Curriculum Vitae

Name : Yan Chen

Email: ychen@northwestern.edu **Web Page:** http://www.cs.northwestern.edu/~ychen

Education

Dec. 2003	Ph.D. degree in Computer Science, University of California at Berkeley. Advisor: Randy H. Katz, the United Microelectronics Corporation Distinguished Professor. Thesis title: *Towards a Scalable, Adaptive and Network-aware Content Distribution Network.*
May. 1998	M.S. degree in Computer Science, State University of New York at Stony Brook. Advisor: Arie E. Kaufman, Distinguished Professor. Thesis title: *Physically Based Volume Graphics Manipulations for Medical Applications.*
May 1995	Honored B.E. degree in Computer Engineering, Zhejiang University, P. R. China. Advisor: Jiaoying Shi, ex-Director of the National Lab of Computer Aided Design and Computer Graphics (CAD&CG). B. E. thesis title: *PVM-G: Parallel Graphics Design Environment.*

Positions, Training, and Experience

Sep. 2014 - Present	Professor, Department of Electrical Engineering and Computer Science, Northwestern University
Jan. 2011 – Present	Adjunct Professor, Institute of Computer Science, Zhejiang University, China.
Sep. 2009 – Aug. 2014	Associate Professor, Department of EECS, Northwestern University.
Dec. 2010 – Sep. 2011	Visiting Professor, Department of Computer Science and Technology, Tsinghua University, China.
Jan. 2004 – Aug. 2009	Assistant Professor, Department of EECS, Northwestern University.
June 2002 – Oct. 2002	AT&T Shannon Lab, Florham Park, NJ, Researcher Summer Intern. Developed research on network monitoring and anomaly detection on high-speed routers
May 1999 – Aug. 1999	Lumeria Inc., Berkeley CA, Software Engineer Summer Intern. Developed research on an XML based online transaction system.

Publications

Based on Google Scholar, my papers have been cited for over 9,000 times (h-index is 40).

Invited Book Chapters

1. Vaibhav Rastogi, Yan Chen and William Enck, "Automatic Security Analysis of Android Applications", invited book chapter for "Android Security and Mobile Cloud Computing", Springer, 2014.
2. Yao Zhao and Yan Chen, "Algebraic Approaches for Scalable End-to-End Monitoring and Diagnosis", invited book chapter for "Algorithms for Next Generation Network Architecture", Springer, 2009.

3. Yan Chen, “Content Replication”, invited book chapter for “Content Delivery Networks: Principles and Paradigms”, Springer, 2008.
4. Zhichun Li, Anup Goyal, and Yan Chen, “Honeynet-based Botnet Scan Traffic Analysis”, invited book chapter for “Botnet Detection: Countering the Largest Security Threat”, Springer, 2008.
5. Ehab Al-Shaer and Yan Chen, Integrated Fault and Security Management, invited book chapter for “Information Assurance: Dependability and Security in Networked Systems”, Morgan Kaufmann Publishers, 2007.

Refereed Journal Publications

1. Xitao Wen, Kai Bu, Bo Yang, Yan Chen, Li Erran Li, Xiaolin Chen, Jianfeng Yang, Xue Leng, “RuleScope: Inspecting Forwarding Faults for Software-Defined Networking", to appear in *ACM/IEEE Transaction on Networking (ToN)*.
2. Kai Chen, Xitao Wen, Xingyu Ma, Yan Chen, Yong Xia, Chengchen Hu, Qunfeng Dong, Yongqiang Liu, “Towards A Scalable, Fault-Tolerant, High-Performance Optical Data Center Architecture", to appear in *ACM/IEEE Transaction on Networking (ToN)*.
3. Tiantian Zhu, Hongyu Gao, Yi Yang, Kai Bu, Yan Chen, Doug Downey, Kathy Lee, Alok Choudhary, “Beating the Artificial Chaos: Fighting OSN Spam Using Its Own Templates”, to appear in *ACM/IEEE Transaction on Networking (ToN)*.
4. Hongyu Gao, Vinod Yegneswaran, Jian Jiang, Yan Chen, Phil Porras, Shalini Ghosh, Haixin Duan, “Reexamining DNS From a Global Recursive Resolver Perspective”, in *ACM/IEEE Transaction on Networking (ToN)*, Vol 24, No. 1, pp. 43-57, 2016.
5. Shihong Zou, Xitao Wen, Kai Chen, Shan Huang, Yan Chen, Yongqiang Liu, Yong Xia, Chengchen Hu, “VirtualKnotter: Online virtual machine shuffling for congestion resolving in virtualized datacenter”, in *Journal of Computer Networks*, Vol 67, pp. 141-153, 2014
6. Vaibhav Rastogi, Yan Chen, and Xuxian Jiang, "Catch Me If You Can: DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks", to appear in *IEEE Transactions on Information Forensics & Security*, Vol 9, No.1, pp. 99-108. 2014.
7. Gao Xia, Zhichun Li, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Junchen Jiang, and Yuezhou Lv, “Massive Semantics-based Vulnerability Signature Matching for High-speed Networks”, to appear in *ACM/IEEE Transaction on Networking (ToN)*, 2014.
8. Kai Chen, David Choffnes, Rahul Potharaju, Yan Chen, Fabian Bustamante, Dan Pei, Yao Zhao, “Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes From P2P Users”, in *IEEE Transactions on Computers (TC)*, Vol. 63, No. 4, pp. 1021-1036, 2014.
9. Chengchen Hu, Bin Liu, Hongbo Zhao, Kai Chen, Yan Chen, and Yu Cheng, "Discount Counting for Fast Flow Statistics on Flow Size and Flow Volume", in *ACM/IEEE Transaction on Networking (ToN)*,Vol. 22, No. 3, pp. 970-981, 2014.
10. Kai Chen, Ankit Singla, Atul Singh, Kishore Ramachandran, Lei Xu, Yueping Zhang, Xitao Wen, Yan Chen, “OSA: An Optical Switching Architecture for Data Center Networks with Unprecedented Flexibility”, in *ACM/IEEE Transaction on Networking (ToN)*, Vol. 22, Number 2, pp. 498-511, 2014.
11. Yao Zhao, Yinzhi Cao, Yan Chen, Ming Zhang, and Anup Goyal, "Rake: Semantics Assisted Network-based Tracing Framework”, in *IEEE Transactions on Network and Service Management*, Vol. 9, No. 4, 2012.
12. Chengchen Hu, Kai Chen, Yan Chen, Gao Xia, Bin Liu, Thanos Vasilakos, "A Measurement Study on Potential Inter-Domain Routing Diversity", in *IEEE Transactions on Network and*

Service Management, Vol. 9, No. 3, pp. 268-278, 2012.
13. Chengchen Hu, Bin Liu, Sheng Wang, Jia Tian, Yu Cheng, and Yan Chen, "Adaptive Non-Linear Sampling Method for Accurate Flow Size Measurement", in *IEEE Transactions on Communications*, Vol. 60, No. 3, pp. 789-798, 2011.
14. Kai Chen, Chuanxiong Guo, Haitao Wu, Jing Yuan, Zhenqian Feng, Yan Chen, Songwu Lu, Wenfei Wu, "DAC: Generic and Automatic Address Configuration for Data Center Networks", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 20, No. 1, 2012.
15. Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang and Yan Chen, "Security Issues in Online Social Networks", in *IEEE Internet Computing*, Volume 15, No. 4, July/August, 2011, pp. 56-63.
16. Kai Chen, Chengchen Hu, Xin Zhang, Kai Zheng, Yan Chen, and Athanasios V. Vasilakos, "Survey on Routing in Data Centers: Insights and Future", in *IEEE Network magazine - Special Issue on Cloud Computing*, Volume 25, No. 4, July/August 2011, pp. 6-10.
17. Zhichun Li, Anup Goyal, Yan Chen, and Vern Paxson, "Towards Situational Awareness of Large-scale Botnet Probing", in *IEEE Transactions on Information Forensics & Security*, Vol. 6, Issue 1, pp. 175-188, 2011.
18. Zhichun Li, Yan Gao, and Yan Chen, "HiFIND, a High-speed Flow-level Intrusion Detection Approach with DoS Resiliency", in *Journal of Computer Networks*, Volume 54, Issue 8, 2010.
19. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, Chi Yin Cheung, and Xing Li, "POPI: A User-level Tool for Inferring Router Packet Forwarding Priority", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 18, Issue 1, Feb. 2010.
20. Lanjia Wang, Zhichun Li, Yan Chen, Zhi (Judy) Fu and Xing Li, "Thwarting Zero-day Polymorphic Worms with Network-level Length-based Signature Generation," in *ACM/IEEE Transaction on Networking (ToN)*, Volume 18, Issue 1, Feb. 2010.
21. Yao Zhao, Yan Chen, and David Bindel, "Towards Unbiased End-to-End Network Diagnosis", *ACM/IEEE Transaction on Networking (ToN)*, Volume 17, Issue 6 (December 2009), Pages: 1724-1737.
22. Yao Zhao and Yan Chen, "FAD and SPA: End-to-end Link-level Loss Rate Inference without Infrastructure", in the *Journal of Computer Networks*, Volume 53, Issue 9, June 2009, pp1303-1318.
23. Leiwen Deng, Yan Gao, Yan Chen and Aleksandar Kuzmanovic, "Pollution Attacks and Defenses for Internet Caching Systems", *Journal of Computer Networks*. Volume 52, Number 5, April, 2008, pp 935-956.
24. Robert Schweller, Zhichun Li, Yan Chen, Yan Gao, A. Gupta, Y. Zhang, P. Dinda, Ming-Yang Kao, and G. Memik, "Flow-level High-speed Network Monitoring with Reversible Sketches", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 15, Issue 5, Oct. 2007.
25. Yan Chen, David Bindel, H. Song, and R. Katz, "Algebra-based Scalable Overlay Network Monitoring: Algorithms, Evaluation, and Applications", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 15, Issue 5, Oct. 2007.
26. Yao Zhao, Yan Chen, B. Li and Q. Zhang, "Hop ID: A Virtual Coordinate based Routing for Sparse Mobile Ad Hoc Networks", in *IEEE Transactions on Mobile Computing (TMC)*, Volume 6, Number 9, September 2007.
27. Pin Ren, Yan Gao, Zhichun Li, Yan Chen and Ben Watson, "IDGraphs: Intrusion Detection and Analysis Using Stream Compositing", invited paper for *IEEE Computer Graphics & Applications, special issue on Visualization for Cyber Security*, Volume 26, Number 2, March/April 2006.

28. Yan Chen, Lili Qiu, Wei Chen, Luan Nguyen, and Randy H. Katz, Efficient and Adaptive Web Replication using Content Clustering, *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Internet and WWW Measurement, Mapping, and Modeling*, Aug., 2003.
29. Yan Chen, Chris Overton, and Randy H. Katz, Internet Iso-bar: A Scalable Overlay Distance Monitoring System, in *Journal of Computer Resource Management*, Computer Measurement Group, Spring Edition, 2002.
30. Yan Chen, Khian Hao Lim, Chris Overton, and Randy H. Katz, On the Stability of Network Distance Estimation, in *ACM SIGMETRICS Performance Evaluation Review (PER)*, September issue, 2002.
31. Qinghong Zhu, Yan Chen, and Arie E. Kaufman, "Real-time Biomechanically-based Muscle Volume Deformation using FEM", *Journal of Computer Graphics Forum*, 1998, pp. C275-C284.

Refereed Conference Publications

(Acceptance rates provided when available. The average paper length is about 10 pages.)

1. Xiang Pan, Yinzhi Cao, Shuangping Liu, Yu Zhou, Yan Chen, Tingzhe Zhou, "CSPAutoGen: Black-box Enforcement of Content Security", in the Proc. of *ACM CCS*, 2016 (137/831=16.5%).
2. Zhengyang Qu, Guanyu Guo, Zhengyue Shao, Vaibhav Rastogi, Yan Chen, Hao Chen and Wangjun Hong, "AppShield: Enabling Multi-entity Access Control Cross Platforms for Mobile App Management", in the Proc. of *Securecomm* 2016 (32/137=23.3%).
3. Xitao Wen, Bo Yang, Yan Chen, Chengchen Hu, Yi Wang, Bin Liu, Xiaolin Chen, "SDNShield: Reconciliating Configurable Application Permissions for SDN App Markets", in the Proc. of *IEEE/IFIP DSN*, 2016 (58/259 = 22.4%)
4. Xitao Wen, Bo Yang, Yan Chen, Li Erran Li, Kai Bu, Peng Zheng, Yang Yang, Chengchen Hu, "RuleTris: Minimizing Rule Update Latency for TCAM-based SDN Switches", in the Proc. of *IEEE ICDCS*, 2016 (68/386 = 17.6%).
5. Kai Bu, Xitao Wen, Bo Yang, Yan Chen, Li Erran Li, Xiaolin Chen, "Is Every Flow on The Right Track?: Inspect SDN Forwarding with RuleScope", in the Proc. of *IEEE INFOCOM*, 2016 (300/1644=18%).
6. Vaibhav, Rastogi, Rui Shao, Yan Chen, Xiang Pan, Shihong Zou, and Ryan Riley, "Detecting Hidden Attacks via the Mobile Web-App Interface", in the Proc. of *NDSS*, 2016.
7. Vaibhav Rastogi, Zhengyang Qu, Jedidiah McClurg, Yinzhi Cao, and Yan Chen, "Uranine: Real-time Privacy Leakage Monitoring without System Modification for Android", in the Proc. of *International Conference on Security and Privacy in Communication Networks (SECURECOMM)*, 2015 (30/108=28%).
8. Yinzhi Cao, Xiang Pan, and Yan Chen, "SafePay: Protecting against Credit Card Forgery with Existing Magnetic Card Readers", in the Proc. of *the IEEE Conference on Communications and Network Security (CNS)*, 2015 (48/171=28%). [Won best paper award]
9. Boyuan He, Vaibhav Rastogi, Yinzhi Cao, Yan Chen, V.N. Venkatakrishnan, Runqing Yang and Zhenrui Zhang, "Vetting SSL Usage in Applications with SSLINT", in the Proc. of *IEEE Symposium on Security and Privacy (Oakland)*, 2015 (55/402=13.7%).
10. Kai Chen, Xitao Wen, Xingyu Ma, Yan Chen, Yong Xia, Qunfeng Dong, "WaveCube: A Scalable, Fault-Tolerant, High-Performance Optical Data Center Architecture", in the Proc. of *IEEE Infocom*, 2015 (316/1640=19%).
11. Xiang Pan, Yinzhi Cao, and Yan Chen, "I Do Not Know What You Visited Last Summer - Protecting users from third-party web tracking with TrackingFree browser", in the Proc. of *Internet Society NDSS Symposium*, 2015 (50/313 = 15.9%).
12. Yinzhi Cao, Yanick Fratantonio, Manuel Egele, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna, and Yan Chen, "EdgeMiner: Automatically Detecting Implicit Control Flow Transitions

through the Android Framework", in the Proc. of *Internet Society NDSS Symposium*, 2015 (50/313 = 15.9%).

