Wei Yang

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

800 W. Campbell Road
Richardson, TX 75080, USA

Research Interests

My research interests lie in **Computer Security** and **Software Engineering**. I have been working on using program analysis, natural language processing, cognitive analysis, and machine learning techniques to bridge the gap between user perceptions and security-sensitive behaviors in mobile security systems. Recently, I have been focusing on enhancing the robustness of these newly-proposed intelligent security techniques in adversarial settings.

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.
Manager: Dr. Marco Pistoia
Mentor: Dr. Peng Liu

Summer 2015 **Research Intern**, Samsung Research America, USA.
Manager: Dr. Hongxia Jin
Mentor: Dr. Deguang Kong, Dr. Bin Liu

Summer 2012-2014 **Research Intern**, Fujitsu Lab of America, USA.
Mentor & Manager: Dr. Mukul Prasad

2010-2011 **Software Engineering Intern**, eBay, Inc., China.

Conference Publications

[C1] 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.

[C2] 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.

[C3] 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.

[C4] 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.

[C5] 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.

[C6] 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.

[C7] 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.

[C8] 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.

[C9] 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.

[C10] 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.

[C11] 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.

[C12] 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

[C13] 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.

[C14] 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.

[C15] 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

[C16] 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.

[C17] 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.

[C18] 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 & Workshop Publications

[W1] Wei Yang and Tao Xie. Telemade: A Testing Framework for Learning-Based Malware Detection Systems. *To appear in Proceedings of the AAAI-18 Workshop on Engineering Dependable and Secure Machine Learning Systems (**EDSMLS**)*, 2018.

[W2] 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? *To appear in Proceedings of the AAAI-18 Workshop on NLP for Software Engineering (**NL4SE**)*, 2018.

[W3] 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.

[J1] 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*, 1(2), pages 1–14, 2016.

[W4] 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.

Patent

[P1] Deguang Kong, Wei Yang, and Hongxia Jin. Malware detection by exploiting malware re-composition variations using feature evolutions and confusions. *US Patent App. 15/388,460*, 2017.

[P2] Mukul Prasad and Wei Yang. Detection of malicious software behavior using signature-based static analysis. *US Patent App. 14/658,204*, 2016.

[P3] Mukul Prasad and Wei Yang. Automatically extracting a model for the behavior of a mobile application. *US Patent App. 13/587,920*, 2014.

Invited Talks

2017 Generating Adversarial Examples with Program Transformations: Practical Attacks to Machine Learner. Midwest Programming Languages Summit (MWPLS 2017), Bloomington, IN, 2017

2017 Contextually-Aware Mobile Security: Attacks and Defense of Mobile Threats. FShanghai Jiaotong University, Shanghai, China, 2017.

2017 Defense and Attacks on Mobile Malware Detection, Fudan University. Shanghai, China, 2017.

2017 Testing Learning-Based Security System: Generating Adversarial Samples for Static Analysis and Machine Learning. East China Normal University, Shanghai, China, 2017.

2017 Defense and Attacks on Mobile Malware Detection. ShanghaiTech University, Shanghai, China, 2017.

2016 Searching Functionally Similar Code via UI Prototype. IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 2016.

2016 Contextually-Aware Mobile Security: Identification, Variation and Fixing of Mobile Threats. IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 2016.

2016 Validating Application Behavior against User Expectations. QualComm Innovation Fellowship Final, San Diego, CA, 2016.

2015 AppContext: Differentiating Malicious and Benign Mobile App Behaviors Using Context. Shanghai Jiao Tong University, Shanghai, China, 2015.

2015 AppContext: Differentiating Malicious and Benign Mobile App Behaviors Using Context. SRI International, Menlo Park, CA, 2015.

2015 Improving Mobile Application Security via Bridging User Expectations and Application Behaviors. 10th CSL student conference, Champaign, IL, 2015.

