Somesh Jha

Lubar Professor
Computer Sciences Department
University of Wisconsin
1210 W. Dayton Street
Madison, WI 53706
jha@cs.wisc.edu;
Office: (608)-262-9519
Home: (608)-836-4022

EDUCATION

1990-1996	Carnegie Mellon University, Pittsburgh, PA. Ph.D. in Computer Science, August 1996. Thesis: *Symmetry and Induction in Model Checking*. Advisor: Prof. E.M. Clarke (Turing Laureate).
1985-1987	Pennsylvania State University, University Park, PA. M.S. in Computer Science, Aug 1987.
1980-1985	Indian Institute of Technology, New Delhi, India. B.Tech. in Electrical Engineering, May 1985.

EMPLOYMENT

1996-2000	Carnegie Mellon University, Pittsburgh, PA. Postdoctoral fellow in the School of Computer Science. **Note:** Also affiliated with CERT, Software Engineering Institute (SEI).
2000-2006	University of Wisconsin, Madison, WI. Assistant Professor.
2006-2009	University of Wisconsin, Madison, WI. Associate Professor.
2009-Present	University of Wisconsin, Madison, WI. Professor.

AWARDS AND HONORS

2003	Distinguished ACM SIGSOFT paper award at the *International Conference on Software Engineering (ICSE)*, 2003.
2004	Distinguished ACM SIGSOFT paper award at the *International Symposium on Software Testing and Analysis (ISSTA)*, 2004.
2004	Best student and best paper award at the *Annual Computer Security Applications Conference (ACSAC)*, 2004.
2005	NSF CAREER award.
2006	Best paper award at the *Annual Computer Security Applications Conference (ACSAC)*, 2006.
2007	Distinguished ACM SIGSOFT paper award at

the *European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007)*, 2007.

2008 Keynote address at
the *4th International Conference on Information Systems Security (ICISS).*

2009 Distinguished lecture at
the Technical University of Darmstadt.

2011 Distinguished lecture at
the University of Illinois, Chicago.

2011 Distinguished lecture at
the Kansas State University.

2012 Best artifact award at
International Symposium on the Foundations of Software Engineering.

2014 Best paper award at
Usenix Security Symposium.

2015 CAV award for fundamental contributions to the field of Computer-Aided Verification.
See `http://i-cav.org/cav-award` for more details about the award.

2015 h-index of $85+$ and $45,000+$ citations according to Google Scholar.
Last checked on Sept 2023.

2016 Sheldon B. Lubar Professorship in Computer Sciences.
Awarded on March 2, 2016.

2016 ACM Fellow.
Awarded on Dec 8, 2016.

2017 Grace Wahba Professorship in Computer Sciences.
Awarded on Mar 28, 2017.

2017 IEEE Fellow.
Awarded on Nov 20, 2017.

2018 Distinguished paper award.
31st IEEE Computer Security Foundations Symposium, 2018.

2018 Lubar Chair in Computer Sciences.
Awarded on Oct 29, 2018.

2021 IIT Delhi Distinguished Alumni Award.
See `https://alumni.iitd.ac.in/home/index.php/distinguished-alums/`
for more details about the award.

2021 AAAS fellow.
See `https://www.aaas.org/page/2021-fellows` for more details about the award.

2023 Conte Distinguished lecture at
Purdue Unversity, West Lafayette, IN.

PUBLICATIONS

Top five publications

1. Automated generation and analysis of attack graphs, O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, *Proceedings of IEEE Symposium on Security and Privacy*, 2002.

2. Counterexample-guided abstraction refinement for symbolic model checking, E. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith, *Journal of the ACM (JACM)*, 50 (5), 2003.

3. Semantics-aware malware detection, M. Christodorescu, S. Jha, S.A. Seshia, D. Song, and R.E. Bryant, *IEEE Symposium on Security and Privacy*, 2005.

4. The limitations of deep learning in adversarial settings. N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, ZB. Celik, A. Swami. *IEEE European symposium on security and privacy (EuroS&P)*, 2016.

5. Practical black-box attacks against machine learning, Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z Berkay Celik, Ananthram Swami, *Proceedings of the 2017 ACM on Asia conference on computer and communications security,* 2017.

Security, Privacy, and Trustworthy Machine Learning

1. E.M. Clarke, S. Jha, and W. Marrero, Using state space exploration and a natural deduction style message derivation engine to verify security protocols, *IFIP Working Conference on Programming Concepts and Methods (PROCOMET)*, June 1998.
2. E.M. Clarke, S. Jha, and W. Marrero, Partial Order Reductions for Security Protocol Verification, *Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, April 2000.
3. E.M. Clarke, S. Jha, and W. Marrero, Verifying Security Protocols with BRUTUS, *ACM Transactions in Software Engineering Methodology (TOSEM)*, Volume 9, Number 4, 2000.
4. S. Jha, R. Linger, T. Longstaff, and J. Wing, Survivability Analysis of Network Specifications, *Proceedings of the International Conference on Dependable Systems and Networks (DSN),* Workshop on Dependability Despite Malicious Faults, New York City, NY, June 25-28, 2000.
5. S. Jha and J. Wing, Survivability Analysis of Networked Systems, *International Conference on Software Engineering (ICSE)*, May, 2001.
6. S. Jha, K. Tan, and R. Maxion, Markov Chains, Classifiers, and Intrusion Detection, *Computer Security Foundations Workshop (CSFW)*, June 2001.
7. O. Shyener, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, Automated Generation and Analysis of Attack Graphs, *IEEE Symposium on Security and Privacy*, April 2002.
8. S. Jha, O. Sheyner, and J.M. Wing, Two formal Analyses of Attack Graphs, *Computer Security Foundations Workshop (CSFW)*, June 2002.
9. S. Jha and T. Reps, Analysis of SPKI/SDSI Certificates Using Model Checking, *Computer Security Foundations Workshop (CSFW)*, June 2002.
10. J. Giffin, S. Jha, and B. Miller, Detecting Manipulated Remote Call Streams, *Usenix Security Symposium*, August 2002.
11. E. Clarke, S. Jha, W. Marrero, Efficient Verification of Security Protocols using Partial-order reductions, *International Journal on Software Tools for Technology Transfer (STTT)*, Volume 4, Number 2, February 2003.
12. S. Schwoon, S. Jha, T. Reps, and S. Stubblebine, On Generalized Authorization Problems, *Computer Security Foundations Workshop (CSFW)*, July 2003.
13. M. Christodorescu and S. Jha, Static Analysis of Executables to Detect Malicious Patterns, *Usenix Security Symposium*, August 2003.
14. V. Ganapathy, S. Jha, D. Chandler, D. Melski, and D. Vitek, Buffer Overrun Detection using Linear Programming and Static Analysis, *ACM Conference on Computer and Communications Security (CCS)*, October 2003.
15. J. Giffin, S. Jha, and B. Miller, Efficient Context-sensitive Intrusion Detection, *Network and Distributed System Security Symposium (NDSS)*, February 2004.
16. V. Yegneswaran, P. Barford, and S. Jha, Global Intrusion Detection in the DOMINO Overlay System, *Network and Distributed System Security Symposium (NDSS)*, February 2004.
17. H.H. Feng, J. Giffin, Y. Huang, S. Jha, W. Lee, B. Miller, Formalizing Sensitivity in Static Analysis for Intrusion Detection, *IEEE Symposium on Security and Privacy*, April 2004.

18. H.B. Wang, S. Jha, P.D. McDaniel, M. Livny, Security Policy Reconciliation in Distributed Computing Environments, *IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY)*, June 2004.

19. M. Christodorescu and S. Jha, Testing Malware Detectors, *International Symposium on Software Testing and Analysis (ISSTA 2004)*, July 11-14, 2004.
    Note: This paper won the outstanding paper award at the conference.

20. Paul Barford, Somesh Jha, and Vinod Yegneswaran, Fusion and Filtering in Distributed Intrusion Detection Systems, *42nd Annual Allerton Conference on Communication, Control and Computing*, September, 2004.

21. S. Rubin, S. Jha, and B. Miller, Automatic generation and analysis of NIDS attacks, *Annual Computer Security Applications Conference (ACSAC)*, December 6-10, 2004.
    Note: This paper won the best student and outstanding paper award at the conference.

22. Somesh Jha, Thomas W. Reps, Model checking SPKI/SDSI, *Journal of Computer Security*, 12(3-4): 317-353 (2004).

23. S. Rubin, S. Jha, B. P. Miller, Using attack mutation to test a high-end NIDS, *Information Security Bulletin*, Volume 10, April, 2005.

