Curriculum Vitæ of Vinod Ganapathy

Professor
Department of Computer Science and Automation
Indian Institute of Science (IISc)
Bangalore-560012, Karnataka, India

April 15, 2022
vg@iisc.ac.in
http://www.csa.iisc.ac.in/~vg

1. Research Interests

The primary focus of my research is computer security. At IISc, I direct the Computer Systems Security Laboratory. I seek to build practical computer systems with sound security guarantees. My research projects have considered security issues in a broad spectrum of computer systems, from cloud platforms through Web browsers to mobile devices. I have wide-ranging interests, and my projects usually draw on ideas and methods developed in a variety of areas, such as applied cryptography, program analysis, formal methods, machine intelligence, and hardware architecture.

2. Educational Background

- **University of Wisconsin–Madison**, Madison, Wisconsin, USA.
  - ▷ ***Ph.D. in Computer Science*** .... August 2007
    Dissertation title: "*Retrofitting Legacy Code for Authorization Policy Enforcement*" [T1].
    Ph.D. minor in Mathematics.
  - ▷ ***M.S. in Computer Science*** .... May 2003
- **Indian Institute of Technology Bombay**, Powai, Mumbai, India.
  - ▷ ***B.Tech. in Computer Science & Engineering*** .... August 2001
    Thesis title: "*Efficient Verification of Synchronous Programs*" [T2].

3. Employment History

- **Indian Institute of Science**, Bangalore, India.
  - ▷ **Department of Computer Science and Automation**, Division of EECS
    Full Professor .... March 2022 onwards
    Associate Professor .... May 2017–March 2022
  - ▷ **Robert Bosch Centre for Cyber-Physical Systems**, Division of Interdisciplinary Research
    Associate Faculty .... August 2020 onwards
- **Rutgers, The State University of New Jersey**, New Brunswick, New Jersey, USA.
  - ▷ **Department of Computer Science**, School of Arts and Sciences
    Visiting Research Professor .... July 2018–June 2019
    Associate Professor (with tenure) .... July 2013–June 2018
    Assistant Professor .... September 2007–June 2013
- **IBM Thomas J. Watson Research Center**, Hawthorne, New York, USA.
  - ▷ Intern in the Secure Systems Department .... May 2005–August 2005
- **Microsoft Research**, Redmond, Washington, USA.
  - ▷ Intern in the Runtime Analysis and Design Group .... May 2004–August 2004
- **Tata Institute of Fundamental Research**, Colaba, Mumbai, India.
  - ▷ Intern in the Visiting Students' Research Program .... May 2000–July 2000

4. Awards and Distinctions

- Prof. Satish Dhawan State Award for Young Engineers (in Engineering Sciences for the year 2019), awarded by the Government of Karnataka, awarded in October 2021.
- Ramanujan Fellowship, awarded by the Science and Engineering Research Board, Department of Science and Technology, Government of India, July 2017.
- 3rd Professor R. Narasimhan Memorial Lecture Award, Tata Institute of Fundamental Research, Mumbai, India, December 2015.

  Awarded annually by TIFR to one individual under 40 with a degree from an Indian institution, in the field of Computer Science and Technology recognizing advances in hardware, software, theoretical aspects of computing, or applications of computing.
- Keynote speaker at the International Conference on Information Systems Security (ICISS), Kolkata, India, December 2015.
- Rutgers University Board of Trustees Fellowship for Scholarly Excellence, May 2013.

  Citation: "In recognition of his outstanding research in cyber-security and software engineering, and for his ability to find elegant and simple solutions to complex problems across the broad areas of operating systems, mobile devices, and Web platforms."
- National Science Foundation Faculty Early-Career Development (NSF CAREER) Award, 2010.
- Outstanding Student Paper Award at the 25th Annual Computer Security Applications Conference, for paper [C25] with advisee Mohan Dhawan, December 2009.
- Outstanding Student Paper Award at the 24th Annual Computer Security Applications Conference, for paper [C30] with advisee Arati Baliga and collaborator Liviu Iftode, December 2008.
- Visiting Students' Research Scholarship, awarded by Tata Institute of Fundamental Research, Mumbai, India, May 2000.

5. Scientific Publications

5.1 Theses

T1. "Retrofitting Legacy Code for Authorization Policy Enforcement," Vinod Ganapathy, Ph.D. dissertation, University of Wisconsin-Madison, Madison, Wisconsin, USA, August 2007, ISBN: 978-0-549-19468-2. