

# ATUL PRAKASH

## Contact Information

2260 Hayward St  
4741 Beyster Building  
CSE Division, U. of Michigan  
Ann Arbor, MI 48109-2121  
Phone: (734) 763-1585

## Education

- Ph.D. in Computer Science, Dept. of EECS, University of California, Berkeley, 1989.
- M.S. in Computer Science, Dept. of EECS, University of California, Berkeley, 1984.
- B.Tech. in Electrical Engineering. Indian Institute of Technology, New Delhi, 1982.

## Professional Experience

**2001-present** University of Michigan, Ann Arbor. Professor. Currently serving as Richard N. Orenstein Division Chair of Computer Science and Engineering.

**09/17-02/18** Visiting Research Scientist, Google, Mountain View, CA.

**1995-2001** University of Michigan, Ann Arbor. Associate Professor, Computer Science Division, Department of EECS.

**5/99-6/99** Visiting Research Scientist, GMD-IPSI, Darmstadt, Germany.

**10/95-5/96** IBM T.J. Watson Research Center, Yorktown Heights, Visiting Research Scientist.

**1989-1995** University of Michigan. Assistant Professor, Computer Science Division, Department of EECS.

## Awards and Honors

- Best Paper Award, IEEE Cybersecurity Development Conference (SecDev), 2018.
- Outstanding Achievement Award, Department of EECS, University of Michigan, 2017 for innovative research in the design of secure systems and the leadership in the development of an undergraduate program in Data Science.

- Distinguished Practical Paper Award, IEEE Symposium on Security and Privacy (Oakland), 2016.
- ITR Award from the National Science Foundation, 2000.
- Inclusion of the the Upper Atmospheric Research Collaboratory project in the Smithsonian Permanent Collections and selection as one of the finalists in the 1998 Smithsonian/Computerworld award for the best Science project.
- Research Excellence Award, Department of EECS, University of Michigan, 1996-97.
- Irving and Lucille Smith Fellowship, Computer Science, University of California, Berkeley, 1988-89.
- Passed with distinction, Ph.D. thesis qualifying examination presentation, University of California, Berkeley, 1988.
- Honored for participating in the Centennial Issue of IEEE Computer, 1984.
- Regents Fellowship, University of California, 1983-84.
- Rajiv Bambawale Memorial Award for the best B.Tech. Electrical Engineering project, IIT Delhi, 1982.
- Merit Prizes, IIT Delhi, 1977, 78, 79, 80, 81 and 82.
- Merit Prize for 4<sup>th</sup> rank in the All India Joint Entrance Examination for admission to the five IITs (among approximately 100,000 students), 1977.
- Merit Scholarship, All India Board of Higher Secondary Education, 1977.

## **Publications**

### **Conference, Workshop, and Tech. Report Publications**

1. Haizhong Zheng, Xiaoyan Bai, Beidi Chen, Fan Lai, Atul Prakash: Learn To be Efficient: Build Structured Sparsity in Large Language Models. Advances in Neural Information Processing Systems (NeurIPS), 2024 (Spotlight).
2. Neal Mangaokar, Ashish Hooda, Jihye Choi, Shreyas Chandrashekar, Kassem Fawaz, Somesh Jha, Atul Prakash: PRP: Propagating Universal Perturbations to Attack Large Language Model Guard-Rails. ACL (1) 2024: 10960-10976.
3. Jiachen Sun, Haizhong Zheng, Qingzhao Zhang, Atul Prakash, Zhuoqing Mao, Chaowei Xiao: CALICO: Self-Supervised Camera-LiDAR Contrastive Pre-training for BEV Perception. ICLR 2024.

4. Leveraging Hierarchical Feature Sharing for Efficient Dataset Condensation [PDF] Haizhong Zheng, Jiachen Sun, Shutong Wu, Bhavya Kailkhura, Z. Morley Mao, Chaowei Xiao, Atul Prakash. European Conference on Computer Vision (ECCV), 2024.
5. Elisa Tsai, Ram S. Raman, Atul Prakash, and Roya Ensafi. Modeling and Detecting Internet Censorship Events. *Proc. NDSS*, 2024.
6. Ashish Hooda, Neal Mangaokar, Ryan Feng, Kassem Fawaz, Somesh Jha, Atul Prakash: D4: Detection of Adversarial Diffusion Deepfakes Using Disjoint Ensembles. *Proc. WACV 2024*: 3800-3810.
7. Shuowei Jin, Yongji Wu, Haizhong Zheng, Qingzhao Zhang, Matthew Lentz, Z. Morley Mao, Atul Prakash, Feng Qian, Danyang Zhuo: Adaptive Skeleton Graph Decoding. *CoRR abs/2402.12280* (2024).
8. Ryan Feng, Ashish Hooda, Neal Mangaokar, Kassem Fawaz, Somesh Jha, Atul Prakash: Stateful Defenses for Machine Learning Models Are Not Yet Secure Against Black-box Attacks. *Proc. ACM Computer and Communication Security (ACM CCS) 2023*: 786-800.
9. Haizhong Zheng, Rui Liu, Fan Lai, and Atul Prakash: Coverage-centric Coreset Selection for High Pruning Rates. *Proc. ICLR*, 2023.
10. Jihye Choi, Jayaram Raghuram, Ryan Feng, Jiefeng Chen, Somesh Jha, and Atul Prakash. Concept-based Explanations for Out-Of-Distribution Detectors. *Proc. ICML*, 2023, pp. 5817-5837.
11. Ryan Feng, Ashish Hooda, Neal Mangaokar, Kassem Fawaz, Somesh Jha, Atul Prakash: Investigating Stateful Defenses Against Black-Box Adversarial Examples. *CoRR abs/2303.06280* (2023).
12. Ashish Hooda, Neal Mangaokar, Ryan Feng, Kassem Fawaz, Somesh Jha, Atul Prakash: Theoretically Principled Trade-off for Stateful Defenses against Query-Based Black-Box Attacks. *CoRR abs/2307.16331* (2023)
13. Renuka Kumar, Apurva Virkud, Ram Sundara Raman, Atul Prakash, and Roya Ensafi. A Large-scale Investigation into Geodifferences in Mobile Apps. *USENIX Security Symposium*, 2022: 1203-1220.
14. Neal Mangaokar, Atul Prakash: Dispelling Misconceptions and Characterizing the Failings of Deepfake Detection. *IEEE Security & Privacy*, 20(2): 61-67 (2022).
15. Ashish Hooda, Neal Mangaokar, Ryan Feng, Kassem Fawaz, Somesh Jha, and Atul Prakash: Towards Adversarially Robust Deepfake Detection: An Ensemble Approach. *CoRR abs/2202.05687* (2022).
16. Sean Peisert, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benzel, Carl E. Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael: Perspectives on the SolarWinds Incident. *IEEE Security and Privacy Magazine* 19(2): 7-13 (2021).

17. Sanjay Kariyappa, Atul Prakash, Moinuddin K. Qureshi: MAZE: Data-Free Model Stealing Attack Using Zeroth-Order Gradient Estimation. CVPR 2021: 13814-13823.
18. Sanjay Kariyappa, Atul Prakash, Moinuddin K. Qureshi: Protecting DNNs from Theft using an Ensemble of Diverse Models. ICLR 2021.
19. Nelson Manohar-Alers, Ryan Feng, Sahib Singh, Jiguo Song, Atul Prakash: Using Anomaly Feature Vectors for Detecting, Classifying and Warning of Outlier Adversarial Examples. CoRR abs/2107.00561 (2021).
20. Tong, Liang, Minzhe Guo, Atul Prakash, and Yevgeniy Vorobeychik. "Towards Robustness against Unsuspicious Adversarial Examples." arXiv preprint arXiv:2005.04272 (2020).
21. Haizhong Zheng, Ziqi Zhang, Honglak Lee, and Atul Prakash. "Understanding and Diagnosing Vulnerability under Adversarial Attacks." arXiv preprint arXiv:2007.08716 (2020).
22. Renuka Kumar, Sreesh Kishore, Hao Lu and Atul Prakash, Security Analysis of Unified Payments Interface and Payment Apps in India, *Usenix Security Symposium*, August 2020.
23. Haizhong Zheng, Ziqi Zhang, Juncheng Gu, Honglak Lee, and Atul Prakash. "Efficient adversarial training with transferable adversarial examples." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1181-1190. 2020.
24. Pratik Vaishnavi, Kevin Eykholt, Atul Prakash and Amir Rahmati. "Transferable Adversarial Robustness using Adversarially Trained Autoencoders." ArXiv abs/1909.05921 (2019).
25. Pratik Vaishnavi, Tianji Cong, Kevin Eykholt, Atul Prakash and Amir Rahmati, Can Attention Masks Improve Adversarial Robustness?, *The AAAI-20 Workshop on Engineering Dependable and Secure Machine Learning Systems*, AAAI 2020, February 2020, Digital proceedings. Paper at: <https://drive.google.com/file/d/1ghHrzJxH7ASPoscf-Pcnv5ItHNcusZri/view>.
26. Feng, Ryan, Jiefeng Chen, Nelson Manohar, Earlence Fernandes, Somesh Jha, and Atul Prakash. "Query-Efficient Physical Hard-Label Attacks on Deep Learning Visual Classification." arXiv preprint arXiv:2002.07088 (2020).
27. Ryan Feng, Jiefeng Chen, Nelson R. Manohar, Earlence Fernandes, Somesh Jha, Atul Prakash: Query-Efficient Physical Hard-Label Attacks on Deep Learning Visual Classification. CoRR abs/2002.07088 (2020)
28. Haizhong Zheng, Earlence Fernandes, and Atul Prakash, Analyzing the Interpretability Robustness of Self-Explaining Models, Poster presentation at Workshop on Security and Privacy of Machine learning, ICML, 2019.
29. Brandon Carlson, Kevin Leach, Darko Marinov, Meiyappan Nagappan, Atul Prakash: Open Source Vulnerability Notification. *OSS 2019*: 12-23.
30. Davino Mauro Junior, Luis Melo, Harvey Lu, Marcelo d' Amorim and Atul Prakash, A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps, workshop paper, SafeThings 2019 Workshop in conjunction with IEEE Symposium on Security and Privacy, San Francisco, May 2019.

31. Kevin Eykholt, Swati Gupta, Atul Prakash, Amir Rahmati, Pratik Vaishnavi, and Haizhong Zheng. "Robust Classification using Robust Feature Augmentation." arXiv preprint arXiv:1905.10904 (2019).
32. Haizhong Zheng, Earlence Fernandes, Atul Prakash: Analyzing the Interpretability Robustness of Self-Explaining Models. CoRR abs/1905.12429 (2019).
33. Davino Mauro Jr., Luis Melo, Harvey Lu, Marcelo d'Amorim and Atul Prakash. "Beware of the App! On the Vulnerability Surface of Smart Devices through their Companion Apps." CoRR abs/1901.10062 (2019).
34. Davino Mauro Junior, Kiev Gama, Atul Prakash: Securing IoT Apps with Fine-grained Control of Information Flows. CoRR abs/1810.13367 (2018). Also appears at 18th Brazilian Symposium on Information and Computational Systems Security (SBSeg), October 2018.
35. Kevin Eykholt and Atul Prakash: Designing Adversarially Resilient Classifiers using Resilient Feature Engineering. CoRR abs/1812.06626 (2018).
36. Dawn Song, Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Florian Tramèr, Atul Prakash, Tadayoshi Kohno: Physical Adversarial Examples for Object Detectors. *WOOT @ USENIX Security Symposium*, 2018.
37. Amir Rahmati, Earlence Fernandes, Kevin Eykholt, Atul Prakash, Tyche: Risk-Based Permissions for Smart Home Platforms. *IEEE SECDEV*, Sept. 30th-Oct. 2nd, 2018. (Best Paper Award). Also see CoRR abs/1801.04609 (2018).
38. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Florian Tramèr, Atul Prakash, Tadayoshi Kohno, Dawn Song, Physical Adversarial Examples for Object Detectors. CoRR abs/1807.07769 (2018).
39. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, Dawn Song Robust Physical-World Attacks on Deep Learning Visual Classification *Proc. Computer Vision and Pattern Recognition (CVPR)*, 2018. Supersedes arXiv preprint 1707.08945, August 2017.
40. Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash: Decentralized Action Integrity for Trigger-Action IoT Platforms. *NDSS*, 2018.
41. Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash: Security Implications of Permission Models in Smart-Home Application Frameworks. *IEEE Security & Privacy* 15(2): 24-30 (2017).
42. Kevin Eykholt, Atul prakash, and Barzan Mozafari, Ensuring Authorized Updates in Multi-user Database-backed Applications, *Proc. of the Usenix Security Symposium*, pp. 1445-1460, Aug. 16-18th, 2017, Vancouver, Canada.
43. Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash, Securing Trigger-Action Platforms, In *2017 USENIX Summit on Hot Topics in Security (HotSec'17)*, Vancouver, BC, August 2017.

44. Earlence Fernandes, Amir Rahmati, Kevin Eykholt, Atul Prakash, Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?, In *IEEE Security & Privacy*, July 2017.
45. Alex Gyori, Earlence Fernandes, Amir Rahmati, Atul Prakash and Darko Marinov, "Support for Security and Safety of Programmable IoT Systems", presented at *ISSTA 2017 Workshop on Testing Embedded and Cyber-Physical Systems (TECPS'17)*. Santa Barbara, CA, July 2017.
46. Amir Rahmati, Earlence Fernandes, Kevin Eykholt, Xinheng Chen, and Atul Prakash, Heimdall: A Privacy-Respecting Implicit Preference Collection Framework, *The 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, Niagara Falls, NY, June 2017.
47. Y. Jia, Q. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. Mao, and A. Prakash. ContextIoT: Towards Providing Contextual Integrity to Applified IoT Platforms, *NDSS*, Feb. 2017.
48. Earlence Fernandes, Amir Rahmati, Kevin Eykholt, Atul Prakash: Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? CoRR abs/1705.08522 (2017).
49. Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash: Decoupled-IFTTT: Constraining Privilege in Trigger-Action Platforms for the Internet of Things. CoRR abs/1707.00405 (2017).
50. Ivan Evtimov, Kevin Eykholt, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, Amir Rahmati, Dawn Song: Robust Physical-World Attacks on Machine Learning Models. CoRR abs/1707.08945 (2017).
51. Amir Rahmati, Earlence Fernandes, Jaeyeon Jung, Atul Prakash: IFTTT vs. Zapier: A Comparative Study of Trigger-Action Programming Frameworks. CoRR abs/1709.02788 (2017).
52. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Dawn Song, Tadayoshi Kohno, Amir Rahmati, Atul Prakash, Florian Tramèr: Note on Attacking Object Detectors with Adversarial Stickers. CoRR abs/1712.08062 (2017).
53. Earlence Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, Atul Prakash. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks. *USENIX Security Symposium*, 2016, 531-548.
54. Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security Analysis of Emerging Smart Home Applications, *IEEE Symposium on Security and Privacy*, May 2016, 636-654. (Distinguished Practical Paper Award).
55. Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao and Atul Prakash. Android UI Deception Revisited: Attacks and Defenses, *Proceedings of 20th International Conference on Financial Cryptography and Data Security*, March 2016.

56. Justin Paupore, Earlence Fernandes, Atul Prakash, Sankardas Roy, and Xinming Ou, Practical Always-on Taint Tracking on Mobile Devices, *15th Workshop on Hot Topics in Operating Systems (HotOS)*, 2015.
57. Earlence Fernandes, Ajit Aluri, Alexander Crowell, and Atul Prakash, Decomposable Trust for Android Applications. *Proc. of 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015, pp. 343-354.
58. Jiaan Zeng, Guangchen Ruan, Alexander Crowell, Atul Prakash, and Beth Plale, Cloud computing data capsules for non-consumptive use of texts, *ScienceCloud'14, Proceedings of the 2014 International Workshop on Scientific Cloud Computing, Vancouver, BC, Canada, June 23-27, 2014*, pp. 9-16, 2014.
59. Mauro Conti, Earlence Fernandes, Justin Paupore, Atul Prakash, Daniel Simionato, OASIS: Operational Access Sandboxes for Information Security, *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, SPSM@CCS 2014, Scottsdale, AZ, USA, November 03 - 07, 2014*, pp. 105–110, 2014.
60. Beng Heng Ng and Atul Prakash, Let the Right One In: Discovering and Mitigating Permission Gaps, *Proc. Intl. Conf. on Information Security and Systems*, Kolkata, India, pp. 297-313, 2013.
61. Beng Heng Ng and Atul Prakash, Expose: Discovering Potential Binary Code Re-Use, *Proc. 37th IEEE Conference on Computers, Software, and Applications (COMPSAC)*, Kyoto, Japan, 2013.
62. Beng Heng Ng, Earlence Fernandes, Ajit Aluri, Jijiang James, and Atul Prakash, Beyond Instruction Level Taint Propagation, presented at *6th European Workshop on Systems Security (EuroSec'13)*, Prague, Czech Republic, April 2013.
63. Beng Heng Ng, Alexander Crowell, Atul Prakash: Adaptive semi-private email aliases. *Proc. of 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Seoul, Korea, 2012.
64. Yilan Zhang, Masahiro Kurata, Jerome P. Lynch, Gwendolyn Van Der Linden, Hassan Sadarat, and Atul Prakash. Distributed cyberinfrastructure tools for automated data processing of structural monitoring data. *Proceedings of SPIE - The International Society for Optical Engineering*, 8347, 2012.
65. Biswajit Panja, Atul Prakash, Priyanka Meharia, Bradley Schneider: Security in sensor network based SCADA system for adaptive traffic signal operation. *International Conference on Collaboration Technologies and Systems (CTS)*, 2012, 195-202.
66. Tzeng, HM, Yin, CY, Anderson, A, and Prakash, A (2012). Nursing staff's awareness of keeping beds in the lowest position to prevent falls and fall injuries in an adult acute surgical inpatient care setting. *MedSurg Nursing*, 21(5), 271–274.

67. Akula, M., Sandur, A., Kamat, V.R., and Prakash, A. (2012). "Context-Aware Computing Framework for Improved Bridge Inspections", Proceedings of the 2012 Construction Research Congress, American Society of Civil Engineers, Reston, VA, 698-707.
68. Heqing Huang, Su Zhang, Xinming Ou, Atul Prakash, and Karem Sakallah. 2011. Distilling critical attack graph surface iteratively through minimum-cost SAT solving. In *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC '11)*. ACM, New York, NY, USA, 31-40.
69. Mark W. Newman, Mark S. Ackerman, Jungwoo Kim, Atul Prakash, Zhenan Hong, Jacob Mandel, and Tao Dong. 2010. Bringing the field into the lab: supporting capture and replay of contextual data for the design of context-aware applications. In *Proceedings of the 23rd annual ACM symposium on User interface software and technology (UIST '10)*. ACM, New York, NY, USA, 105-108.
70. Mark S. Ackerman, Tao Dong, Scott Gifford, Jungwoo Kim, Mark W. Newman, Atul Prakash, Sarah Qidwai, David Garcia, Paulo Villegas, Alejandro Cadenas, Antonio Sanchez-Esguevillas, Javier Aguiar, B. Carro, Sean Mailander, Ronald Schroeter, Marcus Foth, Amiya Bhat-tacharya, and Partha Dasgupta. 2009. Location-Aware Computing, Virtual Networks. *IEEE Pervasive Computing*, Vol. 8, No. 4 (October 2009), 28-32.
71. Prakash, Atul, Ng, Beng Heng, Lau, Billy, and Kamat, Vineet (2009). "Dependable Opportunistic Communication in a Multi-Tier Sensor Network Architecture", Proceedings of the 2009 Workshop on Research Directions in Situational Self-managed Proactive Computing in Wireless Ad-Hoc Networks, Air Force Research Laboratory, St. Louis, MO.
72. Swati Gupta, Kristen LeFevre, and Atul Prakash. SPAN: a unified framework and toolkit for querying heterogeneous access policies. In *Proceedings of the 4th USENIX conference on Hot topics in security (HotSec'09)*, 2009, Usenix Association.
73. Kevin Borders, Eric Vander Weele, Billy Lau, and Atul Prakash. 2009. Protecting confidential data on personal computers with storage capsules. In Proceedings of the 18th conference on USENIX security symposium. USENIX Association, Berkeley, CA, USA, 367-382.
74. Kevin Borders and Atul Prakash. 2009. Quantifying Information Leaks in Outbound Web Traffic. In Proceedings of the 2009 30th IEEE Symposium on Security and Privacy (SP '09). IEEE Computer Society, Washington, DC, USA, 129-140.
75. Xin Zhao, Atul Prakash, and Kevin Borders. Prism: Providing flexible and fast filesystem cloning service for virtual servers, *Proc. of the 9th ACM/IFIP/USENIX International Conference on Middleware (Middleware 2008)*, Springer-Verlag, pp. 388-407.
76. Garrett Brown, Travis Howe, Michael Ihbe, Atul Prakash, and Kevin Borders. Social Networks and Context-Aware Spam, *Proc. of the ACM Conference on Computer-supported Cooperative Work*, Nov. 8-12, 2008.
77. Kevin Borders and Atul Prakash, Towards Quantification of Network-based Information Leaks via HTTP. *Proc. 3rd Usenix Workshop on Hot Topics in Security (HOTSEC)*, July 29, 2008, San Jose, CA.

78. Laura Falk, Atul Prakash, Kevin Borders, Analyzing Websites for User-visible Security Design Flaws, *Proc. Symposium on Usable Security and Privacy (SOUPS)*, July 23-25th, 2008.
79. Atul Prakash. Security in Practice: Security-Usability Chasm. *Proc. of Third International Conference on Information Systems Security (ICISS)*, December 2007. Invited paper.
80. Kevin Borders, Atul Prakash, and Mark Zielinski, Spector: Automatically Analyzing Shell Code. *Proc. of the 23rd Annual Computer Security Applications Conference (ACSAC '07)*, Dec. 2007, 501-513.
81. Kevin Borders and Atul Prakash, Securing Network Input via a Trusted Input Proxy. *Proceedings of the 2nd USENIX Workshop on Hot Topics in Security (HOTSEC '07)*, Aug. 2007.
82. Kevin Borders, Xin Zhao, and Atul Prakash, Sting: Detecting Evasive Malware (short paper), *IEEE Oakland Symposium on Security and Privacy*, 2006.
83. L. Opyrchal, A. Prakash, and A. Agrawal, Designing a Publish-Subscribe Substrate for Privacy/Security in Pervasive Environments, *Proc. of the 2006 ACS/IEEE International Conference on Pervasive Services*, June 26-29, 2006, pages 313-316.
84. Kevin Borders, Xin Zhao, and Atul Prakash, Sting: Detecting Evasive Malware (short paper), *IEEE Symposium on Security and Privacy*, 2006.
85. Xin Zhao and Atul Prakash. WSF: An HTTP-level firewall for hardening web servers. *The 17th IASTED International Conference on Parallel and Distributed Computing Systems*, Nov. 2005, Phoenix, AZ.
86. Xin Zhao, Kevin Borders, and Atul Prakash. SVGrid: a secure virtual environment for untrusted grid applications. *Proc. of the 3rd International workshop on Middleware for Grid Computing (MGC'05)*, Grenoble, France, 2005.
87. Kevin Borders, Xin Zhao, and Atul Prakash, CPOL: High-Performance Policy Evaluation. *Proc. of the 12th ACM Conference on Computer and Communications Security (CCS)*, 2005.
88. Kevin Borders and Atul Prakash, Web Tap: Detecting Covert Web Traffic. *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS)*, Oct. 2004, 110-120.
89. Lukasz Opyrchal, Atul Prakash, and Amit Agrawal, Designing a Publish-Subscribe Substrate for Privacy/Security in Pervasive Environments, presented at the *First Workshop on Pervasive Security (PSPT)*, Boston, MA, August 2004. (refereed, only electronic proceedings).
90. Xin Zhao and Atul Prakash. Source authentication in group communication systems. *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, Sept 2003. pp. 455 -459

91. James Irrer, Atul Prakash, and Patrick McDaniel. Antigone: policy-based secure group communication system and AMirD: antigone-based secure file mirroring system. *Proceedings of the DARPA Information Survivability Conference and Exposition*, Volume 2, April 22-24 2003, pp. 44-46.
92. P. McDaniel and A. Prakash, Methods and Limitations of Security Policy Reconciliation, *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, Oakland CA, pp. 73-87.
93. L. Opyrchal and A. Prakash, Secure Distribution of Events in Content-Based Publish Subscribe Systems, *Proceedings of the 2001 Usenix Security Symposium*, Washington D.C., August 2001.
94. Radu Litiu, Atul Prakash: DACIA: A Mobile Component Framework for Building Adaptive Distributed Applications. *Operating Systems Review* 35(2): 31-42 (2001)
95. P. McDaniel, A. Prakash, J. Irrer, S. Mittal, and T. Thuang, Flexibly Constructing Secure Groups in Antigone 2.0. In *Proceedings of DARPA Information Survivability Conference and Exposition II*. IEEE, June 2001.
96. Radu Litiu and Atul Prakash, Developing Adaptive Groupware Applications Using a Mobile Component Framework”, *the ACM 2000 Conference on Computer Supported Cooperative Work (CSCW 2000)*, Philadelphia, PA, December 2000, pp.
97. Radu Litiu, and Atul Prakash, ”DACIA: A Mobile Component Framework for Building Adaptive Distributed Applications”, *Principles of Distributed Computing (PODC) 2000 Middleware Symposium*, Portland, OR, July 2000; an earlier version appeared as Technical Report CSE-TR-416-99, Department of EECS, University of Michigan, Dec 1999.
98. P. McDaniel, A. Prakash, P. Honeyman, Antigone: A Flexible Framework for Secure Group Communication, *Proceedings of the 8th Usenix Security Symposium*, August 1999, Washington D.C., pp. 99-104.
99. L. Opyrchal and A. Prakash, Efficient Object Serialization in Java, *Workshop on Electronic Commerce and Web-based Applications/Middleware, 1999, at International IEEE Conference on Distributed Computing Systems (ICDCS)*, May-June 1999, pp. 96-101.
100. R. Litiu and A. Prakash, Stateful Multicast Services, *Proc. of the International IEEE Conference on Distributed Computing Systems (ICDCS)*, May-June 1999, pp. 82-89.
101. H.S. Shim and A. Prakash, Tolerating Client and Communication Failures in Distributed Groupware Systems, *Proc. of the IEEE Symposium on Reliable Distributed Systems (SRDS)*, Purdue, 1998, pp. 221-227.
102. R. Litiu and A. Prakash, Adaptive group communication services for groupware systems, *Proc. of the 2nd International Enterprise Distributed Object Computing Workshop*, 1998, IEEE Press, pp. 218-229.

103. H.S. Shim, R. Hall, A. Prakash, and F. Jahanian, Providing Flexible Services for Managing Shared State in Collaborative Systems, *Proc. of the European Conference on Computer-Supported Cooperative Work (ECSCW)*, September 1997, pp. 237-252.
104. B. Mirel, L.A. Olsen, A. Prakash, and E. Soloway, Improving Quality in Teaching Software Engineering through Emphasis on Communication, *Proc. of the 1997 Annual Conference of American Society for Engineering Education (ASEE)*, Milwaukee, Wisconsin, June 15-18, 1997.
105. R. Strom, G. Banavar, K. Miller, A. Prakash, and M. Ward, Concurrency Control and View Notification Algorithms for Collaborative Replicated Objects, *The 17th Proceedings of the International Conference on Distributed Computing Systems (ICDCS)*, Baltimore, MD, May 27-30, 1997, pp. 194-203.
106. Jang Ho Lee, Atul Prakash Trent Jaeger, and Gwobaw Wu Support ing Multi-User, Multi-Applet Workspaces in CBE, *The Proceedings of the Sixth ACM Conference on Computer-Supported Cooperative Work (CSCW)*, November 1996, pp. 344-353.
107. R. W. Hall, A. G. Mathur, F. Jahanian, A. Prakash, and C. Rasmussen, Corona: A Communication Service for Scalable, Reliable Group Collaboration Systems, *Proc. of the Sixth ACM Conference on Computer Supported Cooperative Work (CSCW)*, Boston, MA, November 1996, pp. 140-149.
108. Trent Jaeger, Aviel D. Rubin, and Atul Prakash. A system architecture for flexible control of downloaded executable content. *Proceedings of the Fifth International Workshop on Object Orientation in Operating Systems*, pages 14-18, Seattle, Wa., October 1996.
109. T. Jaeger, A.D. Rubin, and A. Prakash, Building Systems that Flexibly Control Downloaded Executable Content, *Proc. of the 6th USENIX UNIX Security Symposium*, July 22-25, San Jose, CA, pp. 131-148. (*Best Student Paper Award*).
110. A. G. Mathur and A. Prakash, A Protocol Composition-Based Approach to QoS Control in Collaboration Systems, in *Proc. Third IEEE International Conference on Multimedia Computing and Systems (CMCS)*, Hiroshima, Japan, June 1996, pp. 62-69.
111. N. R. Manohar and A. Prakash, A Flexible Architecture for Integrating Heterogeneous Replayable Workspaces, *Proc. Third IEEE International Conference on Multimedia Computing and Systems (CMCS)*, Japan, June 1996, pp. 274-278.
112. N. R. Manohar and A. Prakash, Dealing with timing variability in the playback of interactive session recordings *Proceedings of ACM Multimedia Conference 1995*, San Francisco, November 1995, pp. 45-56.
113. T. Jaeger and A. Prakash, Requirements of Role-based Access Control for Collaboration Systems, in *Proc. of the 1st ACM Workshop on Role-based Access Control (RBAC'95)*, Gaithersburg, MD, Nov. 1995.