24. Vinod Ganapathy, Sanjit A. Seshia, Somesh Jha, Thomas W. Reps, and Randal E. Bryant, Automatic Discovery of API-Level Exploits, *27th International Conference on Software Engineering (ICSE)*, St. Louis, Missouri, May 2005.

25. S. Rubin, S. Jha, and B. Miller, Language-based Generation and Evaluation of NIDS, *IEEE Symposium on Security and Privacy*, May 2005.

26. M. Christodorescu, S. Jha, S. Seshia, D. Song, and R.E. Bryant, Semantics-Aware Malware Detection, *IEEE Symposium on Security and Privacy*, May 2005.

27. Vinod Yegneswaran, Jonathon T. Giffin, Paul Barford, and Somesh Jha, An architecture for generating semantics-aware signatures, *In 14th USENIX Security Symposium*, Baltimore, Maryland, August 2005.

28. Jonathon T. Giffin, David Dagon, Somesh Jha, Wenke Lee, and Barton P. Miller, Environment-sensitive intrusion detection, In *8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Seattle, Washington, September 2005.

29. S. Jha, L. Kruger and P. McDaniel, Privacy Preserving Clustering, *10th European Symposium On Research In Computer Security (ESORICS)*, Milan, Italy - September 12 - 14, 2005.

30. Vinod Ganapathy, Trent Jaeger, and Somesh Jha, Automatic Placement of Authorization Hooks in the Linux Security Modules Framework, *12th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, Virginia, November 2005.

31. Muthian Sivathanu, Andrea C. Arpaci-Dusseau, Remzi H. Arpaci-Dusseau, and Somesh Jha, A Logic of File Systems, *4th Usenix Conference on File and Storage Technologies (FAST 05)*, Dec 14, 2005.

32. Vinod Ganapathy, Trent Jaeger, and Somesh Jha, Retrofitting Legacy Code for Authorization Policy Enforcement, *IEEE Symposium on Security and Privacy*, May 2006.

33. David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha, Towards Automatic Generation of Vulnerability-Based Signatures, *IEEE Symposium on Security and Privacy*, May 2006.

34. S. Rubin, S. Jha, B. Miller, On the Completeness of Attack Mutation Algorithms, *IEEE Computer Security Foundations Workshop (CSFW)*, July 2006.

35. H. Wang, S. Jha, T. Reps, S. Schwoon, and S. Stubblebine, Reducing the Dependence of SPKI/SDSI on PKI, *European Symposium on Research in Computer Security (ESORICS)*, Sept 2006.

36. J. Giffin, S. Jha, and B. Miller, Automated Discovery of Mimicry Attacks, *International Conference on Recent Advances in Intrusion Detection (RAID)*, Sept 2006.

37. E. Goh, L. Kruger, D. Boneh, and S. Jha, Secure Function Evaluation with Binary Decision Diagrams, *ACM Conference on Computer and Communications Security (CCS)*, Nov 2006.

38. S. Rubin, S. Jha, and B. Miller, Protocomatching Network Traffic for High Throughput Network Intrusion Detection, *ACM Conference on Computer and Communications Security (CCS)*, Nov 2006.

39. H. Wang, S. Jha, and V. Ganapathy, NetSpy: Automatic Generation of Spyware Signatures in NIDS, *Annual Computer Security Applications Conference (ACSAC)*, Dec 2006.

40. R. Smith, C. Estan, and S. Jha, Backtracking Algorithmic Complexity Attacks Against NIDS, *Annual Computer Security Applications Conference (ACSAC)*, Dec 2006.

41. Mila Dalla Preda, Mihai Christodorescu, Saumya Debray, and Somesh Jha, A Semantics-Based Approach to Malware Detection, *Symposium on Principles of Programming Languages (POPL)*, Nice, France, January 2007.

42. Somesh Jha, Stefan Katzenbeisser, Christian Schallhart, Helmut Veith and Stephen Chenney, Enforcing Semantic Integrity on Untrusted Clients in Networked Virtual Environments (Extended abstract), *IEEE Symposium on Security and Privacy*, Oakland, California, May 2007.

43. Vinod Ganapathy, David King, Trent Jaeger, and Somesh Jha, Mining Security-sensitive Operations in Legacy Code using Concept Analysis, *29th International Conference on Software Engineering , Minneapolis*, Minnesota, May 2007.

44. Vinod Ganapathy, Arini Balakrishnan, Michael M. Swift, and Somesh Jha, Microdrivers: A New Architecture for Device Drivers, *11th Workshop on Hot Topics in Operating Systems*, San Diego, California, May 2007.

45. David Brumley, Hao Wang, Somesh Jha and Dawn Song, Creating Vulnerability Signatures Using Weakest Pre-conditions, *20th IEEE Computer Security Foundations Symposium (CSF)*, July 2007.

46. Mihai Christodorescu, Somesh Jha, and Christopher Kruegel, Mining Specifications of Malicious Behavior, *Sixth joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007)*, September 3-7, 2007, Dubrovnik, Croatia.

47. Lorenzo Martignoni, Mihai Christodorescu, and Somesh Jha, OmniUnpack: Fast, Generic, and Safe Unpacking of Malware, *Twenty-Third Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, December 2007.

48. Vinod Ganapathy, Matthew J. Renzelmann, Arini Balakrishnan, Michael M. Swift, Somesh Jha, The design and implementation of Microdrivers. *International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2008.

49. Randy Smith, Cristian Estan, Somesh Jha, XFA: Faster Signature Matching with Extended Automata. *IEEE Symposium on Security and Privacy*, 2008.

50. Somesh Jha, Louis Kruger, Vitaly Shmatikov, Towards Practical Privacy for Genomic Computation. *IEEE Symposium on Security and Privacy*, 2008.

51. Lorenzo Martignoni, Elizabeth Stinson, Matt Fredrikson, Somesh Jha, John C. Mitchell, A Layered Architecture for Detecting Malicious Behaviors. *Recent Advances in Intrusion Detection (RAID)*, 2008.

52. Randy Smith, Cristian Estan, Somesh Jha, Shijin Kong, Deflating the big bang: fast and scalable deep packet inspection with extended finite automata. *SIGCOMM*, 2008.

53. Mila Dalla Preda, Mihai Christodorescu, Somesh Jha, Saumya K. Debray, A semantics-based approach to malware detection. *ACM Trans. Program. Lang. Syst. (TOPLAS) 30(5):*, 2008.

54. Dave King, Trent Jaeger, Somesh Jha, and Sanjit A. Seshia, Effective Blame for Information-Flow Violations. *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE)*, 2008.

55. D. Brumley, J. Newsome, D. Song, H. Wang, and S. Jha, Theory and Techniques for Automated Generation of Vulnerability-Based Signatures. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, 5(4), October-December 2008.

56. S. Jha, N. Li, M. Tripunitara, Q. Wang, and W. H. Winsborough, Toward Formal Verification of Role-Based Access Control Policies. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, 5(4), October-December 2008.

57. R. Smith, C. Estan, S. Jha, and I. Siahaan, Fast Signature Matching Using Extended Finite Automaton (XFA). *4th International Conference on Information Systems Security (ICISS)*, Hyderabad, India, 2008.

58. Drew Davidson, Randy Smith, Nic Doyle, Somesh Jha, Protocol Normalization Using Attribute Grammars. *14th European Symposium on Research in Computer Security (ESORICS)*, Saint-Malo, France, September, 2009. ESORICS 2009.

59. William R. Harris, Nicholas Kidd, Sagar Chaki, Somesh Jha, Thomas W. Reps, Verifying Information Flow Control over Unbounded Processes. *Formal Methods, Second World Congress (FM)*, Eindhoven, The Netherlands, November 2009.

60. Daniel Luchaup, Randy Smith, Cristian Estan, Somesh Jha, Multi-byte Regular Expression Matching with Speculation. *Recent Advances in Intrusion Detection (RAID)*, Saint-Malo, France, September 2009.

61. Dave King, Susmit Jha, Divya Muthukumaran, Trent Jaeger, Somesh Jha, Sanjit A. Seshia, Automating Security Mediation Placement. *19th European Symposium on Programming*, March 2010.

62. Somesh Jha, Stefan Katzenbeisser, Christian Schallhart, Helmut Veith, Stephen Chenney, Semantic integrity in large-scale online simulations. *ACM Transactions on Internet Technology*, 10(1), 2010.

63. William R. Harris, Somesh Jha, Thomas W. Reps, DIFC programs by automatic instrumentation. *ACM Conference on Computer and Communications Security (CCS)*, 2010.

64. Matt Fredrikson, Somesh Jha, Mihai Christodorescu, Reiner Sailer, Xifeng Yan, Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors. *IEEE Symposium on Security and Privacy*, 2010.

65. Amit Kumar, Lorenzo De Carli, Sung Jin Kim, Marc de Kruijf, Karthikeyan Sankaralingam, Cristian Estan, and Somesh Jha, Design and implementation of the PLUG architecture for programmable and efficient network lookups. *19th International Conference on Parallel Architecture and Compilation Techniques (PACT)*, 2010.

66. Roberto Paleari, Lorenzo Martignoni, Emanuele Passerini, Drew Davidson, Matt Fredrikson, Jonathon T. Giffin, and Somesh Jha, Automatic Generation of Remediation Procedures for Malware Infections. *USENIX Security Symposium*, 2010.

67. Daniel Luchaup, Randy Smith, Cristian Estan, and Somesh Jha, Speculative Parallel Pattern Matching. *IEEE Transactions on Information Forensics and Security 6(2)*, 2011)

68. Matthew Fredrikson, Mihai Christodorescu, and Somesh Jha, Dynamic Behavior Matching: A Complexity Analysis and New Approximation Algorithms. *CADE*, 2011.

69. Martin Franz, Bjrn Deiseroth, Kay Hamacher, Somesh Jha, Stefan Katzenbeisser, and Heike Schroder, Towards Secure Bioinformatics Services (Short Paper). *Financial Cryptography*, 2011.

70. Mihai Christodorescu, Matthew Fredrikson, Somesh Jha, and Jonathon T. Giffin, End-to-End Software Diversification of Internet Services. *Moving Target Defense*, 2011.

71. Matthew Fredrikson, Richard Joiner, Somesh Jha, Thomas W. Reps, Phillip A. Porras, Hassen Saidi, and Vinod Yegneswaran, Efficient Runtime Policy Enforcement Using Counterexample-Guided Abstraction Refinement. *CAV*, 2012.

72. William R. Harris, Somesh Jha, and Thomas W. Reps, Secure Programming via Visibly Pushdown Safety Games. *CAV*, 2012.

73. Martin Franz, Bjorn Deiseroth, Kay Hamacher, Somesh Jha, Stefan Katzenbeisser, and Heike Schroder, Secure computations on non-integer values with applications to privacy-preserving sequence analysis. *Inf. Sec. Techn. Report 17(3)*, 2013.

74. Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, Marko Wolf, Alexandre Bouard, William R. Harris, Somesh Jha, Thomas Peyrin, Axel Poschmann, and Samarjit Chakraborty, Security challenges in automotive hardware/software architecture design. *DATE*, 2013.

75. Somesh Jha, Matthew Fredrikson, Mihai Christodorescu, Reiner Sailer, and Xifeng Yan, Synthesizing near-optimal malware specifications from suspicious behaviors. *MALWARE*, 2013.

76. William R. Harris, Somesh Jha, Thomas W. Reps, Jonathan Anderson, and Robert N. M. Watson, Declarative, Temporal, and Practical Programming with Capabilities. *IEEE Symposium on Security and Privacy*, 2013.

77. Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart, Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing. *USENIX Security*, 2014.
    Note: Received the best paper award.

78. Daniel Luchaup, Kevin P. Dyer, Somesh Jha, Thomas Ristenpart, and Thomas Shrimpton, LibFTE: A Toolkit for Constructing Practical, Format-Abiding Encryption Schemes. *USENIX Security*, 2014.

79. Matthew Fredrikson and Somesh Jha, Satisfiability modulo counting: a new approach for analyzing privacy properties. *CSL-LICS*, 2014.

80. Daniel Luchaup, Lorenzo De Carli, Somesh Jha, and Eric Bach, Deep packet inspection with DFA-trees and parametrized language overapproximation. *INFOCOM*, 2014.

81. Daniel Luchaup, Thomas Shrimpton, Thomas Ristenpart, and Somesh Jha, Formatted Encryption Beyond Regular Languages. *ACM Conference on Computer and Communications Security (CCS)*, 2014.

82. Lorenzo De Carli, Robin Sommer, and Somesh Jha, Beyond Pattern Matching: A Concurrency Model for Stateful Deep Packet Inspection. *ACM Conference on Computer and Communications Security (CCS)*, 2014.

83. Matt Fredrikson, Somesh Jha, and Thomas Ristenpart, Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *ACM Conference on Computer and Communications Security (CCS)*, 2015.

84. Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik, and Ananthram Swami. The Limitations of Deep Learning in Adversarial Settings. *IEEE European Symposium on Security and Privacy*, March 2016.

85. Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami. Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks. *IEEE Symposium on Security and Privacy*, May 2016.

86. Xi Wu, Matthew Fredrikson, Somesh Jha, and Jeffrey F. Naughton. Methodology for Formalizing Model-Inversion Attacks. *IEEE Computer Security Foundations Symposium*, June 2016.

87. A. Nadkarni, B. Andow, W. Enck, and S.Jha. Practical DIFC Enforcement on Android. *USENIX Security Symposium*, August 2016.

88. L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, and S. Jha. Botnet Protocol Inference in the Presence of Encrypted Traffic. *INFOCOM*, May 2017.

89. Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. Practical Black-Box Attacks against Machine Learning. *AsiaCCS*, 2017.

90. Drew Davidson, Yaohui Chen, Franklin George, Long Lu, and Somesh Jha. Secure Integration of Web Content and Applications on Commodity Mobile Operating Systems. *AsiaCCS*, 2017.

91. Xi Wu, Fengan Li, Arun Kumar, Kamalika Chaudhuri, Somesh Jha, and Jeffrey F. Naughton. Bolt-on Differential Privacy for Scalable Stochastic Gradient Descent-based Analytics. *SIGMOD Conference*, 2017.

92. Tianhao Wang, Jeremiah Blocki, and Ninghui Li, and Somesh Jha. Locally Differentially Private Protocols for Frequency Estimation. *Usenix Security*, 2017.

93. Uyeong Jang, Xi Wu, Google, and Somesh Jha. Objective Metrics And Gradient Descent Algorithms For Adversarial Examples In Machine Learning *ACSAC*, 2017.

94. W. Harris, S. Jha, T. Reps, and S. Seshia. Program synthesis for interactive-security systems. *In Formal Methods in System Design (FMSD)*, (Volume 51, Issue 2), November 2017.

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

96. T. Wang, N. Li, and S. Jha. Locally Differentially Private Frequent Itemset Mining. *IEEE Symposium on Security and Privacy*, 2018.

97. Xi Wu, Uyeong Jang, Jiefeng Chen, Lingjiao Chen, Somesh Jha. Reinforcing Adversarial Robustness using Model Confidence Induced by Adversarial Training *International Conference on Machine Learning (ICML)*, 2018.

98. Yizhen Wang, Somesh Jha, Kamalika Chaudhuri. Analyzing the Robustness of Nearest Neighbors to Adversarial Examples. *International Conference on Machine Learning (ICML)*, 2018.

99. S. Yeom, I. Giacomelli, M. Fredrikson, S. Jha. Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting. *IEEE Computer Security Foundations Symposium (CSF)*, 2018.
Note: Distinguished paper award.

100. Shiqing Ma, Juan Zhai, Yonghwi Kwon, Kyu Hyung Lee, Xiangyu Zhang, Gabriela Ciocarlie, Ashish Gehani, Vinod Yegneswaran, Dongyan Xu, Somesh Jha. Kernel-Supported Cost-Effective Audit Logging for Causality Tracking. *USENIX Annual Technical Conference (ATC 2018)*, 2018.

101. Irene Giacomelli, Somesh Jha, Marc Joye, C. David Page, Kyonghwan Yoon. Privacy-Preserving Ridge Regression with only Linearly-Homomorphic Encryption. *Applied Cryptography and Network Security (ACNS)*, 2018.

102. Irfan Ul Haq, Sergio Chica, Juan Caballero, Somesh Jha. Malware lineage in the wild. *Computers and Security*, 78, 2018.

103. I. Giacomelli, S. Jha, R. Kleiman, D. and K. Yoon. Privacy-Preserving Collaborative Prediction using Random Forests. *AMIA Informatics Summit*, 2019.

104. Tianhao Wang, Ninghui Li, and Somesh Jha. Locally differentially private heavy hitter identification. *IEEE Transactions on Dependable and Secure Computing*, 2019.

105. U. Jang, S. Jha, and S Jha. On the Need for Topology-Aware Generative Models for Manifold-Based Defenses. *International Conference on Learning Representations (ICLR)*, 2019.

106. T Wang, B Ding, J Zhou, C Hong, Z Huang, N Li, and S Jha. Answering multi-dimensional analytical queries under local differential privacy. *Proceedings of the International Conference on Management of Data*, 2019.