13. Yinzhi Cao, Xiang Pan, Yan Chen and Jianwei Zhuge, “JShield: Towards Real-time and Vulnerability-based Detection of Polluted Drive-by Download Attacks”, in the Proc. of *Annual Computer Security Applications Conference (ACSAC)*, 2014 (19.9%).
14. Hongyu Gao, Yi Yang, Kai Bu, Yan Chen, Doug Downey, Kathy Lee, Alok Choudhary, “Spam ain't as Diverse as It Seems: Throttling OSN Spam with Templates Underneath”, in the Proc. of *Annual Computer Security Applications Conference (ACSAC)*, 2014 (19.9%).
15. Zhengyang Qu, Vaibhav Rastogi, Xinyi Zhang, Yan Chen, Tiantian Zhu and Zhong Chen, “AutoCog: Measuring the Description-to-permission Fidelity in Android Applications”, in the Proc. of ACM CCS, 2014 (114/585=19.5%).
16. Yinzhi Cao, Chao Yang, Vaibhav Rastogi, Yan Chen and Guofei Gu, “Abusing Browser Address Bar for Fun and Profit - An Empirical Investigation of Add-on Cross Site Scripting Attacks”, in 10th International Conference on Security and Privacy in Communication Networks (SecureComm), 2014.
17. Yinzhi Cao, Yan Shoshitaishviliz, Kevin Borgoltez, Christopher Kruegelz, Giovanni Vignaz, and Yan Chen, "Protecting Web-based Single Sign-on Protocols against Relying Party, Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel", in the Proc. of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2014 (22/113=19.5%).
18. Xitao Wen, Chunxiao Diao, Xun Zhao, Yan Chen, Erran Li, Bo Yang, and Kai Bu, “Compiling Minimum Incremental Update for Modular SDN Languages”, full paper with long presentation, in the Proc. of ACM SIGCOMM HotSDN Workshop, 2014 (16/114 = 15%).
19. Hongyu Gao, Vinod Yegneswaran, Yan Chen, Phil Porras, Shalini Ghosh, Jian Jiang, Haixin Duan, “An Empirical Reexamination of Global DNS Behavior”, in the Proc. of ACM SIGCOMM 2013 (38/240=15.8%).
20. Xitao Wen, Yan Chen, Chengchen Hu, Chao Shi, Yi Wang, "Towards A Secure Controller Platform for OpenFlow Applications", Short Paper, in the Proc. of ACM SIGCOMM HotSDN Workshop, 2013((24+16)/84=47.6%).
21. Yinzhi Cao, Vaibhav Rastogi, Zhichun Li, Yan Chen, and Alex Moshchuk, Redefining Web Browser Principals with a Configurable Origin Policy, in the Proc. of the IEEE/IFIP International Conference on Dependable Systems and Network - Dependable Computing and Communications Symposium (DSN - DCCS), 2013 (21/107=19.6%).
22. Vaibhav Rastogi, Yan Chen, and Xuxian Jiang, DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks , short paper, in the Proc. of *the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2013 ((35+26)/216=28.2%).
23. Vaibhav Rastogi, Yan Chen, and William Enck, "AppsPlayground: Automatic Large-scale Dynamic Analysis of Android Applications", in the Proc. of Third ACM Conference on Data and Application Security and Privcy (CODASPY), 2013 (24/107=22%).
24. Huichen Dai, Bin Liu, Yan Chen, and Yi Wang, "On Pending Interest Table in Named Data Networking", in the Proc. of *ACM Symposium on Architectures for Networking and Communications Systems (ANCS)*, 2012 (18/64=28%).
25. Xun Lu, Jianwei Zhuge, Ruoyu Wang, Yinzhi Cao, Yan Chen, “Deobfuscation and Detection of Malicious PDF Files with High Accuracy”, Digital Forensics MiniTrack, Proc. of *Hawaii International Conference on System Sciences* (*HICSS*) , 2012.

26. Xitao Wen, Kai Chen, Yan Chen, Yongqiang Liu, Yong Xia, and Chengchen Hu, "VirtualKnotter: Online Virtual Machine Shuffling for Congestion Resolving in Virtualized Datacenter", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
27. Yi Wang, Keqiang He, Huichen Dai, Wei Meng, Junchen Jiang, Bin Liu, and Yan Chen, "Scalable Name Lookup in NDN Using Effective Name Component Encoding", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
28. Xingyu Ma, Chengchen Hu, Kai Chen, Che Zhang, Hongtao Zhang, Kai Zheng, Yan Chen, and Xianda Sun, "Error Tolerant Address Configuration for Data Center Networks with Malfunctioning Devices", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
29. Yinzhi Cao, Zhichun Li, Vaibhav Rastogi, Xitao Wen, and Yan Chen, "Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security", in the Proc. of *ACM ASIACCS*, 2012 (30%)
30. Kai Chen, Ankit Singla, Atul Singh, Kishore Ramachandran, Lei Xu, Yueping Zhang, Xitao Wen, Yan Chen, "OSA: An Optical Switching Architecture for Data Center Networks with Unprecedented Flexibility", in the Proc. of *ACM/USNEIX NSDI*, 2012 (30/169=17.8%).
31. Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia and Alok Choudhary, "Towards Online Spam Filtering in Social Networks", in the Proc. Of *19th Network & Distributed System Security Symposium (NDSS)*, 2012 (46/258=17.8%).
32. Yinzhi Cao, Vinod Yegneswaran, Phillip Porras and Yan Chen, "PathCutter: Severing the Self-Propagation Path of XSS JavaScript Worms in Social Web Networks", to appear in the Proc. Of *19th Network & Distributed System Security Symposium (NDSS)*, 2012 (46/258=17.8%).
33. Yao Zhao, Yinzhi Cao, Anup Goyal, Yan Chen, and Ming Zhang, "Rake: Semantics Assisted Network-based Tracing Framework", in the Proc. of *IEEE/ACM IWQoS*, 2011 (23/80=28.8%).
34. Zhichun Li, Yi Tang, Yinzhi Cao, Vaibhav Rastogi, Yan Chen, Bin Liu, Clint Sbisa, "WebShield: Enabling Various Web Defense Techniques without Client Side Modifications", in the Proc. of *18th Network & Distributed System Security Symposium (NDSS*), 2011 (28/139=20%).
35. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y. Zhao, "Detecting and Characterizing Social Spam Campaigns", in the Proc. of *ACM SIGCOMM IMC*, 2010 (47/211=22.3%).
36. Zhichun Li, Gao Xia, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Junchen Jiang, and Yuezhou Lv, "NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks", in the Proc. of *ACM SIGCOMM*, 2010 (33/276=12%).
37. Kai Chen, Chuanxiong Guo, Haitao Wu, Jing Yuan, Zhenqian Feng, Yan Chen, Songwu Lu, Wenfei Wu, "Generic and Automatic Address Configuration for Data Center Networks", in the Proc. of *ACM SIGCOMM* 2010 (33/276=12%). **Selected as one of three best papers for fast track to ACM/IEEE ToN**.
38. Chengchen Hu, Bin Liu, Hongbo Zhao, Kai Chen and Yan Chen, "DISCO: Memory Efficient and Accurate Flow Statistics for Network Measurement", in the Proc. of *IEEE ICDCS*, 2010 (84/585=14.4%).
39. Zhichun Li, Ming Zhang, Zhaosheng Zhu, Yan Chen, Albert Greenberg, and Yi-Min Wang, "CloudProphet: Automating Performance Prediction for Cloud Services", in the Proc. of *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2010. (29/175=16.6%).
40. Zhichun Li, Anup Goyal, Yan Chen, and Aleksandar Kuzmanovic, "Measurement and Diagnosis of Address Misconfigured P2P Traffic", in the Proc. of *IEEE INFOCOM (main conference)*, 2010 (276/1575 = 17.5%).

41. Chengchen Hu, Kai Chen, Yan Chen and Bin Liu, “Evaluating Potential Routing Diversity for Internet Failure Recovery”, in the Proc. of *IEEE INFOCOM (mini conference)*, 2010 (276+106 /1575 = 24.3%)
42. Kai Chen, David R. Choffnes, Rahul Potharaju, Yan Chen, Fabian E. Bustamante, Dan Pei, Yao Zhao, “Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes From P2P Users”, in the Proc. of *the Fifth ACM International Conference on emerging Networking Experiments and Technologies (CoNEXT)*, 2009 (29/170=17%).
43. Kai Chen, Chengchen Hu, Wenwen Zhang, Yan Chen, Bin Liu, “On the Eyeshots of BGP Vantage Points”, in the Proc. of *IEEE Globecom Next Generation Network (NGN) Symposium*, 2009.
44. Zhaosheng Zhu, Vinod Yegneswaran, and Yan Chen, “Using Failure Information Analysis to Detect Enterprise Zombies,” in the Proc. of *the 5th International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2009 (19/75 =25.3%).
45. Yao Zhao, Sagar Vemuri, Jiazhen Chen, Yan Chen, Hai Zhou and Zhi (Judy) Fu, “Exception Triggered DoS Attacks on Wireless Networks”, in the Proc. of *the 39th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-DCCS)*, 2009 (37/177 = 21%).
46. Yao Zhao, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Chen, and Eliot Gillum, "BotGraph: Large Scale Spamming Botnet Detection", in the Proc. of *the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2009 (32/162=20%).
47. Yao Zhao, Zhaosheng Zhu, Yan Chen, Dan Pei, and Jia Wang, "Towards Efficient Large-Scale VPN Monitoring and Diagnosis under Operational Constraints", in the Proc. of *IEEE INFOCOM (main conference)*, 2009 (282/1435=20%).
48. Zhichun Li, Anup Goyal, Yan Chen, and Vern Paxson, “Automating Analysis of Large-Scale Botnet Probing Events”, in the Proc. of *ACM Symposium on Information, Computer and Communications Security (ASIACCS), full paper*, 2009 (33/147=22.4%).
49. Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, Keesook Han, "Botnet Research Survey," in the Proc. of *the 32nd Annual IEEE International Computer Software and Applications Conference*, 2008, pp.967-972.
50. Yao Zhao, Yan Chen, and Sylvia Ratnasamy, “Load balanced and Efficient Hierarchical Data-Centric Storage in Sensor Networks”, in the Proc. of *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, June 2008 (64/300=21.3%).
51. Chengchen Hu, Sheng Wang, Jia Tian, Bin Liu, Yu Cheng, and Yan Chen, "Accurate and Efficient Traffic Monitoring Using Adaptive Non-linear Sampling Method", in the Proc. of *IEEE INFOCOM*, 2008 (236/1160=20%).
52. Zhichun Li, Lanjia Wang, Yan Chen and Zhi Judy Fu, Network-based and Attack-resilient Length Signature Generation for Zero-day Polymorphic Worms, in Proc. of *the 15th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2007 (32/220=14%).
53. Yan Gao, Yao Zhao, Robert Schweller, Shobha Venkataraman, Yan Chen, Dawn Song, and Ming-Yang Kao, “Detecting Stealthy Spreaders Using Online Outdegree Histograms”, in Proc. of *15th IEEE International Workshop on Quality of Service (IWQoS)*, 2007 (17/64=26.6%).
54. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, Chi Yin Cheung, and Xing Li, “End-to-end Inference of Router Packet Forwarding Priority”, in Proc. of *IEEE Infocom* 2007 (252/1400=18%).
55. Yao Zhao and Yan Chen, “A Suite of Schemes for User-level Network Diagnosis without Infrastructure”, in Proc. of *IEEE Infocom* 2007 (252/1400=18%).
56. Yan Gao, Leiwen Deng, Aleksandar Kuzmanovic, and Yan Chen, “Internet Cache Pollution

Attacks and Countermeasures", in Proc. of *the 14th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2006 (33/232=14%).

57. Prasad Narayana, Ruiming Chen, Yao Zhao, Yan Chen, Zhi Fu, and Hai Zhou, "Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+", in Proc. of *the Second Workshop on Secure Network Protocols (NPSec)*, co-located with ICNP 2006 (7/21 = 33%).
58. Yao Zhao, Yan Chen, and David Bindel, "Towards Unbiased End-to-End Network Diagnosis", in Proc. of *ACM SIGCOMM*, 2006 (37/340=10%).
59. Zhichun Li, Yan Chen, and Aaron Beach, "Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing", in Proc. of *ACM SIGCOMM Workshop on Large-Scale Attack Defense*, 2006 (11/33=33%).
60. Yan Gao, Zhichun Li and Yan Chen, "A DoS Resilient Flow-level Intrusion Detection Approach for High-speed Networks", in Proc. of *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2006 (75/536=14%).
61. Yao Zhao, Yand Chen, and David Bindel, "Deterministic Overlay Diagnosis", poster paper, in Proc. of *ACM SIGMETRICS*, 2006 (30 full + 17 poster papers out of 217 (14-22%)).
62. Zhichun Li, Manan Sanghi, Brian Chavez, Yan Chen and Ming-Yang Kao, "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience", in Proc. of *IEEE Symposium on Security and Privacy*, 2006 (23/251=9%).
63. Robert Schweller, Zhichun Li, Yan Chen, Yan Gao, Anup Gupta, Yin Zhang, Peter Dinda, Ming-Yang Kao, and Goken Memik, "Reverse Hashing for High-speed Network Monitoring: Algorithms, Evaluation, and Applications", in the Proc. of *IEEE INFOCOM*, 2006 (252/1800=18%).
64. Yao Zhao, Bo Li, Qian Zhang, Yan Chen, and Wenwu Zhu, Efficient HopID based Routing for Sparse Ad Hoc Networks, Proc. of *the 13th IEEE International Conference on Network Protocols (ICNP)*, 2005 (36/212=17%).
65. Pin Ren, Yan Gao, Zhichun Li, Yan Chen, and Ben Watson, IDGraphs: Intrusion Detection and Analysis Using Histographs, Proc. of *the IEEE Workshop on Visualization for Computer Security (VizSEC)*, 2005.
66. Yan Chen, Zhichen Xu, and Chengxiang Zhai, A Scalable Semantic Indexing Framework for Peer-to-Peer Information Retrieval, Proc. of *ACM SIGIR Workshop on Heterogeininneous and Distributed Information Retrieval*, 2005.
67. Robert Schweller, Anup Gupta, Elliot Parsons, and Yan Chen, Reverse Hashing for Sketch-based Change Detection on High-speed Networks, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2004 (39/157 = 25%).
68. Yan Chen, David Bindel, Hanhee Song, and Randy H. Katz, An Algebraic Approach to Practical and Scalable Overlay Network Monitoring, Proceedings of *ACM SIGCOMM*, Aug. 2004 (31/340= 9%).
69. Yan Chen, David Bindel, and Randy H. Katz, Tomography-based Overlay Network Monitoring, poster in *ACM SIGCOMM*, 2003. Abstract of the poster in *ACM Computer Communication Review (CCR)*, Jan. 2004.
70. Yan Chen, David Bindel, and Randy H. Katz, Tomography-based Overlay Network Monitoring, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2003 (33/109=30%).
71. Bala Krishnamurthy, Subhabrata Sen, Yin Zhang, and Yan Chen, Sketch-based Change Detection: Methods, Evaluation, and Applications, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2003 (33/109=30%).

72. Yan Chen, Lili Qiu, Wei Chen, Luan Nguyen and Randy H. Katz, Clustering Web Content for Efficient Replication, Proceedings of *the 10th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2002.
73. Yan Chen, Randy H. Katz and John D. Kubiatowicz, SCAN: a Dynamic Scalable and Efficient Content Distribution Network, Proceedings of *the First International Conference on Pervasive Computing*, Zurich, Switzerland, Aug. 2002.
74. B. Raman, S. Agarwal, Yan Chen, M. Caesar, W. Cui, P. Johansson, K. Lai, T. Lavian, S. Machiraju, Z. M. Mao, G. Porter, T. Roscoe, M. Seshadri, J. Shih, K. Sklower, L. Subramanian, T. Suzuki, S. Zhuang, A. D. Joseph, Randy H. Katz, and I. Stoica, The SAHARA Model for Service Composition Across Multiple Providers, *invited paper*, Proceeding of *the First International Conference on Pervasive Computing*, Zurich, Switzerland, Aug. 2002.
75. Yan Chen, Randy H. Katz and John Kubiatowicz, "Dynamic Replica Placement for Scalable Content Delivery", Proceedings of *1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.
76. Yan Chen, Adam Bargteil, David Bindel, Randy H. Katz and John Kubiatowicz, "Quantifying Network Denial of Service: A Location Service Case Study, Proceeding of *the Third International Conference on Information and Communications Security (ICICS)*, Nov. 2001.
77. John Kubiatowicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishna Gummadi, Sean Rhea, Hakim Weatherspoon, Westley Weimer, Chris Wells, and Ben Zhao, "OceanStore: An Architecture for Global-Scale Persistent Storage", Proceedings of *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, Oct. 2000.
78. Yan Chen, Qinghong Zhu, and Arie Kaufman, "Physically-based Animation of Volumetric Objects", Proceeding of *IEEE Computer Animation*, 1998.

Patents

1. B. Krishnamurthy, S. Sen, Y. Zhang, and Yan Chen, "Sketch-based Change Detection in Massive Data Streams", U.S. Patent 7,751,325, awarded on July 6, 2010.
2. Yan Chen, Zhichun Li, Gao Xia and Bin Liu, "Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense," U.S. Patent 8,522,348, awarded on August 27, 2013.
3. Zhichun Li, Lanjia Wang, Yan Chen, and Zhi Fu, "Method and Apparatus to Facilitate Generating Worm-Detection Signatures Using Data Packet Field Lengths", filed on December 18, 2007. U.S. Patent Application No. 11/985,760.
4. Jia Wang, Yan Chen, Dan Pei, Yao Zhao, and Zhaosheng Zhu, "Towards Efficient Large-Scale Network Monitoring and Diagnosis Under Operational Constraints", filed on January 2009. U.S. Patent Application No. 12/186,096.
5. Kai Chen, Xitao Wen, Yan Chen, Yong Xia, and Yongqiang Liu, "The Optical Architecture and Wavelength Allocation Methods for Optical Data Center Networks", filed on Sep. 13, 2012 in China, Patent Application No. 201210338781.6.
6. Yinzhi Cao, Xiang Pan, Yan Chen, Jianwei Zhuge, Xiaobin Qian, and Jian Fu, "De-obfuscation and Signature Matching Technologies for Detecting Malicious Code", filed on March 14, 2013, under U.S. Patent Application No. 61/786,200.
7. Yan Chen, Vaibhav Rastogi, Zhengyang Qu, and Jedidiah McClurg, "Real-time Privacy Leakage Detection and Prevention System without Operating System Modification for Mobile Operating Systems", filed on February 5, 2015. U.S. Patent Application No. 14/615,254.
8. Yan Chen, Zhengyang Qu, and Vaibhav Rastogi, "System and Method for Determining Description-to-permission Fidelity in Mobile Applications", filed on May 15, 2014. U.S. Patent Application No. 61/993,398.

9. Yan Chen, Xiang Pan, and Yang Hu, “System and Method for Full-screen Delay-aware Mobile Ads Display”, filed on October 23, 2015. U.S. Patent Application No. 62/245,645.

Software Artifacts

All the tools below are available at http://list.cs.northwestern.edu/projects.html except denoted otherwise.

- JShield -- Real-time and vulnerability-based detection of polluted drive-by download attacks. System **adopted by one of the biggest networking vendors, Huawei Inc**., in its high-end firewall product.
- DroidChamleon – a tool to evaluate the robustness of Android anti-malware apps against transformation attacks. Requested by several security companies such as Lookout, AVG, and McAfee and numerous researchers over the world.
- AppsPlayground -- a framework that automates dynamic analysis of Android applications. It integrates multiple components comprising different detection and automatic exploration techniques and is effective at detecting privacy leaks and malicious functionality in applications.
- DNS based malicious domain group detection system.
- Scavenger – A system for real-time online social network spam detections. It includes both syntactic based detection and semantic based detection.
- Social network spam campaign analysis data – released the largest social network spam analysis on the spam URLs.
- NetShield – a network intrusion detection/prevention system with massive vulnerability signatures. http://www.nshield.org/ with hundreds of download.
- Hamsa – A system for zero-day polymorphic worm signature generation. The download also includes test cases such as polymorphic engines. System released and used by researchers from numerous institutes such as Columbia Univ., UT Austin, Purdue Univ.,Georgia Tech, UC Davis, etc..
- TOM and LEND – A suite of tools for scalable overlay network monitoring and unbiased overlay network diagnosis.
- FAD – A tools for end user-based based network diagnosis without infrastructure.
- POPI – A tool for router packet forwarding priority inference from end hosts.
- Reversible Sketches – A suite of tools for online high-speed network traffic monitoring and anomaly/intrusion detection.
- CachePollution – Tools for novel DOS attacks on Web caches and the corresponding defense. http://www.cs.northwestern.edu/~drc915/webBrowsPerf/

Grants (total grants $12,598,515, my share $4,392,592, no pure equipment grant)

1. “MARPLE: Mitigating APT Damage by Reasoning with Provenance in Large Enterprise Networks”, DARPA Transparent Computing grant, 7/2015-6/2019, joint grant with IBM, Stony Brook University and UIC, single PI for Northwestern, $6,000,000 (my share $1,000,000)
2. “TWC: TTP Option: Medium: Collaborative: Identifying and Mitigating Trust Violations in the Smartphone Ecosystem", NSF TWC Award, 10/2014-9/2018, joint grant with UCSB, single PI for Northwestern University, $1,600,000 (my share $533,200).
3. “Securing Information Flow of Android Apps without Firmware Modification”, Qatar National Research Fund, co-PI, (PI: Ryan Riley of Qatar University), 9/2013-8/2016, $1,014,736 (my share $352,363).
4. “Automatic Security Analysis of Android Applications”, Extension Grant for Book Chapter Contribution, Air Force Research Lab Information Institute, 8/2013, $12,000.
5. “NeTS: Small: WaveCube: A Scalable, Fault-Tolerant, High- Performance Optical Data Center Architecture”, NSF NeTS Award, single PI, 8/2012-7/2015, $400,000.

6. “Malicious Javascript Detection with Web Sandbox”, Huawei Technology Inc., $216,000, single PI, 3/2012-6/2013.
7. “Integrated Agent-based Cyber Behavior Anomaly Detection and Analysis Approach for Enterprise Networks and Workstations”, DoD SBIR Award, subcontractor of Intelligent Automation Inc., Phase I (4/2010-3/2011), $9,000 and Phase II (4/2011-3/2013), $60,000 (total award $150K for phase I and $750K for phase II).
8. “NeTS: Small: Parallax -- Leveraging the Perspective of Ten Million Peers”, NSF NeTS Award, co-PI (PI Fabian Bustamante), 9/2009 – 8/2012, $500,000 (my share $250,000).
9. “CT-ISG: High-Speed Network Defense with Massive and Diverse Vulnerability Signatures”, NSF CyberTrust Award, single PI, 9/2008 – 8/2011, $400,000.
10. “RTFM: Network Penetration and Security Course Development”, Walter P. Murphy Society Grant, Northwestern University, single PI, 9/2007 - 8/2008, $15,000.
11. "Intrusion Detection and Forensics for Self-defending Wireless Networks", Air Force of Scientific Research (AFOSR) Young Investigator Award, single PI, 12/2006 - 11/2009, $368,326.
12. “CT-ISG: Router-Based Signature Generation for Zero-Day Polymorphic Worms”, NSF CyberTrust Award, PI, (co-PI Ming-Yang Kao), 9/2006 – 8/2009, $200,000 (my share $100,000).
13. “CT-ISG: Pollution Resilience for Internet Caches”, NSF CyberTrust Award, co-PI, (PI Aleksandar Kuzmanovic), 9/2006 – 8/2009, $350,000 (my share $175,000).
14. “HPNAIDM: The High-Performance Network Anomaly/Intrusion Detection and Mitigation System”, DOE Early Career Award, single PI, 8/2005-8/2008, $296,980.
15. Microsoft Research Trustworthy Computing Award 2006, PI, (co-PIs: Fabian Bustamante, Peter Dinda and Aleksandar Kuzmanovic), 9/2006-8/2007, $50,000 (my share $25,000).
16. "Information and Communication Security Curriculum Development – Phase II: National Accreditation", Walter P. Murphy Society Grant, Northwestern University, single PI, 9/2005 - 8/2006, $13,393.
17. “A Virtual Lab for Experimental Systems Education”, Walter P. Murphy Society Grant, Northwestern University, co-PI, (PI: Fabian Bustamante, Other co-PIs: Brian Dennis, Peter Dinda, and Aleksandar Kuzmanovic), $35,750, 9/2005 - 8/2006.
18. "Adaptive Intrusion Detection and Mitigation Systems for WiMAX Networks", Northwestern-Motorola Center for Telecommunications, PI (co-PI Hai Zhou), 9/2005-8/2007, $150,000 (my share $110,000)
19. Microsoft Research Trustworthy Computing Award 2005, PI (co-PI: Andrea Matwyshyn), 9/2005-8/2006, $50,000 (my share $30,000)
20. “Information and Communication Security Curriculum Development”, Walter P. Murphy Society Grant, Northwestern University, single PI, 09/01/2004 to 08/31/2005, $26,330.

Honors

- Fellow of IEEE, 2017
- Best Paper Runner Up, IEEE ICDCS, 2016
- Best Paper Award, the IEEE International Conference on Networking Security (CNS), 2015.
- Recognition of Service Award, by ACM SIGSAC (Special Interest Group on Security, Audit and Control), Oct. 2011
- Won the Best Paper Nomination in ACM SIGCOMM 2010 and fast track publication to ACM/IEEE Transaction on Networking (ToN)
- Selected to Attend the University Leadership Program offered by the Kellogg School of Management, 2009
- DoD (Air Force of Scientific Research) Young Investigator Award, 2007
- Department of Energy (DOE) Early CAREER Award, 2005

- Microsoft Trustworthy Computing Awards, 2004 (with Andrea M. Matwyshyn) and 2005 (with Fabian Bustamante, Peter Dinda and Aleksandar Kuzmanovic)
- AGEP Professor, Midwest Crossroads AGEP (Alliances for Graduate Education and the Professoriate) - a partnership of Northwestern, Indiana and Purdue University to increase minority participation in graduate studies and academia, 2005
- Searle Junior Fellow, Northwestern University, 2004

Synergistic Activities

- Associate Editor, ACM/IEEE Transaction on Networking (ToN), 2014 – present.
- Associate Editor, ZTE Communications, 2016 – present.
- Area TPC Chair, the IEEE Conference on Communications and Network Security (CNS), 2013, 2015, 2016.
- Founding Editorial Board (EB) of ICST Transactions on Security and Safety, 2009 – 2015.
- TPC Co-Chair, the IEEE Conference on Communications and Network Security (CNS), 2014.
- Area TPC Chair, the IEEE International Conference on Networking Protocols (ICNP), 2014.
- Local Co-Chair, ACM SIGCOMM 2014.
- Member of the Illinois Governor Pat Quinn's Internet Privacy Task Force, 2012 – present.
- TPC Co-Chair, the first International Workshop on the Security of Embedded Systems and Smartphones (co-located with ASIACCS) 2013.
- Vice Chair of World Wide Web conference in charge of the "Security, Privacy, Trust, and Abuse" track, 2012.
- General Chair, the 18th ACM Conference on Computer and Communication Security (CCS), 2011.
- Poster Co-chair, the 41st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2011.
- Steering Committee member, the IEEE International Workshop on Quality of Service (IWQoS), 2007 – 2010.
- TPC Co-Chair, the Next Generation Networking Symposium (NGN) of the IEEE GLOBECOM 2010.
- TPC Co-Chair, the 5th International Conference on Security and Privacy on Communication Networks (SecureComm) 2009.
- Local Arrangement Committee Chair, the ACM Conference on Computer and Communication Security (CCS), 2009 and 2010.
- Local Arrangement Committee Co-Chair, the ACM/USENIX Internet Measurement Conference (IMC) 2009.
- Organization and TPC Co-Chair, the 15th IEEE International Workshop on Quality of Service (IWQoS) 2007.
- TPC Member, ACM CCS 2014, 2015, 2016
- TPC member, IEEE ICDCS 2007, 2008, 2011, 2017.
- TPC member, World Wide Web Conference (WWW), 2014
- TPC member, IEEE Symposium on Security and Privacy (Oakland), 2013.
- TPC member, IEEE INFOCOM 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014.
- TPC member, Network & Distributed System Security Symposium (NDSS) 2010, 2011, 2012, 2014.
- TPC member, IEEE ICNP 2007, 2011, 2012, 2013.
- TPC member, IEEE Workshop on Mobile Security Technologies (MoST, co-located with Oakland), 2013.
- TPC member, IEEE Workshop on Secure Network Protocols (NPSec, co-located with IEEE ICNP), 2013.

- TPC member, International Conference on Security and Privacy on Communication Networks (SecureComm) 2008, 2011, 2015.
- TPC member, the 40th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2010.
- TPC member, IEEE ICPP 2009
- TPC member, IEEE International Workshop on Network Security and Privacy (NSP) 2008
- TPC member, IEEE International Conference on Broadband Communications, Networks, and Systems (BroadNets), 2008
- TPC member, IEEE International Conference on Sensors and Ad Hoc Communications and Networks (SECON) 2008
- TPC member, the IEEE International Workshop on Quality of Service (IWQoS), 2006, 2008-2010
- TPC member, ACM MobiCom 2007
- TPC member, IFIP/IEEE International Symposium on Integrated Management (IM) 2007
- TPC member, the International Conference on Mobile and Ad-hoc and Sensor Networks (MSN) 2006
- TPC member, IEEE GLOBECOM, 2006
- TPC member, ACM SIGCOMM Posters 2005, 2007
- TPC member, IADIS International Conference Applied Computing 2004, 2005
- NSF GENI panelist, 2008
- NSF CISE panelist for CAREER Program, 2008, 2009.
- NSF CISE panelist for CyberTrust Program, 2004, 2006, 2007, 2008, and 2009.
- Invited panelist for the Cyber Security Panel at the Transportation Center Advisory Board Committee meeting, Northwestern University, 2009
- Invited Reviewer for Qatar National Research Fund, 2011, 2014.
- Technology Reviewer for Hong Kong SAR Government ITS program proposals, 2009.
- Reviewer for AFOSR proposals, 2007, 2008, and 2009
- Reviewer for DOE SBIR/STTR proposals, 2006, 2007 and 2008
- Invited reviewer for the book “Internet Measurements” by Mark Crovella and Bala Krishnamurthy, John Wiley and Sons, Feb. 2005
- Invited reviewer for the book “Computer Networks and Data Communication” from Dr. Moshen Guizani, Wiley Publisher, Aug. 2004
- Invited reviewer for
    - IEEE Transactions on Information Forensics & Security 2012-2014, IEEE Transactions on Network and Service Management 2014, ACM Transaction on Information and System Security 2012-2013, ACM Computer Communication Review (CCR) 2012, ACM/IEEE Transaction on Networking (ToN) 2005, 2006, 2007-2013, IEEE Transaction on Mobile Computing 2009, IEEE Transaction for Parallel and Distributed Systems 2005, 2010-2013, ACM SIGCOMM CCR 2010, IEEE Transaction on Dependable and Secure Computing 2010.
    - Journal of Parallel and Distributed Computing 2008, IEEE Networks Special Issue on Implications and Control of Middleboxes in the Internet 2008, ACM Transaction on the Web (TWEB) 2007.
    - IEEE Networking magazine 2006, IEEE ICNP 2006, USNEIX Security Symposium 2006, SIGCOMM IMC 2006, IEEE Journal on Selected Areas in Communications (J-SAC) 2006, IEEE INFOCOM 2006, USENIX Security Symposium 2006, IEEE Wireless Communications Magazine 2005, IEEE Journal of Computer Networks 2005

- **Consulting Experience**
  - 2008 – 2013 Consultant for Intelligence Automation Inc., a technology innovation company that specializes in providing advanced technology solutions and R&D services to federal agencies, and corporations throughout the United States.
  - 2020 Consultant for G-Bar Limited Partnership, a startup on a cloud-based trading platform.