114. N. R. Manohar and A. Prakash, The Session Capture and Replay Paradigm for Asynchronous Collaboration, *Proceedings of European Conference on Computer-supported Cooperative Work(ECSCW)*, Stockholm, Sweden, September 1995, pp. 149-164.
115. T. Jaeger and A. Prakash, Management and Utilization of Knowledge for the Improvement of Workflow Performance, *Proc. of the 1995 ACM Conference on Organizational Computing Systems (COOCS '95)*, Milpitas, CA, August 1995, pp. 32-43.
116. T. Jaeger and A. Prakash, Implementation of a Discretionary Access Control Model for Script-based Systems, *Proc. of the 8th IEEE Computer Security Foundations Workshop*, County Kerry, Ireland, June 1995, pp. 70-84.
117. T. Jaeger and A. Prakash, Representation and Adaptation of Organization Coordination Knowledge for Autonomous Agent Systems, *Proc. of the 7th International Conference on Software Engineering and Knowledge Engineering*, June 1995, pp. 103-105.
118. T. Jaeger and A. Prakash, Support for File System Security Requirements of Computational E-Mail Systems, *Proc. 2nd ACM Conference on Computer and Communications Security (CCCS)*, Fairfax, VA, ACM Press, November 1994, pp. 1-9.
119. S. Paul and A. Prakash, Object Data Models to Support Source Code Queries: Implementing SCA within REFINE, *1994 Proc. of the IEEE Third Workshop on Program Comprehension*, Washington D.C., November 1994, IEEE Computer Society Press, pp. 145-152.
120. T. Jaeger, A. Prakash, and M. Ishikawa, A Framework for Automatic Improvement of System Specifications to Meet Delivery Performance Goals, *Proc. Sixth IEEE Conference on Tools for AI*, New Orleans, November 1994, pp. 640-646.
121. A. Mathur and A. Prakash, Protocols for Integrated Audio and Shared Windows in Collaborative Systems, *Proc. ACM Multimedia 94*, October 1994, pp. 381-388.
122. A. Prakash and H. S. Shim, DistView: Support for Building Efficient Collaborative Applications using Replicated Active Objects, *Proc. Fifth ACM Conference on Computer-Supported Cooperative Work (CSCW)*, October 1994, pp. 153-164.
123. S. Paul and A. Prakash, Querying Source Code Using an Algebraic Query Language, *Proc. International Conference on Software Maintenance*, IEEE Press, September 1994, pp. 127-136.
124. S. Paul and A. Prakash, Generating Programming Language-based Pattern Matches, *Proc. of the 1993 Conference of the Center for Advanced Studies on Collaborative Research: Software Engineering - Volume 1*, IBM Press, October 1993, pp. 227-243.
125. T. Jaeger and A. Prakash, BizSpec: A Business-Oriented Model for System Specification and Generation, *The 5th International Conference on Software Engineering and Knowledge Engineering (SEKE)*, June 14-18, 1993, pp. 191-199.

126. S. Paul and A. Prakash, Source Code Retrieval Using Program Patterns, *IEEE CASE'92 (Fifth International Workshop on Computer-Aided Software Engineering)*, Montreal, July 1992, pp. 95-105.
127. A. Prakash and M.J. Knister, Undoing Actions in Collaborative Work, *Proc. of The Fourth ACM Conference on Computer-Supported Cooperative Work (CSCW)*, October 1992, Toronto, Canada, pp. 273-280.
128. A. Prakash and R. Subramanian, An Efficient Optimistic Distributed Simulation Scheme based on Conditional Knowledge, *Proc. of The Sixth Parallel and Distributed Simulation Workshop, 1992 SCS Western Multiconference*, Newport Beach, CA, January 1992, pp. 85-94.
129. S. Paul, A. Prakash, E. Buss, and J. Henshaw, Theories and Techniques of Program Understanding, *Proc. of the 1991 Conference of the Center for Advanced Studies on Collaborative Research*, IBM Press, Toronto, Canada, October 1991, pp. 37-54.
130. A. Prakash and R. Subramanian, Filter: An Algorithm for Reducing Cascaded Rollbacks in Optimistic Distributed Simulation, *Proc. of the 24th Annual Simulation Symposium, 1991 Simulation Multiconference*, New Orleans, April 1991, pp. 123-132.
131. M.J. Knister and A. Prakash, DistEdit: A Distributed Toolkit for Supporting Multiple Group Editors, *Proc. of the Third ACM Conference on Computer-Supported Cooperative Work*, Los Angeles, October 1990, pp. 343-355.
132. A. Prakash and C.V. Ramamoorthy, Hierarchical Distributed Simulations, *Proc. of the 8th International Conference on Distributed Computing Systems*, San Jose, IEEE Press, 1988, pp. 341-348.
133. Y.F. Chen, A. Prakash, and C.V. Ramamoorthy, Pulsating Computations, *Proc. of the International Computer Symposium*, Taiwan, December 1986, pp. 1107-1115.
134. Y.F. Chen, A. Prakash, and C.V. Ramamoorthy, The Network Event Manager, *Proc. of the Computer Networks Symposium*, Washington D.C., IEEE Press, November 1986, pp. 169-177.
135. C. V. Ramamoorthy, W.-T. Tsai, Y. Usuda, and A. Prakash, Genesis: An Integrated Environment for Development and Evolution of Software Systems, *Proc. of the 19th International Conference on Computer Software Applications*, Chicago, IEEE Press, November 1985, pp. 472-479.

## Journal Publications

1. Szu-Yun Lin, Andrew W. Hlynka, Lichao Xu, Hao Lu, Omar A. Sediek, Sherif El-Tawil, Vineet R. Kamat, Jason McCormick, Carol C. Menassa, Seymour M. J. Spence, Atul Prakash, Benigno Aguirre: Simple Run-Time Infrastructure (SRTI): An accessible distributed computing platform for interdisciplinary simulation. *J. Comput. Sci.* 55: 101455 (2021).

2. Zhang, Y., O'Connor, S., van der Linden, G., Prakash, A., and Lynch, J. (2016). "SenStore: A Scalable Cyberinfrastructure Platform for Implementation of Data-to-Decision Frameworks for Infrastructure Health Management." *Journal of Computing in Civil Engineering*, ASCE, Online publication date: February 2016.
3. Akula, M., Sandur, A., Kamat, V. R., and Prakash, A. Context-Aware Framework for Highway Bridge Inspections. *Journal of Computing in Civil Engineering*, 29(1), January 2015 (online publication: 19th Jan. 2013).
4. Crowell, A., Ng, B. H., Fernandes, E., and Prakash, A. (2013). The Confinement Problem: 40 Years Later. *Journal of Information Processing Systems*, 9(2), June 2013, pp. 189-204.
5. Tzeng, H. M., Prakash, A., Brehob, M., Anderson, A., Devacsery, D. A., and Yin, C. Y. (2013). How feasible was a bed-height alert system?. *Clinical nursing research*, 22(3), 300-309.
6. Sharad Sharma, Harpreet Singh, Atul Prakash. Multi-agent modeling and simulation of human behavior in aircraft evacuations. *IEEE Transactions on Aerospace and Electronic Systems*, Oct. 2008, Vol. 44, No. 4, pp. 1477-1488.
7. Xin Zhao, Kevin Borders, and Atul Prakash. Using a virtual machine to protect sensitive Grid resources. *Concurrency and Computation: Practice and Experience*. Special issue on Middleware for Grid Computing: A Possible Future. Vol. 19, No. 14, Sept. 2007, pages: 1917-1935.
8. Patrick McDaniel and Atul Prakash, Enforcing provisioning and authorization policy in the Antigone system, *Journal of Computer Security*. 14(6):483-511, 2006.
9. Patrick McDaniel and Atul Prakash, Methods and Limitations of Security Policy Reconciliation. *ACM Transactions on Information and System Security (TISSEC)*, Association for Computing Machinery, 9(3):259-291, August, 2006.
10. Trent Jaeger, Atul Prakash, Jochen Liedtke and Nayeem Islam, Flexible control of downloaded executable content, *ACM Transactions on Information and System Security*, Vol. 2, Issue 2, May 1999, pp. 177-228.
11. S. Subramanian, G.R. Malan, H.S. Shim, J.H. Lee, P. Knoop, T.E. Weymouth, F. Jahanian, A. Prakash, Software architecture for the UARC Web-based collaboratory, *IEEE Internet Computing*, Mar-Apr. 1999, Vol. 3, Issue 2, pp. 46-54.
12. A. Prakash, H.S. Shim, and J.H. Lee, Issues and Trade-offs in CSCW Systems, *IEEE Transactions on Data and Knowledge Engineering*, Jan.-Feb. 1999, Vol. 11, Issue 1, pp. 213-227.
13. G. Olson, D.E. Atkins, R. Clauer, T. Finholt, F. Jahanian, T.L. Killeen, A. Prakash, and T. Weymouth, The Upper Atmospheric Research Collaboratory, *ACM Interactions*, Vol. 3, May-June 1998, pp. 48-55.

14. R. Strom, G. Banavar, K. Miller, A. Prakash, and M. Ward, Concurrency Control and View Notification Algorithms for Collaborative Replicated Objects, *IEEE Transactions on Computers*, Vol. 47, No. 8, April 1998, pp. 458-471.
15. S. Paul and A. Prakash, A Query Algebra for Program Databases, *IEEE Transactions on Software Engineering*, Vol. 22, No. 1, March 1996, Vol. 22, No. 3, pp. 202-217.
16. R. Al-Zoubi and A. Prakash, Program View Generation and Change Analysis Using Attributed Dependency Graphs, *Journal of Software Maintenance — Research and Practice*, Volume 7, No. 4, July-August 1995.
17. A. Prakash and M. Knister, A Framework for Undoing Actions in Collaborative Systems, *ACM Transactions on Computer-Human Interaction*. December 1994.
18. C. R. Clauer, J. D. Kelly, T. J. Rosenberg, C. E. Rasmussen, P. Stauning, E. Friis-Christensen, R. J. Niciejewski, T. L. Killeen, S. B. Mende, Y. Zambre, T. E. Weymouth, A. Prakash, S. E. McDaniel, G. M. Olson, T. A. Finholt, and D. E. Atkins, A New Project to Support Scientific Collaboration Electronically, *EOS Trans. Amer. Geophys. Union*, Vol. 75, June 28, 1994.
19. E. Buss, R. De Mori, M. Gentleman, J. Henshaw, H. Johnson, K. Kontogiannis, E. Merlo, H. Muller, J. Mylopoulos, S. Paul, A. Prakash, M. Stanley, S. Tilley, J. Troster and K. Wong, Investigating Reverse Engineering Technologies: The CAS Program Understanding Project, *IBM Systems Journal*, Vol. 33, No. 3, August 1994, pp. 477-500.
20. S. Paul and A. Prakash, Supporting Queries on Source Code: A Formal Framework, *International Journal of Software Engineering and Knowledge Engineering* (Special Issue on Reverse Engineering), Vol. 4, No. 3, September 1994, pp. 325-348.
21. S. Paul and A. Prakash, Framework for Source Code Search Using Program Patterns, *IEEE Transactions on Software Engineering*, Volume 20, Number 6, June 1994, pp. 463-475.
22. C.R. Clauer, D.E. Atkins, T.E. Weymouth, G.M. Olson, R. Niciejewski, T. Finholt, A. Prakash, C.E. Rasmussen, T.J. Rosenberg, J.D. Kelly, Y. Zambre, P. Stauning, E. Friis-Christensen, and S.B. Mende, A Prototype Upper Atmospheric Research Collaboratory (UARC) (**Abstract**), *EOS, Transactions on American Geophysical Union*, Vol. 74, 1993.
23. M. Knister and A. Prakash, Issues in the Design of a Toolkit for Supporting Multiple Group Editors, *Computing Systems*, Journal of the Usenix Association, Vol. 6, No. 2, Spring 1993, pp. 135-166.
24. C.V. Ramamoorthy, Y. Usuda, A. Prakash, and W.T. Tsai, The Evolution Support Environment System, *IEEE Trans. on Software Engineering*, Vol. 16, No. 11, November 1990, pp. 1225-1234.
25. C.V. Ramamoorthy, V. Garg, and A. Prakash, Support for Reusability in Genesis, *IEEE Transactions in Software Engineering*, Vol 14, No. 8, August 1988, pp. 1145-1154.
26. C.V. Ramamoorthy, V. Garg, and A. Prakash, Programming in the Large, *IEEE Transactions on Software Engineering*, Vol. 12, No. 7, July 1986, pp. 769-783.

27. C. V. Ramamoorthy, A. Prakash, W.-T. Tsai, and Y. Usuda, Software Engineering: Status and Perspectives, *IEEE Computer*, Vol. 17, No. 10, October 1984, pp. 191-209.

## Keynote and Invited Conference Talks

1. Robust Physical-World Attacks on Deep Learning Visual Classifiers and Detectors, Keynote talk, 14th International Conference on Information Systems Security, Bengaluru, India, Dec. 2018.
2. Robust Physical-World Attacks on Deep Learning Visual Classifiers, ESCAR USA Conference (Embedded Security in Cars), Ypsilanti, June 21-22, 2018. Invited Talk.
3. Information Confinement in Commodity Systems, SecureComm Conference, 2012. Keynote talk.
4. Security in Practice: Security-Usability Chasm, Third International Conference on Information Systems Security, Kolkata, Dec. 2009. Keynote talk.

## Book Chapters

- Hyong-Sop Shim, Atul Prakash, and Jang Ho Lee. Distributed and Collaborative Development. *Wiley Encyclopedia of Computer Science and Engineering*, DOI: 10.1002/9780470050118.ecse118. John Wiley & Sons, Dec. 14, 2007.
- L. Opyrchal and A. Prakash, Publish Subscribe Middleware, Chapter in *Scalable Enterprise Systems: An Introduction to Recent Advances*, ed. V. Prabhu, S. Kumara, and M. Kamath, Kluwer Academic Publishers, July 2003.
- Atul Prakash, Group Editors, Chapter in *Trends in Computer-Supported Cooperative Work*, John Wiley & Sons. (Editor: M. Beaudouin-Lafon), 1998.
- C.R. Clauer, D.E. Atkins, T.E. Weymouth, G.M. Olson, R. Niciejewski, T.A. Finholt, A. Prakash, C.E. Rasmussen, T. Killeen, T.J. Rosenberg, D. Detrick, J.D. Kelly, Y. Zambre, C. Heinselman, P. Stauning, E. Friis-Christtensen, and S.B. Mende, A Prototype Atmospheric Research Collaboratory (UARC), in *Applications of Data Handling and Visualization Technique in Space Atmospheric Sciences*, E. Szuszczewicz (ed), NASA SP-519, pp. 105-112.
- C.V. Ramamoorthy, A. Prakash, V. Garg, T. Yamaura, and A. Bhide, Issues in the Development of Large, Distributed, and Reliable Software, *Advances in Computers*, Vol. 26, 1987, pp. 396-443.
- C. V. Ramamoorthy, A. Prakash, W.-T. Tsai and Y. Usuda, Software Reliability: Its Nature, Models, and Improvement Techniques, in *Theory of Reliability*, ed. A. Serra and R.E. Barlow, Proceedings of the International School of Physics "Enrico Fermi", North-Holland, 1986, pp. 287-320.

