deep Learning for Computer Vision (**ICCV-W**)*, 2023.

[C11] Simin Chen*, Cong Liu, Mirazul Haque*, Zihe Song*, Wei Yang. NMTSloth: Understanding and Testing Efficiency Degradation of Neural Machine Translation Systems. *In the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**FSE**)*, 2022.

[C12] Simin Chen*, Mirazul Haque*, Cong Liu, Wei Yang. DeepPerform: An Efficient Approach for Performance Testing of Resource-Constrained Neural Networks. *In the 37th IEEE/ACM International Conference on Automated Software Engineering. (**ASE**)*, 2022.

[C13] Guanqun Yang, Mirazul Haque*, Qiaochu Song, Wei Yang, Xueqing Liu. TestAug: A Framework for Augmenting Capability-based NLP Tests. *In The 29th International Conference ON Computational Linguistics (**COLING**)*, 2022.

[C14] Zihe Song*, Yingfeng Chen, Lei Ma, Shangjie Lu, Honglei Lin, Changjie Fan, Wei Yang. An Empirical Analysis of Compatibility Issues for Industrial Mobile Games. *In the 33rd IEEE International Symposium on Software Reliability Engineering (**ISSRE**)*, 2022.

[C15] Simin Chen*, Hamed Khanpour, Cong Liu, Wei Yang. Learning to Reverse DNNs from AI Programs Automatically. *In The 31st International Joint Conference on Artificial Intelligence (**IJCAI**)*, 2022.

[C16] Simin Chen*, Zihe Song*, Mirazul Haque*, Cong Liu, Wei Yang. NICGSlowDown: Evaluating the Efficiency Robustness of Neural Image Caption Generation Models. *In The IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**)*, 2022.

[W17] Mirazul Haque*, Christof Budnik, Wei Yang CorrGAN:Input Transformation Technique Against Natural Corruptions. *In CVPR Workshop on The Art of Robustness: Devil and Angel in Adversarial Machine Learning (**CVPR-W**)*, 2022.

[W18] Senrong Xu, Yuan Yao, Liangyue Li, Wei Yang, Feng Xu, Hanghang Tong Detecting Topology Attacks against Graph Neural Networks. *In the CIKM 2022 Workshop on Trust Worthy Learning on Graphs. (**CIKM-W**)*, 2022.
       Best Paper Award RunnerUp.

[C19] Mirazul Haque*, Yaswanth Yadlapalli, Wei Yang, Cong Liu. EREBA: Black-box Energy Testing of Adaptive Neural Networks. *In The 44th International Conference on Software Engineering (**ICSE**)*, 2022.

[C20] Yueming Wu*, Deqing Zou, Shihan Dou, Wei Yang, Duo Xu, Hai Jin. VulCNN: An Image-inspired Scalable Vulnerability Detection System. *In The 44th International Conference on Software Engineering (**ICSE**)*, 2022.

[C21] Wenyu Wang, Wei Yang, Tianyin Xu, Tao Xie. Vet: Identifying and Avoiding UI Exploration Tarpits. *In The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**FSE**)*, 2021.
       ACM SIGSOFT Distinguished Paper Award.

[C22] Ke Chen†, Yufei Li*†, Yingfeng Chen, Changjie Fan, Zhipeng Hu, Wei Yang. GLIB: Towards Automated Test Oracle for Graphically-Rich Applications. *In The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**FSE**)*, 2021.
† First two authors contributed equally.

[C23] Yueming Wu*, Deqing Zou, Wei Yang, Xiang Li, Hai Jin. HomDroid: Detecting Android Covert Malware by Social-Network Homophily Analysis. *In ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA**)*, 2021.

[C24] Fei Shao, Rui Xu, Wasif Haque*, Jingwei Xu, Ying Zhang, Wei Yang, Yanfang Ye, Xusheng Xiao. WebEvo: Taming Web Application Evolution via Detecting Semantic Structure Change. *In ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA**)*, 2021.

[C25] Alan Romano, Zihe Song*, Sampath Grandhi*, Wei Yang, Weihang Wang. An Empirical Analysis of UI-based Flaky Tests. *In 43rd International Conference on Software Engineering (**ICSE**)*, 2021.