Teaching (All in Northwestern University)

- **EECS 213 Introduction to Computer Systems** (Fall 2006).
- **EECS 317 Data Management and Information Processing**, (Spring 2005).
- **EECS 340 Introduction to Computer Networking** (every other Winter, 2004-2014).
- **Developed EECS 350 Introduction to Computer Security** (Winter 2005 and Winter 2007).
- **Developed EECS 354 Network Penetration and Security** (every Fall, 2007 - present).
- **Developed EECS 450 Internet Security** (Spring 2004, Spring 2005, Spring 2007, Winter 2009, Spring 2010, 2012 - present).
- **Developed MSIT 458: Information and Security Assurance** (for a professional MS program in IT, Spring 2007, Spring 2008, and Spring 2009, every Winter or Fall 2010 - present).
- **Developed EECS 395/495 - Mobile Apps and Systems** (Spring 2015)
- **Developed EECS 395/495: Programming Language and Analysis for Security** (Spring 2013).
- **Developed EECS 395/495 Basic Information Security: Technology Business and Laws** (with Prof. Andrea M. Matwyshyn of Law School, for non-CS majors, Fall 2005).
- **Developed EECS 395/495: Internet Measurement and its Reverse Engineering** (Spring 2006).

Current Research Staff and Graduate Students

- Prof. Bin Liu (Adjunct Professor, from Tsinghua University, China)
- Prof. Junfeng Yang (Visiting scholar from Wuhan University, China)
- Haitao Xu (Research Assistant Professor)
- Xutong Chen (Ph.D. student)
- Xiang Pan (Ph.D. student)
- Zhenyang Qu (Ph.D. student)
- Libin Song (Ph.D. student)
- Boyuan He, Rui Shao, and Tiantian Zhu (Ph.D. students at Zhejiang University, China)
- Bo Yang, Guoyu Guo, and Zhenyue Shao (M.S. students at Zhejiang University, China)

Graduated Students

- Xitao Wen (Ph.D. 2016. First job: Software Engineer at Google)
  - Thesis title: On Efficient, Secure and Reliable Management of Software-Defined Networks
- Vaibhav Rastogi (Ph.D. 2015. First job: Postdocal Scientist at University of Wisconsin at Madison)
  - Thesis title: Towards a Trustworthy Android Ecosystem
- Yinzhi Cao (Ph.D. 2014, First job: Postdoctal Scientist at Columbia University, Now: Assistant Professor at Lehigh University)
  - Thesis title: Protecting Client Browsers with a Principal-based Approach
- Hongyu Gao (Ph.D. 2013, First job and Now: Software Engineer at Google)
  - Thesis title: Towards Online Heterogeneous Spam Detection and Mitigation for Online Social Networks
- Kai Chen (Ph.D. 2012. First job and Now: Assistant Professor at Hongkong University of Science and Technology)

    - Thesis title: Architecture Design and Management for Data Center Networks
- Zhichun Li (Ph.D. 2009. First job and Now: Reearcher at NEC Labs America)
    - Thesis title: Router-based Anomaly/Intrustion Detection and Mitigation Systems
- Yao Zhao (Ph. D., 2009. First job: Researcher at Bell Labs, Now: Shape Security)
    - Thesis title: Internet Networking and Application Troubleshooting.
    - Won the EECS Best Dissertation Award in Northwestern University
- Guohan Lv (Ph. D. of Tsinghua University China, 2008, co-advised with Prof. Xing Li at Tsinghua. First job: Associate Researcher at Microsoft Research Asia.)
    - Thesis title: Measurement-based Inference Techniques for TCP Throughput Diagnosis and Packet Forwarding Priority Discovery.

- Hongjun Wang (M. S. 2016, first employer: Facebook)
- Chao Shi (M. S. 2013, first employer: HP)
- Chenjin Liang (M.S. 2013, first employer: Amazon)
- Peng Xu (M. S. 2013)
- Clint Sbisa (M.S., 2011, first employer: Amazon)
- Kenny Tay (M. S., 2011, first employer: Microsoft)
- Rahul Potharaju (M.S. 2009, now at Purdue University)
    - Thesis title: Exploring More Complete AS Topologies for Internet Emergency Recovery
- Zhaosheng Zhu (M.S. 2009, now at Data Domain Inc.)
    - Thesis title: Using Failure Information Analysis to Detect Enterprise Zombies and Network Anomalies.
- Anup Goyal (M. S. 2009, first employer: Yahoo! Inc.)
    - Thesis title: Rake: Semantics Assisted Network-based Large Distributed System Diagnosis
- Jiazhen Chen (M. S. 2009, first employer: Morningstar Inc.)
    - Thesis title: Discovery and Countermeasures for Exception Triggered Attacks on Wireless Networks.
- Sagar Vemuri (M. S. 2008, first employer: Riverbed Technology.)
    - Thesis title: Error Message Based DoS Attacks on Wireless Networks
- Prasad Narayana (M. S. 2007, first employer: Nextwave Broadband Inc.)
    - Thesis title: Vulnerability Analysis of Wireless Network Protocols
- Yan Gao (M. S. 2007)
    - Thesis title: Online Scalable Intrusion Detection Systems for High-speed Networks
- Leon Zhao (M. S. 2006, first employer: Vibes Inc.)
    - Thesis title: Anomaly/Intrusion Detection on Wireless Networks.

Past visiting students and visiting scholars.

- Prof. Xiaolin Chen (visiting scholar from Chuxiong Normal University, China), 2014-2016
- Prof. Shihong Zou (visiting scholar from Beijing University of Post and Telecommunication, China), 2013
- Prof. Hao Tu (visiting scholar from Huazhong University of Science and Technology, China), 2012-2013
- Yusen Chen (from Zhejiang University, China), summer 2013
- Youfu Zhang (from Zhejiang University, China), summer 2013
- Xinyi Zhang (from Fudan University, China), summer 2013
- Jun Hu (from Huazhong University of Science and Technology, China), 2009-2011.
- Jin Yuan (from Tsinghua University, China) 2009-2010.

- Yi Tang (from Tsinghua University, China) 2008-2009.
- Chengchen Hu (from Tsinghua University, China), 2007.
- Gao Xia (from Tsinghua University, China), 2007.
- Ying He (from the Beihang University China), 2007-2008.
- Lanjia Wang (from Tsinghua University, China), 2006.
- Yanmei Zhang (from Chinese University of Finance and Economics), 2006-2007.

Invited Talks

- "Emerging Mobile Threats and Our Defense", Invited talk at Cyber Security Summit at Tsinghua University, at the West Lake Forum at Zhejiang University, at and at Jinan University, all at China, 2016.
- "Emerging Mobile Threats and Our Defense", Keynote speech at the Second International Conference of Young Computer Scientists, Engineers and Educators (ICYCSEE) August 2016.
- "Detecting Hidden Attacks via the App-Web Interface", Invited talk at the Internet Security Conference (ISC), Beijing, China, September 2015.
- "Towards a Trustworthy Android Ecosystem", Invited talk at Tencent Inc. and Huawei Inc., China, June 2015.
- "Towards a Trustworthy Android Ecosystem", Keynote speech at the 12th Annual Conference of National Computer network Emergency Response technical Team/Coordination Center of China (CNCERT/CC), May 2015.
- "Towards a Trustworthy Android Ecosystem", Invited talk at the Wuhan University, Huazhong University of Science and Technology (HUST), Central University of Finance and Economics (CUFE), China, May-June 2015
- "Towards a Trustyworthy SDN Ecosystem", Invited talk at the National Key Lab of Networking and Switching Technology, Beijing University of Post and Telecommunication (BUPT), July 2014.
- "Towards a Trustworthy Android Ecosystem", Invited talk at China Academy of Sciences (CAS), July 2014.
- "Towards a Trustyworthy SDN Ecosystem", Invited talk at the 27th IEEE Annual Computer Communications Workshop, Niagra Falls, NY, November 2013.
- "AppsPlayground: Automatic Security Analysis of Smartphone Applications", Invited talk at the Air Force Research Lab, Rome, NY, August 2013.
- "Towards a Trustworthy Android Ecosystems", Invited talk at Huawei Inc. and Chinese Academy of Sciences, China, July 2013.
- "Towards a Trustworthy Software Defined Networking (SDN) Ecosystems", Invited talk at West Lake Forum of Zhejiang University, China, June 2013.
- "Towards a Trustworthy Android Ecosystems", Invited talk at the Department of Computer Science, Illinois Institute of Technology, April 2013.
- "Intrusion Detection and Prevention for the Internet of Things", invited talk at the West Lake Forum of Zhejiang University, Hangzhou, China, March 2012.
- "Detecting and Characterizing Social Spam Campaigns", Invited lecture at NICO Seminar, Northwestern University, March 2012.
- "Intrusion Detection and Prevention for Emerging and Challenging Network Environments", invited talk at the Hong Kong Polytechnic University, National University of Defense Technology, and Xi'an Jiaotong University in China, July-August 2011.
- "NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks", invited talk at Tsinghua Information Forum, Tsinghua University, China, March 2011.
- "Detecting and Characterizing Social Spam Campaigns", invited talk at Toronto Networking Seminar Series, University of Toronto, Canada, February, 2011.

- "Configuring, Diagnosing, and Securing Data Center Networks and Systems", invited talk at the Institute of Computing Technology, Chinese Academy of Sciences, January, 2011.
- "NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense", invited talk at DIMACS Workshop on Network Data Streaming and Compressive Sensing, October 2010.
- "NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense", invited talk at Shanghai Jiaotong University, China, June 2010.
- "NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense", invited talk at University of Toronto Networking Seminar, October 2009.
- "NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense", invited talk at Juniper Networks Inc., July 2008.
- "Anomaly/Intrusion Detection and Prevention in Challenging Network Environments", Distinguished Lecture at Intelligent Automation, Inc., one of the top technology incubator company with over 10 million dollar annual grant from federal agencies, June 2008.
- "P2P Doctor: Measurement and Diagnosis of Misconfigured Peer-to-Peer Traffic", University of Toronto, January 2008.
- "P2P Doctor: Measurement and Diagnosis of Misconfigured Peer-to-Peer Traffic", TSS seminar at the Information Trust Institute, UIUC, December 2007.
- "Network-based Intrusion Detection, Prevention and Forensics System", Tsinghua University and Peking University, China, August 2007.
- "Vulnerability Analysis for WiMAX Networks", Microsoft Research Asia, August 2007.
- "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience", the School of Computer Science, Telecommunications and Information Systems, DePaul University, Jul. 2006.
- "IRC-based Botnet Detection on Routers", invited talk at ARO-DARPA-DHS workshop on Botnets, June 2006.
- "High-Performance Network Anomaly/Intrusion Detection and Mitigation Systems (HPNAIDM)", Honeywell, Mar. 2006.
- "Efficient HopID based Routing for Sparse Ad Hoc Networks", Honeywell, Mar. 2006.
- "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience", the Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, Feb. 2006.
- "Scalable and deterministic overlay network diagnosis", School of Computing, Georgia Institute of Technology, June, 2005.
- "Network Intrusion Detection and Mitigation", Motorola Labs, Schaumburg, IL, Feb. 2005.
- "Tomography-based Overlay Network Monitoring", ICIR (The ICSI Center for Internet Research), Berkeley, California, Sep. 2003.
- "Clustering Web Content for Efficient Replication", University of California at Davis, Dec. 2002.
- "SCAN: a Dynamic Scalable and Efficient Content Distribution Network", AT&T Labs - Research, Florham Park, NJ, Aug. 2002.
- "Wide-Area Network Measurement and Monitoring Services", Cisco Inc., Mountain View, California, Jul. 2001.
- "Wide-Area Network Measurement and Monitoring Services", Ericsson Research Lab at Berkeley, California, Jan. 2002.
- "Dynamic Replica Placement for Scalable Content Delivery", Ericsson Research Lab, Stockholm, Sweden, Jun. 2001.

Media Coverage

- My joint work with Xuxian Jiang of North Carolina State University on “DroidChameleon: Evaluating state-of-the-art Android anti-malware against transformation attacks”, was featured by the Wall Street Journal, Dark Reading, Information Week, The H Heise Security, Security Week, Slashdot, Help Net Security, ISS Source, EFY Times, Tech News Daily, Fudzilla, VirusFreePhone, McCormick Northwestern News, and ScienceDaily, 2013.
- As a member of the IL Cyber Task Force, I was invited to attend the Illinois Governor Pat Quinn’s Cyber Challenge Press Conference at James R. Thompson Center on April 1st, 2013.
- My joint work with Ben Zhao of UCSB resulted with the paper "*Detecting and Characterizing Social Spam Campaigns"*, was featured in the Wall Street Journal, INTERNET: Dissecting Facebook Spam, and MIT Technology Review, "Scrutinizing Facebook Spam", and ACM Tech News, 2010.
- Interviewed and featured in the article entitled “AFOSR-Supported YIP Research Leads to Algorithms That Deflect Network Attackers”, in Air Force Print News, October 18, 2010. http://www.wpafb.af.mil/news/story.asp?id=123226799
  Further selected in ACM TechNews, Oct. 25, 2010 (see the link below)
  http://technews.acm.org/archives.cfm?fo=2010-10-oct/oct-25-2010.html#488908
- Interviewed by Towers Productions, Inc. for an episode of *Investigative Reports* on the A&E Network, 2007. The program is about cybercrime/ computer security.
- “Getting their hands dirty – McCormick students find real solutions to today’s problems”, Fall 2005, McCormick By Design Magazine.

University Services

- Member of Advisory Board for the MSIT program in McCormick, 2012-present.
- Department representative to attend the McCormick Undergraduate Convocation, 2012.
- Director of Computer Science program for Weinberg School of Arts and Sciences, AY 2011-present.
- Member of the Computer Science Undergraduate Curriculum Committee, AY 2011.
- Chair of Computer Science Undergraduate Curriculum Committee, Member of Computing Facilities Committee, and Member of Computer Engineering Undergraduate Curriculum Committee for AY 09, Department of Electrical Engineering and Computer Science.
- Department representative to attend the Weinberg Undergraduate Convocation, 2009
- Chair of Computer Science Undergraduate Curriculum Committee, Member of Computing Facilities Committee, and Member of Computer Engineering Undergraduate Curriculum Committee for AY 08, Department of Electrical Engineering and Computer Science.
- Ph.D. Thesis Committee of Taghrid Samak (invited external member), Department of Computer Science, DePaul University, April. 2009.
- Department representative to attend the McCormick Undergraduate Convocation, 2008
- Member of the Graduate Committee, Member of the Computer Science Undergraduate Curriculum Committee and Member of Faculty Search Committee for AY 2007, Department of Electrical Engineering and Computer Science.
- Attend the demo and help evaluate a security product from Elemental Security for the Dean’s office, July 2006.
- Member of the Graduate Committee and Member of the Computer Science Undergraduate Curriculum Committee for AY 2006, Department of Electrical Engineering and Computer Science
- Attend the meeting with NUIT and Dean Jay Walsh to evaluate a NUIT-proposed security measures as well as its impact, July 2005.
- Chair of the Departmental Colloquia and Member of the Curriculum Committee for Academic Year 2005, Department of Computer Science

- Member of the Graduate Student Admission Committee and Member of the Curriculum Committee for Academic Year 2004, Department of Computer Science