## Patents

- Patent #6,425,016 (and related patent #6,988,270) on System and method for providing collaborative replicated objects for synchronous groupware application.

## Recent Research Grants

- National Science Foundation, TWC: Small: Exposing and mitigation permission gaps, 09/01/2013-08/31/2016, \$488,744, PI.
- General Motors, Analyzing Apps for undesirable information flows, 09/15/2014-09/14/2016, \$157,400, PI
- University of Michigan/Shanghai Jiao Tong University joint grant, Adaption and Coordination Technology of Large Scale EV Charging and Variable Renewable Energy Based on Big Data and Electricity Network Reliability Analysis, 09/01/2016-08/31/2018, \$50,000, PI.
- Didi Labs, Making Machine Learning more Robust and Trustworthy, \$150,000, 09/01/2018-08/31/2019, PI.
- National Science Foundation, EAGER: USBRCCR: Collaborative: Lightweight Policy Enforcement of Information Flows in IoT Infrastructures, \$163,714, 09/01/2017-08/31/2020, PI.
- National Science Foundation, CPS: Synergy: Collaborative Research: Support for Security and Safety of Programmable IoT Systems, 01/01/2017-12/31/2020, \$447,912, PI.
- National Science Foundation, CRISP Type 2: Interdependencies in Community Resilience (ICoR): A Simulation Framework, 09/01/2016-08/31/2021, \$231,383 (Prakash's share), Senior personnel.
- DARPA, Enhancing ML Robustness Using Physical-world Constraints, \$199,590 (first year funding received so far), 12/01/2019-11/30/2023, co-PI.
- Ford, Robust decision-making in autonomous vehicles in the presence of adversarial sensor inputs, \$220,000, 05/01/2019-04/30/2021, PI.
- Cisco Systems, On the data efficiency of LLMs fine-tuning with RLHF, \$153,448.00, 11/01/2023-02/28/2024.
- National Science Foundation, Using Semantic Constraints towards Machine Learning Model Robustness, \$32,568.85. Subcontract from University of Washington, St. Louis, 09/01/2021-08/31/2023.
- National Science Foundation, EAGER: SaTC-EDU: Identifying Educational Conceptions and Challenges in Cybersecurity and AI, \$300,000. Role: PI (Joint grant with Emily Provost, Mark Guzdial, and Nicola Banovic). 09/01/2020-08/30/2024.
- OpenAI, Intelligent Assistants for Detecting Social Engineering Scams, \$120,000. Unrestricted gift.

# Selected Service

## University

- Chair, Computer Science and Engineering Division, 07/01/2024-present.
- Member, First-year Task Force ad hoc committee, College of Engineering, University of Michigan, Oct. 2023-April 2024.
- Freshmen faculty mentor, University of Michigan Mentorship Program, August 2023-April 2024.
- Senior Associate Chair, CSE Division, Fall 2020-06/30/2024.
- Member (ex-officio), Executive Committee, CSE Division, Fall 2020-present.
- Member, EECS Administrative Committee, Fall 2020-present.
- Member, Honors and Awards Committee, CSE Division, Fall 2020-present.
- Member, Lecturer Search Committee, Fall 2020-present.
- Chief Program Advisor, Data Science Undergraduate Program in Engineering, Winter 2017, 2018-2019, 2019-2020. Also member of the Data Science Program Committee.
- Member, Executive Committee, Computer Science and Engineering, 2018-19, 2019-2020.
- Chair, EECS Teaching Committee, Winter 2017.
- Chair, CSE Faculty Search Committee, 2015-17.
- Member, CSE Executive Committee, 2016-17.
- Chief program advisor, Data Science, College of Engineering, 2015-16.
- Member, Informatics Steering Committee, 2015.
- Chair, Data Science Program Committee, 2015-2016.
- Member, CSE Faculty Search Committee, 2014-2015.
- Co-lead, Design of undergraduate Data Science program, University of Michigan, 2012-2014.
- Director, Software Systems Lab, Fall 2012, Winter 2013.
- Chair, Informatics Steering Committee, Fall 2011-2013.
- Chair, CSE Internal Review Committee, Fall 2012, Winter 2013.
- Member, ad hoc committee on the Data Science Program, Winter 2013.

- Member, CSE Search Committee, Winter 2012.
- Undergraduate advisor, CS LS&A program, Fall 2012.
- Member, Committee for Redesigning CS LS&A Program, 2012.
- Member, Informatics Steering Committee, 2010.
- Undergraduate advisor, Informatics Program, 2010.
- Member, CSE Executive Committee, 2009
- Member, Steering Committee, Informatics Program, 2007-2009
- Undergraduate Advisor, Informatics Program, 2008-2009
- Director, Software systems lab, 2004-2007
- College undergraduate advisor, 2004-2005
- Computer engineering advisor, 2003-2004.
- Chair, EECS curriculum committee, 2002-2003.
- Member, College curriculum committee, 2002-2003.
- Member, EECS Executive Committee, 1998-2002.
- Member, CSE curriculum committee, 1998-2002.
- Member, EECS committee to examine reorganization of degree programs in EECS, 1999-2000.
- Director, Industrial Partners program of Computer Science and Engineering (IPoCSE), University of Michigan, March 1999-2001
- Graduate Student Advising, 1990-2009
- Marshall, Engineering Honors Convocation, Winter 2000.
- Member, reappointment committee for Sugih Jamin, 1999.
- Computer Engineering Undergraduate Advisor, 1996-1999.
- Help prepare ABET information for EECS 482 and EECS 380 in 1997 and 1999.
- Member, EECS Departmental Computing Organization Committee, 1998.
- Member, College ad-hoc committee to examine large enrollments in Computer Science Engineering, 1997-98.
- Chair, Reappointment Committee for Nandit Soparkar. 1996.

- Coordinator, Software Qualifying Examination, January 1997.
- Invited by Dan Atkins to help formulate the direction of the new School of Information, 1995.
- Member, CSE Curriculum Committee, 1994-1995. The work on the committee led to stream-lining of the CSE curriculum by eliminating outdated courses and revision of lower division courses.
- Member, CSE Graduate Committee, 1992-1995.
- Coordinator, Software Qualifying Examination, January 1993.
- Volunteer, EECS student lucheon, 1991
- Member, Faculty Search Committee, 1990.
- Founding member of the Software Systems Research Laboratory, Department of EECS, University of Michigan, 1989.
- Marshall, May 1989 commencement.

### **Selected Professional Service**

- Associate Editor, IEEE Security and Privacy Magazine, 2020-present.
- PC member, IEEE/IFIP Distributed Systems and Networks, 2020.
- PC member and Steering Committee member, International Conference on Information Systems Security, 2020.
- Served on NSF Panel, CPS program, 2019
- PC Co-Chair, SafeThings 2020 at IEEE Symposium on Security and Privacy, 2019.
- Member, Program Committee, IoTSec 2019.
- Served on NSF Panel, SaTC program, 2018.
- Member, Committee on C.V. Ramamoorthy Award Nomination, 2019
- PC member, IEEE/IFIP Distributed Systems and Networks, 2019.
- PC member and Steering Committee member, International Conference on Information Systems Security, 2019.
- PC Co-Chair, SafeThings 2018
- PC member, International Conference on Information Systems Security, 2018.
- PC member, International Conference on Information Systems Security, 2017.