[C26] Shudi Shao, Zhengyi Qiu, Xiao Yu, Wei Yang, Guoliang Jin, Tao Xie, Xintao Wu. Database-Access Performance Antipatterns in Database-Backed Web Applications. *In the International Conference on Software Maintenance and Evolution (**ICSME**)*, 2020.

[C27] Yueming Wu*, Deqing Zou, Shihan Dou, Siru Yang, Wei Yang, Feng Cheng, Hong Liang, Hai Jin. SCDetector: Software Functional Clone Detection Based on Semantic Tokens Analysis. *In the 35th IEEE/ACM International Conference on Automated Software Engineering. (**ASE**)*, 2020.

[C28] Simin Chen*, Soroush Bateni, Sampath Grandhi*, Xiaodi Li*, Cong Liu, Wei Yang. DENAS: Automated Rule Generation by Knowledge Extraction from Neural Networks *In ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. (**FSE**)*, 2020.

[C29] Mirazul Haque*, Anki Chauhan*, Cong Liu, Wei Yang. ILFO: Adversarial Attack on Adaptive Neural Networks. *In IEEE/CVF Conference on Computer Vision and Pattern Recognition. (**CVPR**)*, 2020.

[C30] Yuyu He, Lei Zhang, Zhemin Yang, Yinzhi Cao, Keke Lian, Shuai Li, Wei Yang, Zhibo Zhang, Min Yang, Yuan Zhang, and Haixin Duan. TextExerciser: Feedback-driven Text Input Exercising for Android Applications. *In Proceedings of 41st IEEE Symposium on Security and Privacy. (**IEEE S&P**)*, 2020.

[C31] Yueming Wu*, Xiaodi Li*, Deqing Zou, Wei Yang, Xin Zhang, and Hai Jin. MalScan: Fast Market-Wide Mobile Malware Scanning by Social-Network Centrality Analysis. *In Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering. (**ASE**)*, 2019.

[C32] Qi Wang, Pubali Datta, Wei Yang, Si Liu, Carl Gunter, and Adam Bates. Charting the Attack Surface of Trigger-Action IoT Platforms. *In Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, 2019.

[C33] Zhengkai Wu, Evan N. Johnson*, Wei Yang, Osbert Bastani, Dawn Song, Jian Peng, and Tao Xie. REINAM: Reinforcement Learning for Input-Grammar Inference. *In Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**FSE**)*, 2019.

[C34] Wujie Zheng, Wenyu Wang, Dian Liu, Changrong Zhang, Qinsong Zeng, Yuetang Deng, Wei Yang, Pinjia He and Tao Xie. Detecting Failures of Neural Machine Translation in the Absence of Reference Translations. *Proceedings of the 49th IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN**)*, **Industry Track**, 2019.

[C35] Wujie Zheng, Wenyu Wang, Dian Liu, Changrong Zhang, Qinsong Zeng, Yuetang Deng, Wei Yang, Pinjia He, and Tao Xie. Testing Untestable Neural Machine Translation: An Industrial Case. *Proceedings of the 41st International Conference on Software Engineering (**ICSE**)*, **Poster**, 2019.

[C36] Zexuan Zhong, Jiaqi Guo, Wei Yang, Jian Peng, Tao Xie, Jian-Guang Lou, Ting Liu and Dongmei Zhang. SemRegex: A Semantics-Based Approach for Generating Regular Expressions from Natural Language Specifications. *In Proceedings of the Conference on Empirical Methods in Natural Language Processing (**EMNLP**)*, 2018.

[C37] Karan Ganju, Qi Wang, Wei Yang, Carl Gunter and Nikita Borisov. Property Inference Attacks on Deep Neural Networks using Permutation Invariant Representations. *In Proceedings of the 25th ACM Conference on Computer and Communications Security (**CCS**)*, 2018.

[C38] Wenyu Wang, Dengfeng Li, Wei Yang, Yurui Cao*, Zhenwen Zhang, Yuetang Deng and Tao Xie. An Empirical Study of Android Test Generation Tools in Industrial Cases. *In Proceedings of the 33rd International Conference on Automated Software Engineering (**ASE**)*, 2018.

[C39] Xueqing Liu, Yue Leng, Wei Yang, Wenyu Wang, Chengxiang Zhai, and Tao Xie. A Large-Scale Empirical Study on Android Runtime Permission Rationale Messages. *In Proceedings of the IEEE Symposium on Visual Languages and Human-Centric Computing (**VL/HCC**)*, 2018.