Professional Services

Organizing Committee Member — International Conference on Automated Software Engineering (ASE), 2017

PC Member — International Conference on Software Engineering (ICSE), Artifact Evaluation, 2019

PC Member — International Conference on Computer-Aided Verification (CAV2019), Artifact Evaluation, 2018

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

Student PC Member — IEEE Symposium on Security and Privacy (IEEE S&P), 2016

Student PC Member — European Conference on Computer Systems (EuroSys), 2016

Reviewer — ACM Asia Conference on Computer and Communications Security (ASIACCS), 2016

Reviewer — ACM Conference on Computer and Communications Security (CCS), 2015

Co-Reviewer — IEEE Symposium on Security and Privacy (IEEE S&P), 2018

Co-Reviewer — International Symposium on Software Testing and Analysis (ISSTA), 2017

Co-Reviewer — IEEE Symposium on Security and Privacy (IEEE S&P), 2017

Co-Reviewer — International Conference on Automated Software Engineering (ASE), 2017

Co-Reviewer — IEEE Symposium on Security and Privacy (IEEE S&P), 2016

Co-Reviewer — International Conference on Automated Software Engineering (ASE), 2016

Co-Reviewer — The International Symposium on the Foundations of Software Engineering (FSE), 2016

Co-Reviewer — International Conference on Software Engineering (ICSE), 2016

Co-Reviewer	International Conference on Automated Software Engineering (ASE), 2015
Co-Reviewer	International Conference on Software Testing, Verification and Validation (ICST), 2015
Co-Reviewer	International Conference on Software Engineering (ICSE), 2015
Co-Reviewer	International Conference on Software Testing, Verification and Validation (ICST), 2014
Co-Reviewer	Working Conference on Mining Software Repositories (MSR), 2014
Co-Reviewer	International Symposium on Software Testing and Analysis (ISSTA), 2013
Co-Reviewer	International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA), 2013
Co-Reviewer	International Symposium on Software Testing and Analysis (ISSTA), 2012
Co-Reviewer	International Conference on Software Maintenance (ICSM), 2012
Co-Reviewer	International Conference on Automated Software Engineering (ASE), 2012

Teaching

UT Dallas

Fall 2019	CS/CE 3354, Software Engineering
Spring 2019	CS 6301, Machine Learning in Cyber Security
Fall 2018	CS 6332, Systems Security and Binary Code Analysis

UIUC (TA)

Fall 2014	CS 427, Software Engineering I
Spring 2012	CSC 333, Automata, Grammars, and Computability

NCSU (TA)

Spring 2012	CSC 379, Computer Ethics
Fall 2011	CSC/ECE 517, Object-Oriented Languages and Systems

Students

Graduate Students

Ph.D. Students	Mirazul Haque, Xiaodi Li, Simin Chen, Wasif Haque
M.S. Students	Kaiyuan Zhang, Anki Chauhan

Undergraduate Students

Since Fall 2017	Dean Lin, Sherry Wu, Xiang Li, Rittika Adhikary
Since Spring 2017	Ximin Lin, Evan N. Johnson, Chaeyun Jung
Spring 2017	Lucas J. Hsiung
Fall 2016	Jerry R. Guo

Honors and Awards

2016	Qualcomm Innovation Fellowship Finalist
2015–2018	Student Conferenceship Award: MVD 2015; RWC 2016; VMCAI 2016; POPL 2016; ACSAC 2017; AAAI 2018
2015	Best Pitch Award (Samsung Innovation Jam)
2012–2018	Volunteer: CCS 2012; FSE 2012; POPL 2016; ASE 2017; AAAI 2018

References

Tao Xie
Professor
Dept. of Computer Science
University of Illinois
at Urbana-Champaign, USA
taoxie@illinois.edu
+1-217-244-5931

Carl A. Gunter
Professor
Dept. of Computer Science
University of Illinois
at Urbana-Champaign, USA
cgunter@illinois.edu
+1-217-244-1982

Mukul Prasad
Research Manager
Software Quality & Security Laboratory
Fujitsu Lab of America
Sunnyvale, USA
mukul.prasad@us.fujitsu.com
+1-408-503-4628

Chengxiang Zhai
Professor
Dept. of Computer Science
University of Illinois
at Urbana-Champaign, USA
czhai@illinois.edu
+1-217-244-4943

Dawn Song
Professor
Computer Science Division
University of California, Berkeley
Berkeley, USA
dawnsong.letters@gmail.com
+1-510-642-1042