107. S. Jha, S. Raj, S. Fernandes, SK. Jha, S. Jha, B. Jalaian, G. Verma, and A. Swami. Attribution-based confidence metric for deep neural networks. *Proceedings Advances in Neural Information Processing Systems (NeurIPS)*, 2019.

108. J. Chen, X. Wu, V. Rastogi, Y. Liang, and S. Jha. Robust attribution regularization. *Proceedings in Advances in Neural Information Processing Systems (NeurIPS)*, 2019.

109. P. Chalasani, J. Chen, AR. Chowdhury, X. Wu, and S Jha. Concise explanations of neural networks using adversarial training. *International Conference on Machine Learning (ICML)*, 2020.

110. AR. Chowdhury, T. Rekatsinas, S. Jha. Data-dependent differentially private parameter learning for directed graphical models. *International Conference on Machine Learning (ICML)*, 2020.

111. W. Zhang, TK. Panum, S. Jha, P. Chalasani, and D. Page. CAUSE: Learning Granger Causality from Event Sequences using Attribution Methods. *International Conference on Machine Learning (ICML)*, 2020.

112. T. Wang, B. Ding, M. Xu, Z. Huang, C. Hong, J. Zhou, N. Li, and S. Jha. Improving utility and security of the shuffler-based differential privacy. *Proceedings of the VLDB Endowment (VLDB)*, 2020.

113. A. Roy Chowdhury, C. Wang, X. He, A. Machanavajjhala, and S. Jha. Cryptϵ: Crypto-Assisted Differential Privacy on Untrusted Servers. *Proceedings of ACM SIGMOD*, 2020.

114. S. Garg, S. Jha, S. Mahloujifar, and M. Mohammad. Adversarially Robust Learning Could Leverage Computational Hardness. *Algorithmic Learning Theory (ALT)*, 2020.

115. SA. Seshia, S. Jha, and T. Dreossi. Semantic Adversarial Deep Learning. *IEEE Design & Test*, 37(2), 2020.

116. S. Yeom, I. Giacomelli, A. Menaged, M. Fredrikson, S. Jha. Overfitting, robustness, and malicious algorithms: A study of potential causes of privacy risk in machine learning. *Journal of Computer Security (JCS)*, 28(1), 2020.

117. V. Chandrasekaran, K. Chaudhuri, I. Giacomelli, S. Jha, and S. Yan. Exploring connections between active learning and model extraction. *USENIX Security Symposium*, 2020.

118. A. Xiong, T. Wang, N. Li, and S. Jha. Towards effective differential privacy communication for users data sharing decision and comprehension. *IEEE Symposium on Security and Privacy (Oakland)*, 2020.

119. Z. Sun, B. Feng, L. Lu, and S. Jha. OAT: Attesting operation integrity of embedded devices. *IEEE Symposium on Security and Privacy (Oakland)*, 2020.

120. N. Carlini, S. Deng, S. Garg, S. Jha, S. Mahloujifar, M. Mahmoody, A. Thakurta. Is Private Learning Possible with Instance Encoding? *IEEE Symposium on Security and Privacy (Oakland)*, 2021.

121. W. Garcia, A. Chhotaray, J.I. Choi, S.K. Adari, K. Butler, and S. Jha. Brittle Features of Device Authentication. *Proceedings of the Eleventh ACM Conference on Data and Application Security (ACSAC)*, 2021.

122. H. Irshad, G. Ciocarlie, A. Gehani, V. Yegneswaran, K.H. Lee, J. Patel, S. Jha. TRACE: Enterprise-wide provenance tracking for real-time APT detection. *IEEE Transactions on Information Forensics and Security 16*, 2021.

123. J. Raghuram, V. Chandrasekaran, S. Jha, and S. Banerjee A general framework for detecting anomalous inputs to DNN classifiers. *International Conference on Machine Learning (ICML)*, 2021.

124. R. Bhattacharjee, S. Jha, and K. Chaudhuri. Sample Complexity of Robust Linear Classification on Separated Data. *International Conference on Machine Learning (ICML)*, 2021.

125. J. Chen, Y. Li, X. Wu, Y. Liang, and S. Jha. Atom: Robustifying out-of-distribution detection using outlier mining. *ECML*, 2021.

126. T. Wang, J.Q. Chen, Z. Zhang, D. Su, Y. Cheng, Z. Li, N. Li, and S Jha. Continuous release of data streams under both centralized and local differential privacy. *ACM CCS*, 2021.

127. S. Deng, S. Garg, S. Jha, S. Mahloujifar, M. Mahmoody, and A. Guha Thakurta. A Separation Result Between Data-oblivious and Data-aware Poisoning Attacks. *NeurIPS*, 2021.

128. J. Chen, F. Liu, B. Avci, X. Wu, Y. Liang, and S. Jha. Detecting errors and estimating accuracy on unlabeled data with self-training ensembles. *NeurIPS*, 2021.

129. A. Roy Chowdhury, B. Ding, S. Jha, W. Liu, and J Zhou. Strengthening order preserving encryption with differential privacy, *ACM CCS*, 2022.

130. S. Maddock, G. Cormode, T. Wang, C. Maple, and S Jha. Federated boosted decision trees with differential privacy, *ACM CCS*, 2022.

131. A. Roy Chowdhury, C. Guo, S. Jha, and L van der Maaten. Eiffel: Ensuring integrity for federated learning, *ACM CCS*, 2022.

132. Z. Wang, A. Albarghouthi, G. Prakriya, S. Jha. Interval universal approximation for neural networks, *POPL*, 2022.

133. J. Henkel, G. Ramakrishnan, Z. Wang, A. Albarghouthi, S. Jha, and T Reps. Semantic robustness of models of source code, *IEEE SANER*, 2022.

134. R. Feng, N. Mangaokar, J. Chen, E. Fernandes, S. Jha, and A. Prakash. Graphite: Generating automatic physical examples for machine-learning attacks on computer vision systems, *IEEE EuroSP*, 2022.

135. M. Alhanahnah, R. Jain, V. Rastogi, S. Jha, and T. Reps. Lightweight, multi-stage, compiler-assisted application specialization, *IEEE EuroSP*, 2022.

136. Y. Wang, M. Alhanahnah, X. Meng, K. Wang, M. Christodorescu, and S. Jha. Robust learning against relational adversaries, *NeurIPS*, 2022.

137. S. Garg, S. Jha, S. Mahloujifar, M. Mahmoody, and M Wang. Overparameterization from computational constraints, *NeurIPS*, 2022.

138. Z Wang, G Prakriya, and S Jha. A quantitative geometric approach to neural-network smoothness, *NeurIPS*, 2022.

139. H. Rosenberg, B. Tang, K. Fawaz, and S. Jha. Fairness properties of face recognition and obfuscation systems, *Usenix Security*, 2023.

140. M. Alhanahnah, S. Ma, A. Gehani, G.F. Ciocarlie, V. Yegneswaran, S. Jha, and X. Zhang. autoMPI: automated multiple perspective attack investigation with semantics aware execution partitioning, *IEEE Transactions on Software Engineering*, 2022.

141. W. Garcia, P.Y. Chen, H.S. Clouse, S. Jha, K.R.B. Butler. Less is More: Dimension Reduction Finds On-Manifold Adversarial Examples in Hard-Label Attacks, *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, 2023.

142. Z. Sun, R. Sun, C. Liu, A.R. Chowdhury, L. Lu, and S. Jha. Shadownet: A secure and efficient on-device model inference system for convolutional neural networks, *IEEE Symposium on Security and Privacy (Oakland)*, 2023.

143. J. Choi, J. Raghuram, R. Feng, J. Chen, S. Jha, and A. Prakash. Concept-based explanations for out-of-distribution detectors, *ICML*, 2023.

144. J. Chen, J. Raghuram, J. Choi, X. Wu, Y. Liang, and S. Jha. Stratified Adversarial Robustness with Rejection, *ICML*, 2023.

Formal Methods, Programming Languages, and Software Engineering

1. E.M. Clarke, O. Grumberg, H. Hirashi, S. Jha, D.E. Long, K.L. McMillan, and L.A. Ness, Verification of the Futurebus+ Cache Coherence Protocol, *Formal Methods in System Design*, Volume 6/2, 1995. A preliminary version appeared in CHDL, 93.

2. E.M. Clarke, R. Enders, T. Filkorn, and S. Jha, Exploiting Symmetry in Temporal Logic Model Checking, *Formal Methods in System Design*, Volume 9/2, 1996. A preliminary version appeared in CAV, 95.

3. A. Browne, E.M. Clarke, S. Jha, D.E. Long, and W. Marrero, An Improved Algorithm for Evaluation of Fixpoint Expressions, *Theoretical Computer Science*, Volume 178, 1997. A preliminary version appeared in CAV, 94.