[C40] Xueqing Liu, Yue Leng, Wei Yang, Chengxiang Zhai and Tao Xie. Mining Android App Description for Permission Requirements Recommendation. *In Proceedings of the 26th International Requirements Engineering Conference (**RE**)*, 2018.

[C41] Wei Yang, Mukul Prasad, and Tao Xie. EnMobile: Entity-based Characterization and Analysis of Mobile Malware. *In Proceedings of the 40th International Conference on Software Engineering (**ICSE**)*, 2018.

[W42] Wei Yang and Tao Xie. Telemade: A Testing Framework for Learning-Based Malware Detection Systems. *In Proceedings of the AAAI-18 Workshop on Engineering Dependable and Secure Machine Learning Systems (**AAAI-W**)*, 2018.

[W43] Zexuan Zhong, Jiaqi Guo, Wei Yang, Tao Xie, Jian-Guang Lou, Ting Liu, and Dongmei Zhang. Generating Regular Expressions from Natural Language Specifications: Are We There Yet? *In Proceedings of the AAAI-18 Workshop on NLP for Software Engineering (**AAAI-W**)*, 2018.

[C44] Wei Yang, Deguang Kong, Tao Xie and Carl A. Gunter. Malware Detection in Adversarial Settings: Exploiting Feature Evolutions and Confusions in Android Apps. *In Proceedings of the 33rd Annual Computer Security Applications Conference (**ACSAC**)*, pages 288–302, 2017

[C45] Haibing Zheng, Dengfeng Li, Beihai Liang, Xia Zeng, Wujie Zheng, Yuetang Deng, Wing Lam, Wei Yang, and Tao Xie. Automated test input generation for Android: Towards getting there in an industrial case *In Proceedings of the 39th International Conference on Software Engineering (**ICSE**)*, **SEIP**, pages 253–262, 2017.

[C46] Dengfeng Li, Wing Lam, Wei Yang, Zhengkai Wu, Xusheng Xiao, Tao Xie. Towards Privacy-Preserving Mobile Apps: A Balancing Act. *ACM Symposium and Bootcamp on the Science of Security (**HotSoS**)*, 2017.

[C47] Xia Zeng, Dengfeng Li, Wujie Zheng, Fan Xia, Yuetang Deng, Wing Lam, Wei Yang, and Tao Xie. Automated Test Input Generation for Android: Are We Really There Yet in an Industrial Case? *In Proceedings of the 24th ACM SIGSOFT Symposium on the Foundations of Software Engineering (**FSE**)*, **Industry Track**, pages 987–992, 2016.

[C48] Soteris Demetriou, Whitney Merrill, Wei Yang, Aston Zhang and Carl A. Gunter Free for All! Assessing User Data Exposure to Advertising Libraries on Android. *In Proceedings of the 23rd Annual Network and Distributed System Security Symposium (**NDSS**)*, 2016

[C49] Wei Yang, Xusheng Xiao, Sihan Li, Benjamin Andow, William Enck, and Tao Xie. AppContext: Differentiating Malicious and Benign Mobile App Behaviors Using Context. *In Proceedings of the 37th International Conference on Software Engineering (**ICSE**)*, pages 303–312, 2015.

[C50] Wei Yang, Xusheng Xiao, Rahul Pandita, William Enck, and Tao Xie. Improving Mobile Application Security via Bridging User Expectations and Application Behaviors. *ACM Symposium and Bootcamp on the Science of Security (**HotSoS**)*, 2014.

[C51] Rahul Pandita, Xusheng Xiao, Wei Yang, William Enck, and Tao Xie. WHYPER: Towards Automating Risk Assessment of Mobile Applications. *In Proceedings of the 22nd USENIX Security Symposium (**USENIX Security**)*, pages 527–542, 2013.

[C52] Wei Yang, Mukul Prasad, and Tao Xie. A Grey-box Approach for Automated GUI-Model Generation of Mobile Applications. *In Proceedings of the 16th International Conference on Fundamental Approaches to Software Engineering (**FASE**)*, pages 250–265, 2013.