- PC member, ACM CCS workshop on IoT security and privacy, 2017.
- PC member, IFIP/IEEE Dependable Systems and Networks, 2017.
- PC member, IFIP/IEEE Dependable Systems and Networks, 2016.
- PC member, SecureComm, 2015.
- PC and steering committee member, International Conference on Information Systems Security, 2015.
- PC member, Intl. Conf. on Security, Privacy, and Applied Cryptography Engineering, 2015.
- Program Co-chair, International Conference on Information Security and Systems, 2014.
- PC member, 1st Workshop on Cloud Security Auditing, 9th IEEE World Congress on Services, 2013.
- PC member, 9th International Conference on Information Systems Security, 2013.
- PC member, CRISIS 2013.
- Best paper awards committee Co-Chair, IEEE Symposium on Reliable Distributed Systems, 2012.
- PC member, IEEE PASSAT, 2012.
- Program committee and steering committee: Intl. Conference on Information Security and Systems, 2011.
- Best Paper Awards Committee Co-Chair, IEEE Symposium on Reliable Distributed Systems, 2011.
- Associate Editor, IEEE Transactions on Dependable Computing (2009-2012).
- PC member and Advisory committee: Collaborative Technology Systems, 2011.
- PC member: IEEE Intl. Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2011
- PC member, IEEE Symposium on Reliable Distributed Systems, 2011
- PC member: IEEE Intl. Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2010
- Program committee and steering committee: Intl. Conference on Information Security and Systems, 2010.
- Program Co-chair, IEEE Symp. of Reliable Distributed Systems (SRDS), 2010.
- PC member and Advisory committee: Collaborative Technology Systems, 2010.

- Program Co-chair, Intl. Conf. on Information Security and Systems, 2009.
- Editor, Information Systems Security, Proc. of Intl. Conf. on Information Security and Systems, Springer-Verlag, DOI 10.1007/978-3-642-10772-6, 2009.
- Best paper award committee co-chair, IEEE Symp. of Reliable Distributed Systems, 2009.
- PC member, SECRIPT 2009.
- PC member, PASSAT 2009
- PC member, CRIWG 2009.
- Program committee member, IEEE Oakland Symp. on Security and Privacy, 2008.
- Program committee member, SECRIPT 2008.
- Advisory committee member and program committee member, 2008 International Symposium on Collaborative Technologies and Systems.
- PC member, ICDCN, 2008.
- PC member, ICISS, 2008.
- PC Member, CRIWG 2008.
- PC member, IEEE Workshop on Specialized Ad Hoc Networks and Systems, 2007.
- PC member, SECRIPT, 2007.
- Committee member, International Symp. on Collaborative Technology and Systems, 2007.
- Reviwer, IEEE Transactions on Distributed Computing
- Reviewer, IEEE Internet Computing
- PC member, Workshop on Software Application Security (WSAS'07).
- PC Member, International Conference on Collaborative Computing, 2006.
- PC member, Next-generation web services Practices (NWeSP'06), 2006.
- Advisory committee, International Symposium on Collaborative Technology and Systems, 2006.
- PC member, CollaborateCom 2006.
- PC member, SecCrypt'06.
- PC member, IEEE eScience Collaborative Remote Laboratories Symposium, 2006.
- Program committee member, WISA 2005, NGWSP 2005, CTS 2005, CNIS 2005.

- Program committee member, WWW'2004 (Security track).
- Program committee member, European CSCW Conference, 1995, 1997, 1999, 2001.
- Program committee member, The Fifth International Symposium on Autonomous Decentralized Systems, March 2001.
- Associate Program Chair, IEEE Tools with AI Conference, 1999.
- Associate Program Chair, ACM Conference on Computer-supported Cooperative Work, 1998.
- Program committee member, IEEE International Conference on Distributed Computing Systems (ICDCS), 1998.
- Program committee member, Multimedia Software Engineering Workshop (held in conjunction with IEEE International Conference on Software Engineering), April 20-21, Kyoto, 1998.
- Program committee member, IEEE Conference on Tools with AI, 1997, 1998.
- Program committee member, the IEEE Singapore International Conference on Networks, April 1997.
- Program committee member, the Fifth and Sixth ACM Conference on Computer-Supported Cooperative Work, 1994, 1996.
- Program committee member, European Conference on Computer-Supported Cooperative Work, 1995, 1997
- Panel member, Multimedia for Collaboration Support, International Conference on Multimedia Computing and Systems (IEEE Multimedia 1996).
- mini-track coordinators on Web-based multimedia and collaboration technologies mini-track at the HICCS conference, 1996.
- Panel member, Distributed systems issues in Computer-Supported Cooperative Work, International Conference on Distributed Computing Systems, Vancouver, 1995.
- Program Vice-Chair, Software Engineering Track, 7th IEEE Conference on Tools with AI, Nov. 1995.
- Co-chair, ACM CSCW'94 Workshop on Distributed Systems, Multimedia, and Infrastructure Support in CSCW, October, 1994.
- Minitrack coordinator on Parallel and Distributed Programming Toolkits and Environments, Software Track of the 26th Hawaii International Conference on System Sciences, January 1993.
- Program committee member, 25th Annual Simulation Symposium, April 1992.

- Session Chair, 24th Annual Simulation Symposium, April 1991
- Program Committee Member, First IEEE International Conference on System Integration, New Jersey, April 1990.

## **Graduated Ph.D. Students and last known whereabouts**

- Haizhong Zheng (Ph.D. 2024), Starting postdoc at CMU from January 2025.
- Renuka Kumar (Ph.D. 2023), Engineering Lead, Cisco Systems.
- Kevin Eykholt (Ph.D. 2019), Postdoc, IBM Research.
- Amir Rahmati (Ph.D. 2017), Assistant Professor, Computer Science, Stony Brook University.
- Earlence Fernandes (Ph.D., 2017), Assistant Professor, Computer Science, U. of California, San Diego.
- Beng Heng Ng (Ph.D., 2013), Govt. of Singapore.
- Kevin Borders (Ph.D., 2009), Founder and CEO, Minware.
- Xin Zhao (Ph.D., 2007), Staff Software Engineer, Google.
- Lukasz Opyrchal (Ph.D. 2004), Software Engineer, Netflix.
- Patrick McDaniel (Ph.D. 2001), Professor, Computer Science, University of Wisconsin.
- Radu Litiu (Ph.D. 2001), Last position: Senior Software Engineer, F5 Networks.
- Amit Mathur (Ph.D. 2001), CEO, Vector Brook, Pune, India.
- Hyong Sop Shim, (Ph.D. 1999), Senior Scientist, Applied Communication Sciences, New Jersey.
- Jang Ho Lee,(Ph.D. 1999), Professor, Hongik University.
- Nelson Manohar (Ph.D. 1998). Research staff member, U. of Michigan.
- Trent Jaeger (Ph.D. 1997), Professor, UC Riverside.
- Santanu Paul (Ph.D. 1994), Founder and CEO, TalentSprint, Hyderabad, India.
- Ratib Al-Zoubi, Ph.D. 1992.

## **Current Ph.D. Students**

- Ryan Feng
- Elisa Tsai
- Neal Mangaokar

## **Teaching**

I have taught the following undergraduate and graduate courses at the University of Michigan.

- EECS 182: Building Information Environments
- EECS 280: Programming and Introductory Data Structures
- EECS 281 (formerly 380): Data Structures and Algorithms
- EECS 282: Information Systems Design and Programming
- EECS 481: Software Engineering
- EECS 482: Operating Systems
- EECS 484: Introduction to Databases
- EECS 498: Special topics course on computer security and trustworthy computing
- EECS 581: Advanced Software Engineering
- EECS 585: Web Technologies
- EECS 588: Computer and Network Security
- EECS 598: Special Topics course on groupware systems
- EECS 598: Special Topics course on multimedia systems
- EECS 598: Special Topics course on Web Technologies
- CSE 601: Introduction to Graduate Studies.

## **Professional Affiliations**

- ACM and IEEE