4. E.M. Clarke and S. Jha, Symmetry and Induction in Model Checking, *Computer Science Today (Recent Trends and Developments)*, Special LNCS 1000-th volume, September 1995, Editor J. Van Leeuwen.

5. D. Jackson, S. Jha, and C. Damon, Faster Checking of Software Specifications by Eliminating Isomorphs, *Principles of Programming Languages (POPL)*, January 1996.

6. C. Damon, D. Jackson, and S. Jha, Checking Relational Specifications with BDDs, *Fourth ACM SIGSOFT Symposium on Foundations of Software Engineering (FSE 4)*, October 1996.

7. E.M. Clarke, O. Grumberg, and S. Jha, Verifying Parameterized Networks, *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Volume 19/5, 1997. A preliminary version appeared in CONCUR, 95.

8. E.A. Emerson, S. Jha, and D. Peled, Combining Partial Order and Symmetry Reductions, *Proceedings of Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, April 1997.

9. S. Jha, M. Minea, Y. Lu, and E.M. Clarke, Equivalence Checking using Abstract BDDS, *Proceedings of International Conference on Computer Design (ICCD)*, October 1997.

10. E.M. Clarke, E.A. Emerson, S. Jha, and A.P. Sistla, Symmetry Reductions in Model Checking, *Computer Aided Verification (CAV)*, 1998.

11. D. Jackson, S. Jha, and C. Damon, Isomorph-free Model Enumeration: A New Method for Checking Relational Specifications, *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Volume 20, No. 2, 1998.

12. J. Dingel, D. Garlan, S. Jha, and D. Notkin, Towards a Formal Treatment of Implicit Invocation using Rely/Guarantee Reasoning, *Formal Aspects of Computing*, volume 10, 1998.

13. J. Dingel, D. Garlan, S. Jha, and D. Notkin, Reasoning about Implicit Invocation, *Sixth ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 6)*, November 1998.

14. E.M. Clarke, S. Jha, Y. Lu, and D. Wang, Abstract BDDs: a general methodology for using abstraction in Model Checking, *10-th IFIP WG10.5 Advanced Research Working Conference on Correct Hardware Design and Verification Methods (CHARME)*, September 1999.

15. Sullivan, K.J., P. Chalasani, S. Jha, and V. Sazawal, Software Design as an Investment Activity: A Real Options Perspective, in *Real Options and Business Strategy: Applications to Decision Making*, L. Trigeorgis, consulting editor, Risk Books, 1999.

16. S. Berezin, E. Clarke, S. Jha, and W. Marrero, Model checking algorithms for the μ-calculus, in *Proof, Language, and Interaction*, Edited by G. Plotkin, MIT Press, 2000.

17. Edmund M. Clarke, Orna Grumberg, Somesh Jha, Yuan Lu, and Helmut Veith, Counterexample-Guided Abstraction Refinement, *Computer Aided Verification (CAV)*, July 2000.

18. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith, Progress on the State Explosion Problem in Model Checking, *Dagstuhl* 10^{th} *Anniversary: Informatics 1- 10 Years Back and 10 Years Ahead*, LNCS volume 2000, Springer Verlag, editor Rienhard Wilhelm, 2001.

19. P. Chauhan, E.M. Clarke, S. Jha, J.H. Kukula, H. Veith, and D. Wang, Using Combinatorial Optimization Methods for Quantification Scheduling, *Correct Hardware Design and Verification Methods (CHARME)*, Sept 2001.

20. P. Chauhan, E.M. Clarke, S. Jha, J.H. Kukula, H. Veith, and D. Wang, Non-linear Quantification Scheduling in Image Computation, *ICCAD*, 2001.

21. A. Campialla, S. Chaki, E.M. Clarke, S. Jha and H. Veith, Efficient Filtering in Publish Subscribe Systems Using Binary Decision Diagrams, *International Conference on Software Engineering (ICSE)*, May, 2001.

22. E.M. Clarke, S. Jha, Y. Lu, H. Veith, Tree-like Counterexamples in Model Checking, *Logic in Computer Science (LICS)*, July 2002.

23. S. Jha, J. Palsberg, and T. Zhao, Efficient Type Matching, *Foundations of Software Science and Computation Structures (FOSSACS)*, April, 2002.

24. T. Reps, S. Schwoon, S. Jha, Weighted Pushdown Systems and their Applications to Interprocedural Dataflow Analysis, *International Static Analysis Symposium (SAS)*, June 2003.

25. S. Chaki, E. Clarke, A. Groce, S. Jha and H. Veith, Modular Verification of Software Components in C, *International Conference on Software Engineering (ICSE)*, May, 2003.
    Note: This paper won the outstanding paper award at the conference.

26. S. Chaki, P. Fenkam, H. Gall, S. Jha, E. Kirda, H. Veith, Integrating Publish/Subscribe into a Mobile Teamwork Support Platform, *International Conference on Software Engineering and Knowledge Engineering (SEKE)*, July 2003.

27. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, H. Veith, Counterexample-guided abstraction refinement for symbolic model checking, *Journal of the ACM (JACM)*, Volume 50, Issue 5, September 2003.

28. T. Reps, S. Schwoon, S. Jha, and D. Melski, Weighted pushdown systems and their application to interprocedural dataflow analysis, *Science of Computer Programming*, 58, 1-2 (Oct. 2005).

29. Sagar Chaki, Edmund Clarke, Somesh Jha, Helmut Veith, An Iterative Framework for Simulation Conformance, *Journal of Logic and Computation (JLC)*, Oxford University Press, volume 15, number 4, page 465-488, August 2005.

30. Wenchao Li, Sanjit A. Seshia, and Somesh Jha, CrowdMine: towards crowdsourced human-assisted verification. *DAC*, 2012.

31. Marc de Kruijf, Karthikeyan Sankaralingam, Somesh Jha, Static analysis and compiler design for idempotent processing. *PLDI*, 2012.

32. Damien Octeau, Somesh Jha, Patrick McDaniel, Retargeting Android applications to Java bytecode. *SIGSOFT FSE*, 2012.

33. William R. Harris, Guoliang Jin, Shan Lu, Somesh Jha, Validating Library Usage Interactively. *CAV*, 2013.

34. Richard Joiner, Thomas W. Reps, Somesh Jha, Mohan Dhawan, Vinod Ganapathy, Efficient runtime-enforcement techniques for policy weaving. *SIGSOFT FSE*, 2014.

35. Damien Octeau, Daniel Luchaup, Matthew Dering, Somesh Jha, and Patrick McDaniel, Composite Constant Propagation: Application to Android Inter-Component Communication Analysis. *37th International Conference on Software Engineering (ICSE)*, May 2015.

36. Damien Octeau, Somesh Jha, Matthew Dering, Patrick McDaniel, Alexandre Bartel, Hongyu Li, Jacques Klein, and Yves Le Traon, Combining Static Analysis with Probabilistic Models to Enable Market-Scale Analysis. *Symposium on Principles of Programming Languages (POPL)*, January 2015.

37. Damien Octeau, Daniel Luchaup, Somesh Jha, Patrick D. McDaniel, Composite Constant Propagation and its Application to Android Program Analysis. *IEEE Transactions Software Engineering (TSE)*, 42(11), 2016.

38. V. Rastogi, D. Davidson, L. De Carli, S. Jha, and P. McDaniel. Cimplifier: Automatically Debloating Containers *FSE*, 2017.

39. Jinman Zhao, Aws Albarghouthi, Vaibhav Rastogi, Somesh Jha and Damien Octeau. Neural-Augmented Static Analysis of Android Communication. *The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*, 2018.

40. V. Ganesh, S.A. Seshia, and S Jha. Machine learning and logic: a new frontier in artificial intelligence, *Formal Methods in System Design (FMSD)*, 2023.

Computational Finance

1. P. Chalasani, S. Jha, and A. Varikooty, Accurate Approximations for European Asian Options, *Journal of Computational Finance (JCF)*, Volume 1/Number 4, 1998.

2. P. Chalasani, S. Jha, F. Egriboyun, and A. Varikooty, A Refined Binomial Lattice for Pricing American Asian Options, *Review of Derivatives Research (REDR)*, Volume 3, Issue 1, 1999. Also appeared in *8th Annual Derivative Securities Conference,* 1998.

3. P. Chalasani, S. Jha, and I. Saias, Approximate Option Pricing, *Algorithmica*, Volume 25, 1999. Also appeared in *Proceedings of Foundations of Computer Science (FOCS)*, 1996.