Journal Publications

[J1] Yueming Wu*, Shihan Dou, Deqing Zou, Wei Yang, Weizhong Qiang, Hai Jin. Contrastive Learning for Robust Android Malware Familial Classification. *In IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, 2022.

[J1] Deqing Zou, Yueming Wu*, Siru Yang, Anki Chauhan*, Wei Yang, Jiangying Zhong, Shihan Dou, Hai Jin. IntDroid: Android Malware Detection Based on API Intimacy Analysis. *In ACM Transactions on Software Engineering and Methodology (**TOSEM**)*, 2021.

[J2] Wei Yang, Xusheng Xiao, Dengfeng Li, Huoran Li, Xuanzhe Liu, Haoyu Wang, Yao Guo, and Tao Xie. Security Analytics for Mobile Apps: Achievements and Challenges. *Journal of Cyber Security(**JCS**)*, 2016.

Patent

[P1] Deguang Kong, Wei Yang, and Hongxia Jin. Malware detection by exploiting malware re-composition variations using feature evolutions and confusions. *US Patent 10,505,960*, 2019.

[P2] Mukul Prasad and Wei Yang. Automatically extracting a model for the behavior of a mobile application. *US Patent 10,360,027*, 2019.

[P3] Mukul Prasad and Wei Yang. Detection of malicious software behavior using signature-based static analysis. *US Patent 9,779,239*, 2017.

Professional Services

Associate Editor	ACM Transactions on Software Engineering and Methodology (TOSEM), 2023-2029
Organizing Committee Member	International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2023), PC Chair for Dependability and Security Track, 2023
Organizing Committee Member	International Symposium on Software Testing and Analysis (ISSTA), Sponsorship Chair, 2020
Organizing Committee Member	ASIA-PACIFIC Software Engineering Conference (APSEC), Poster Chair, 2020

Organizing Committee Member	International Conference on Automated Software Engineering (ASE), Web Chair, 2017
PC Member	International Conference on Software Engineering (ICSE), 2025
PC Member	International Workshop on Large Language Models for Code (LLM4Code), 2024
PC Member	Symposium on the Foundations of Software Engineering (FSE), 2024
PC Member	International Symposium on Software Testing and Analysis (ISSTA), 2024
PC Member	International Conference on Software Testing (ICST), 2024
PC Member	International Conference on Software Engineering (ICSE), 2023
PC Member	International Conference on Automated Software Engineering (ASE), 2023
PC Member	Mining Software Repositories Conference (MSR), 2023
PC Member	International Conference on Software Testing (ICST), 2023
PC Member	International Symposium on Software Reliability Engineering (ISSRE), 2023
PC Member	The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), Demo Track, 2023
PC Member	International Conference on Automated Software Engineering (ASE), 2022
PC Member	International Symposium on Software Reliability Engineering (ISSRE), 2022
PC Member	Mining Software Repositories Conference (MSR), 2022
PC Member	International Conference on Software Testing (ICST), 2022
PC Member	International Symposium on Software Testing and Analysis (ISSTA), Doctoral Symposium, 2022
PC Member	International Conference on Software Engineering (ICSE), Demo Track, 2022
PC Member	International Conference on Software Testing (ICST), 2021
PC Member	International Conference on Software Engineering (ICSE), 2021
PC Member	AAAI Conference on Artificial Intelligence (AAAI), 2021
PC Member	International Symposium on Software Testing and Analysis (ISSTA), Demo Track, 2020
PC Member	International Conference on Software Engineering (ICSE), Artifact Evaluation, 2019
PC Member	International Conference on Computer-Aided Verification (CAV), Artifact Evaluation, 2019
PC Member	International Symposium on Software Testing and Analysis (ISSTA), Artifact Evaluation, 2018
PC Member	International Symposium on Software Testing and Analysis (ISSTA) Artifact Evaluation, 2017
PC Member	International Symposium on Software Testing and Analysis (ISSTA) Artifact Evaluation, 2016
PC Member	International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA) Artifact Evaluation, 2016
PC Member	European Conference on Object-Oriented Programming (ECOOP), Artifact Evaluation, 2015
Shadow PC Advisor	Mining Software Repositories Conference (MSR), 2022
Shadow PC Member	IEEE Symposium on Security and Privacy (IEEE S&P), 2016
Shadow PC Member	European Conference on Computer Systems (EuroSys), 2016