4. P. Chalasani, and S. Jha, Randomized Stopping Times and American Option Pricing with Transaction Costs, *Mathematical Finance*, Volume 11/1, January 2001. Also appeared in *9th Annual Derivative Securities Conference,* 1999.

Multi-agents systems

1. O. Shehory, K. Sycara, and S. Jha, Multi-agent Coordination through Coalition Formation, Lecture Notes in Artificial Intelligence no. 1365, *Intelligent Agents IV*, edited by A. Rao, M. Singh and M. Wooldridge, pages 143-154. Springer, 1997.

2. P. Chalasani, S. Jha, O. Shehory, and K. Sycara, Strategies for Querying Information Agents, Lecture Notes in Artificial Intelligence no. 1435, edited by M. Klusch and G. Weiss, pages 94-107, 1998.

3. P. Chalasani, S. Jha, O. Shehory, and K. Sycara, Query restart strategies for web agents, *In Proceedings of Autonomous Agents 98*, pages 124-131, Minneapolis, May 1998.

4. O. Shehory, K. Sycara P. Chalasani, and S. Jha, Agent cloning: an approach to agent mobility and resource allocation, *IEEE Communications*, pages 58-67, vol. 36, no. 7, 1998.

Miscellaneous

1. A. Pothen, S. Jha, and U. Vemulapati, Orthogonal Factorization on a Distributed Memory Multiprocessor, *Hypercube Multiprocessors*, September 1987, edited by M.T. Heath.

2. P. Pardalos and S. Jha, Graph Separation Techniques for Quadratic zero-one Programming, *Computers Math Applications*, Volume 6/7, 1991.

3. P. Pardalos and S. Jha, Complexity of Uniqueness and Local Search in Quadratic 0-1 Programming, *Operations Research Letters*, Volume 11/2, 1992.

GRANTS

Note: I have received several industrial gifts from various companies (e.g., Symantec and Google), but I have only listed my grants that are peer reviewed.

Principal Investigator, “Vulnerability and Information Flow Analysis for COTS”, ONR University Research Initiative, 2001-2006. Award amount: $ 3,000,000.00

Co-Principal Investigator, “Static Analysis to Enhance the Power of Model Checking for Concurrent Software”, ONR University Research Initiative, 2001-2006. Award amount: $ 5,000,000.00
Note: This was a joint project with Carnegie Mellon University (CMU).

Co-Principal Investigator, “Coordinated Anomaly Detection and Characterization in Wide Area Network Flows”, ARO, 2002-2005. Award amount: $ 300,000.00

Principal Investigator, “CAREER: Combating Malicious Behavior in Commodity Software”, NSF, 2005-2009. Award amount: $ 400,000.00

Co-Principal Investigator, “Advanced Methods for Checking Information-Security Properties”, NSF 2005-2008. Award amount: $ 390,000.00

Co-Principal Investigator, “Infrastructure to Support Cyberforensics”, ARO 2005-2006. Award amount: $ 280,000.00

Principal Investigator, “Collaborative Research: CT-T: Towards Behavior-Based Malware Detection”, NSF, 2007-2010. Award amount: $ 560,000.00

Co-Principal Investigator, “CT-ISG: Alternate Representation of NIDS/NIPS Signatures for Fast Matching”, NSF 2007-2010. Award amount: $ 360,000.00

Principal Investigator, “Collaborative Techniques for Botnet Detection”, ARO, 2007-2010. Award amount: 480,000.00
Note: This is a joint project with Stanford University.

Principal Investigator, “An Optimizing Compiler for Secure Function Evaluation”, IARPA 2009-2011. Award amount: $ 980,000.00
Note: This is a joint grant with University of Texas, Austin.

Co-Principal Investigator, “Collaborative Research:Techniques to Retrofit Legacy Code with Security”, NSF 2009-2011. Award amount: $ 1,200,000.00
Note: This is a joint grant with Penn State, Maryland, and Purdue.

Co-Principal Investigator, “Policy weaving for system security”, DARPA CRASH, 2010-2014. Award amount: $ 3,200,000.00

Principal Investigator, “TC: Medium: Collaborative Research: Building Trustworthy Applications for Mobile Devices”, NSF 2010-2015. Award amount: $ 838,818.00
Note: Joint project with Penn State University.

Principal Investigator,”TWC: Phase: Medium: Collaborative: Understanding and Exploiting Parallelism in Deep Packet Inspection on Concurrent Architectures”, NSF 2013-2017. Award amount: $ 999,778.00
Note: Joint project with ICSI, Berkeley.

Principal Investigator, “TWC: Medium: Collaborative: Extending Smart-Phone Application Analysis”, NSF 2013-2017. Award amount: $ 487,101.00
Note: Joint project with Penn State University.

Principal Investigator, “TRACE: Tracing and Analysis of Causality Enterprise-level”, DARPA Transparent Computing (TC), 2014-2018. Award amount: $ 5,100,000.00 (UW share: $ 800,000)
Note: This is a joint project with SRI (lead), Purdue, and University of Georgia.

Principal Investigator, “TWC: Medium: Collaborative: Scaling and Prioritizing Market-Sized Application Analysis”,

NSF 2017-2021. Award amount: $ 599,703.00
Note: This is a joint project with Penn State.

Principal Investigator, “Techniques and Tools for De-bloating Containers”, ONR, Sept-30 2017 to Sept-30 2022. Award amount: $ 6,134,379 (UW share: $ 2,000,000)
Note: This is a joint project with University of Illinois, University of Toronto, Oregon State, and Grammatech.

Principal Investigator, “Robustness and Stability for Data Analysis in Security”, ARO, Aug 1, 2017 to July 30, 2020. Award amount: $ 400,000.00

Principal Investigator, “Automated Protocol Specialization and Diversification for Individualized Defense”, ONR, 08/01/2018 to 07/31/2021. Award amount: $ 3,092,379 (UW share: 800,000)
Note: This is a joint project with Northeastern, SRI, and WPI.

Principal Investigator, “SaTC: CORE: Frontier: Collaborative: End-to-End Trustworthiness of Machine-Learning Systems”, NSF, 10/01/2018 to 09/31/2023. Award amount: $ 10,000,000 (UW share: Variable). **Note:** This is a joint project with Penn State, Stanford, Berkeley, Virginia, and UCSD.

Principal Investigator, “Enhancing ML Robustness Using Physical-World Constraints”, DARPA, 12/01/2019 to 11/31/2023. Award amount: $ 2,800,000 (UW share: Variable). **Note:** This is a joint project with University of Michigan and University of Toronto.

Principal Investigator, “Cohesive and Robust Human-Bot Cybersecurity Teams”, DOD, ARMY, 07/01/2021 to 06/30/2024. Award amount: $3,750,000 (UW share: Variable). **Note:** This is a joint project with Carnegie Mellon University and University of California, San Diego.

Ph.D. Students and Postdocs advising (current)

1. Mohannad Alhanahnah (Postdoc, third year)
2. Jihye Choi (Ph.D, student, second year).
3. Ashish Hooda (Ph.D. student, fourth year).
4. Nils Polumbo (Ph.D. student, fourth year).
5. Zi Wang (Ph.D. student, fifth year).

Ph.D. Students graduated (includes postdoc advisees)

1. Jon Giffin (graduated in Aug 2006).
   First employment: Assistant Professor at Georgia Tech.
2. Shai Rubin (graduated in Aug 2006).
   First employment: Microsoft, Haifa, Israel.
3. Hao Wang (graduated in Dec 2006).
   First employment: Novashield Technologies, Madison, WI.
4. Mihai Christodorescu (graduated in July 2007).
   First employment: IBM, T.J. Watson Research Center, Hawthorne, NY.
5. Vinod Ganapathy (graduated in July 2007).
   First employment: Assistant Professor at Rutgers.
6. Randy Smith (graduated in Aug 2009).
   First employment: Sandia National Laboratories in Albuquerque, NM.

7. Louis Kruger (graduated in Dec 2011).
   First employment: Two Sigma, NY.

8. Bill Harris (graduated in Dec 2014).
   First Employment: Assistant Professor at Georgia Tech.

9. Daniel Luchaup (graduated in Dec 2014).
   First Employment: Postdoctoral Fellow at Cylab, CMU.

10. Matt Fredrikson (graduated in June 2015).
    First Employment: Assistant Professor at Carnegie Mellon University.

11. Damien Octeau (post-doc from Sept 1, 2014 to Sept 1, 2015).
    First Employment: Google.

12. Xi Wu (graduated in July 2016).
    First Employment: Google.

13. Drew Davidson (graduated in Oct 2016).
    First Employment: University of Kansas.

14. Lorenzo De Carli (graduated in Nov 2016).
    First Employment: Colorado State University.

15. Irene Giacomelli (postdoc, Oct 15, 2016 to Apr 30, 2018).
    First Employment: ISI Foundation, Torino, Italy.

16. Maliheh Monshizadeh (postdoc, Feb 1, 2017 to Aug 30, 2018).
    First Employment: Remitly, Seattle, USA.

17. Vaibhav Rastogi (postdoc, Aug 17, 2015 to Aug 30, 2019).
    First Employment: Google, Mountain View, USA.

18. Jinman Zhao (graduated in Jan 2020).
    First Employment: Amazon.

19. Uyeong Jang (graduated in August 2021).
    First Employment: Not known.

20. Amrita Roy Chowdhury (graduated in Dec 2021).
    First Employment: CI Postdoctoral fellow at UCSD (advisor Kamalika Chowdhuri).

21. Jiefeng Cheng (graduated in June 2023).
    First Employment: Applied Scientist at AWS AI Labs.

Selected thesis and prelim committees

1. Xiaozhu Meng (May 2018, Ph.D student at UW-Madison).

2. Calvin Smith (Oct 2018, Ph.D student at UW-Madison).

3. Tony Nowatzki (Dec 2016, Ph.D student at UW-Madison).

4. Robby Cohran (October 2015, Ph.D. student at UNC Chapell Hill).

5. Adam Everspaugh (July 2017, Ph.D student at UW-Madison).

6. Venkatraman Govindaraju (July 2014, Ph.D student at UW-Madison).

7. Aditya Thakur (Aug 2014, Ph.D student at UW-Madison).
8. Ian Alderman (Ph.D student at UW-Madison).
9. Lakshmi N. Bairavasundaram (graduated in 2008 from UW-Madison).
10. Sandeep Bhatkar (graduated in 2007 from SUNY, Stony Brook).
11. Joseph Bockhorst (graduated in 2005 from UW-Madison).
12. Dennis Brylow (graduated in 2003 from Purdue).
13. Scott Diehl (graduated in 2008 from UW-Madison).
14. Stephen Jones (Ph.D. student at UW-Madison)
15. Alexey Loginov (Ph.D student at UW-Madison).
16. Nathan Rosenblum (Ph.D. student at UW-Madison).
17. Oleg Sheyner (graduated in 2004 from Carnegie Mellon).
18. Vinod Yegneswaran (Ph.D. student at UW-Madison).

TEACHING EXPERIENCE

2000-Present Developed two new courses at UW-Madison.
The first course (CS 706) is *Analysis of Software Artifacts*, and
the second course (CS 642) is *Introduction to Information Security*.

1998-1999 Instructor and developer of four new graduate classes at CMU.
I was teaching in the *Masters of Software Engineering* and the
Masters of Computational Finance programs.

1991-1996 I was a teaching assistant for two undergraduate courses at CMU.
Both these courses were advanced algorithms courses for seniors.

1985-1987 Graduate instructor at Penn State.
I taught the introductory programming course for engineers.

SELECTED TALKS

Aug 1995 "Verifying Parametrized Networks using Abstraction and Regular Languages."
Presented at the 6-th International Conference on Concurrency Theory (CONCUR), 1995.

Oct 1996 "Checking Relational Specifications with Binary Decision Diagrams."
Presented at the Fourth Symposium on Foundations of Software Engineering (FSE), 1996.

May 1999 "The potential of portfolio theory in guiding software decisions."
Presented at the first Workshop on Economics-Driven Software Engineering Research (EDSER-1),
Affiliated with the 1999 International Conference on Software Engineering (ICSE).

May 2001 “Survivability Analysis of Networked Systems.”
Presented at the 23-rd International Conference on Software Engineering (ICSE).

June 2001 “Markov Chains, Classifiers, and Intrusion Detection.”
Presented at the 14-th Computer Security Foundations Workshop (CSFW).

July 2001 “WiSA Project Overview.”
Presented at the ONR/OSD CIP/SW URI Kick Off Meeting in Arlington, Virginia.

June 2003 “Static Analysis Techniques for Identifying Malicious Executables”
Presented at the *Software Security Workshop* arranged by
University of Washington, Microsoft, and CMU.

Oct 2003 “Efficient Context-sensitive Intrusion Detection”
Presented at the Computer Science Department, University of Arizona

July 2005 “Malware Detection”
Presented at the Idaho National Labs

Feb 2006 “Behavior-Based Malware Detection”
Frontiers in Computer Science Lecture Series
Computer Science and Engineering Department
University of California, San Diego

Mar 2006 “Distributed Model-Checking Algorithms for WPDS with Applications to Trust-Management Systems”
Invited talk at TACAS 2006, Vienna, Austria.

Nov 2006 “Towards Behavior-Based Malware Detection”
Computer Science Department
Florida International University (FIU), Miami, FL.

Dec 2006 “Towards Behavior-Based Malware Detection”
Computer Science Department
University of Illinois at Urbana-Champaign, Illinois.

Sept 2007 “Retrofitting Legacy Code for Security”
Computer Science Department
State University of New York (SUNY), Stony Brook.

Nov 2008 “Retrofitting Legacy Code for Security”
Invited talk at Program Analysis for Software Tools and Engineering (PASTE).

Dec 2008 “Efficient Signature Matching with Extended Automata”
Keynote address at the 4th International Conference on Information Systems Security.

July 2009 “Retrofitting Legacy Code for Security”
Distinguished Lecture in Technical University of Darmstadt.

July 2010 “Retrofitting Legacy Code for Security”
Invited Talk at Computer Aided Verification (CAV).

Mar 2011 “Retrofitting Legacy Code for Security”
Distinguished Lecture at the University of Illinois, Chicago.

Mar 2011 “Retrofitting Legacy Code for Security”
Distinguished Lecture at the Kansas State University.

Dec 2011 “Retrofitting Legacy Code for Security”
Distinguished Lecture at the University of North Carolina (UNC), Chapel Hill.

Apr 2013 “Retrofitting Legacy Code for Security”
Distinguished Lecture at the University of Oregon.

June 2015 “Thoughts on Retrofitting Legacy Code for Security”
SoS Speaker Seres at the University of Illinois, Urbana Champaigne.

April 2016 “Synthesis Techniques for Security”
Keynote at Hot Issues in Security Principles and Trust, Eindhoven, Netherlands.

July 2018 “Semantic Adversarial Deep Learning”
Invited talk at Computer Aided Verification, Ocford, UK.

Oct 2018 “Towards Semantic Adversarial Examples”
Booz Allen Hamilton Colloquium, University of Maryland, USA.

PROGRAM COMMITTEES (Selected)

- *Computer Aided Verification (CAV)*, Paris, France, 2001.
- *Foundations of Computer Security (FCS)*, Copenhagen, Denmark, 2002.
  This workshop was a part of the 2002 Federated Logic Conference (FLoC’02).
- *International Conference on Software Engineering (ICSE)*, 2003.
- *The 10th International SPIN Workshop on Model Checking of Software*, 2003.
- *WWW 2004 [Security and Privacy Track]*, 2004,
- *International Symposium on Software Testing and Analysis (ISSTA)*, 2004.
- *Second ACM-IEEE International Conference on Formal Methods and Models for Co-design (MEMOCODE)*, 2004.
- *The 12th Annual Network and Distributed System Security Symposium (NDSS’2005).*
- *WWW 2005[Security and Privacy Track]*
- *7th International Conference on Computer Aided Verification (CAV 2005).*
- *14th USENIX Security Symposium*, 2005.
- *The 12th ACM Conference on Computer and Communication Security (CCS 2005).*
- *Eighth International Symposium on Recent Advances in Intrusion Detection (RAID 2005)*
- *Software Engineering for Secure Systems (SESS05)*, 2005.
- *The 3rd Workshop on Rapid Malcode (WORM)*, 2005.
- *15th USENIX Security Symposium*, 2006.

- *9th International Symposium On Recent Advances In Intrusion Detection (RAID)*, 2006.
- *The 13th ACM Conference on Computer and Communication Security (CCS)*, 2006.
- *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2007.
- *IEEE Symposium on Security and Privacy*, 2007.
- *16th USENIX Security Symposium*, 2007.
- *The 14th ACM Conference on Computer and Communication Security (CCS)*, 2007.
- *IEEE Symposium on Security and Privacy*, 2008.
- *17th USENIX Security Symposium*, 2008.
- *The 15th ACM Conference on Computer and Communication Security (CCS)*, 2008.
  Note: I am the program co-chair for this conference.
- *Twelfth International Symposium on Recent Advances in Intrusion Detection (RAID 2009).*
- *The 15th ACM Conference on Computer and Communication Security (CCS)*, 2009.
  Note: I am the program co-chair for this conference.
- Chair of *Thirteenth International Symposium on Recent Advances in Intrusion Detection (RAID 2010).*
- *IEEE Symposium on Security and Privacy*, 2010.
- *19th USENIX Security Symposium*, 2010.
- Co-chair of *IEEE Symposium on Security and Privacy*, 2011.
- *20th USENIX Security Symposium*, 2011.
- *International Symposium on Software Testing and Analysis (ISSTA)*, 2014.
- *Computer Aided Verification*, 2014.
- *Computer Security Foundations (CSF)*, 2014.
- *Symposium on Principles of Programming Languages (POPL)*, 2016.
- *International Conference on Software Engineering (ICSE)*, 2017.
- *IEEE Symposium on Security and Privacy*, 2018.
- *Computer Aided Verification*, 2018.
- *IEEE Symposium on Security and Privacy*, 2019.
- *The 26th ACM Conference on Computer and Communication Security (CCS)*, 2019.

SERVICE (PROFESSIONAL)

- Editorial board of *Journal of Computer Security* (2004-2014).
- Editorial board of *ACM Transactions on Information and System Security (TISSEC)* (2009-2014).
- Chair of the steering committee for the *ACM Conference on Computer and Communications Security (CCS)*, (2014-Present).

- Member of the new publications committee for the ACM (ACM-NPC), (2018-2022).

SERVICE (DEPARTMENTAL)

- Curriculum committee [chair: Remzi Arpaci-Dusseau], Spring and Fall, 2002.
- Admissions committee [chairs: Raghu Ramakrishnan and Chuck Dyer], Spring 2003.
- Arranged the distinguished lecture series, Fall 2003 and Spring 2004.
- Admissions committee [chairs: Raghu Ramakrishnan and Steven Wright], Spring 2005.
- Curriculum committee [chair: Marvin Solomon], Fall 2005 to Spring 2006.
- Admissions committee [chairs: Chuck Dyer and Somesh Jha], Fall 2006 to Spring 2007.
- Admissions committee [chairs: Remzi Arpaci-Dusseau and Somesh Jha], Fall 2007 to Fall 2008.
- Committee for alumni relations, Fall 2010.
- Recruiting and Budget Committee, Fall 2016.
- Undergraduate-advising and Recruiting Committees, Fall 2017.
- Recruiting and Budget Committee, Fall and Spring (2018-2019).
- Chair of Curriculum Committee, (Fall 2023 – Present).

REFEREE FOR CONFERENCES AND JOURNALS (Selected)

Journals

Referee for ACM Transactions on Software Engineering Methodology (TOSEM), IEEE Transactions on Software Engineering (TSE), Formal Methods in Systems Design (FORM), ACM Transactions on Programming Languages and Systems (TOPLAS), Journal of the ACM (JACM), and ACM Transactions on Information and System Security (TISSEC).

Conferences

International Conference on Software Engineering (ICSE), Foundations of Software Engineering (FSE), Computer Aided Verification (CAV), International Conference on Concurrency Theory (CONCUR), IEEE Annual Symposium on Logic in Computer Science (LICS), Principles of Programming Languages (POPL), ACM Conference on Programming Language Design and Implementation (PLDI), and Tools and Algorithms for Construction and Analysis of Systems (TACAS).

Expert Witness Experience

- Intertrust Technologies Corporation v. Apple, Inc., Case No. 4:13-cv-1235 (N.D. Cal): Represented Apple Inc. on behalf of Kirkland & Ellis LLP in a patent infringement action against Intertrust Technologies Corp. entitled Intertrust Technologies.
  Testimony: I did not testify as an expert at trial or by deposition in this case.
- Wang v. Palo Alto Networks, Inc. et al, Case No. 3:12-cv-05579-WHA (N.D. Cal.): Represented plaintiff on behalf of Durie Tangri LLP and Niro, Haller & Niro in a patent infringement action against Palo Alto Networks, inc. and Fengmin Gong.
  Testimony: I did not testify as an expert at trial or by deposition in this case.
- Cellular Communications Equipment LLC v. Microsoft Corp., Case No. 6:13-cv-00738-LED (E.D. Tex.): Represented defendant Microsoft on behalf of Sidley Austin LLP in a patent infringement action.
  Testimony: I did not testify as an expert at trial or by deposition in this case.

- ContentGuard Holdings, Inc. v. Amazon, Inc. et al., 2:13-cv-01112-JRG (E.D. Tex.): Represented Apple Inc. on behalf of Sidley Austin LLP in a patent infringement action against ContentGuard Holdings, Inc. *Testimony:* I did not testify as an expert at trial or by deposition in this case.
- SYMANTEC CORP (Petitioner) v FINJAN, INC. (Patent Owner): Retained by Symantec Corporation (Symantec) on behalf of Bryan Cave, LLP for the Inter Partes Review (IPR) proceeding. This case is ongoing and the expert reports have been filed.
- Apple Inc. v Intertrust Technologies Corp. (Case no. 2:13-cv-01112 (JRG)): Filed a report on behalf of the law firm of Sidley Austin LLP, counsel for Apple Inc., as an expert witness in the above-captioned litigation. The report provided my opinion about the invention dates of certain claims in the following Intertrust Technologies Corp. patents: U.S. Patent Nos. 7,844,835, 8,191,157, and 8,191,158.
- MICROSOFT CORPORATION (Petitioner) v OPTIMUM CONTENT PROTECTION (Patent Owner): Represented Microsoft Corporation (Microsoft) as an expert witness on behalf of Sidley Austin LLP in the above-captioned proceeding. Prepared an Expert Declaration for Inter Partes Review (IPR) of U.S. Patent No. 7,218,923.
  Testimony: I did not testify as an expert in this case.
- Fortinet Inc. v. FireEye Inc. (Case No. 5:13-cv-02496-HSG-PSG): Retained by Quinn Emanuel Urquhart & Sullivan on behalf of Fortinet, Inc. as a consultant in connection with the above mentioned case filed by Fortinet against FireEye. Did preparatory work (i.e., studying patents and prior art), but the case was settled before the expert reports were prepared.
- Finjan vs Rapid 7 Finjan, Inc. v. Rapid7 LLC and Rapid7, Inc. Case No. 1:18-cv-01519-MN (D. Del.) Provided consulting services to Rapid7 LLC and Rapid7, Inc. (collectively, “Rapid7”) in connection with the above-captioned litigation matter involving claims of patent infringement related to 8 patents. Expert reports were submitted, and I was deposed in the case for more than three days (due to Covid the deposition was done online). This case was going to trial but settled around Mar 3, 2023.

INDUSTRIAL EMPLOYMENT and CONSULTING

I worked for four years (1987 to 1991) as a computer consultant before returning for my Ph.D. During these four years I worked on several projects. These projects exposed me to several types of systems, such as compilers, operating systems, and transaction management systems.

- *Consultant to IBM, Danbury, CT*
  AGS consulting, Clarke, NJ
  Aug, 1987–Jan, 1989
  Was involved in the development of `FORTRAN` and `C` compilers for the PS-2 computer. Was responsible for writing code, fixing bugs, and optimizing the compiler.
- *Consultant to UPS, Louisville*
  AGS consulting, Clarke, NJ
  Feb, 1989–July, 1989
  Worked on software for load balancing planes and routing packages. Development was done on a STRATUS machine and code was written in `C`. Code was highly intricate and required interfacing with hardware components using device drivers.
- *Senior Programmer*
  AGS consulting, Clarke, NJ
  Aug, 1989–July, 1990
  Worked on a software for checking whether a `C` program confirms to the POSIX and ANSI standards. This project was done for AT&T.
- *Consultant to IBM, Kingston, NY*
  Pencom, New York, NY
  Sept, 1990–July, 1991
  Worked on porting the OSF kernel to the IBM-ESA architecture. Specifically, I was responsible for porting and maintaining the threads library. The job required me becoming intimately familiar with the threads code on the IBM-ESA architecture.

I have also consulted and worked for a few companies during the last few years.

- *Consultant for Meta (May 1, 2021 – Apr 30, 2022).* Worked on projects related to privacy and machine learning (ML).

- *Full time at Google (Aug 1, 2022 – July 31, 2022).* I was part of the Android Safety and Privacy (ASAP) group. I worked on topics related to Machine Learning. I also worked with the Data-core group. I was heavily involved with Large Language Models (LLMs).
- *Part time (20%) at Google (Aug 1, 2023 – Present).* Continue to work on topics related to machine learning (ML) and privacy and security. I continue also working with topics related to LLMs.

PERSONAL

Born in India and naturalized citizen of the US. I am also an "overseas citizen of india" (OCI card holder).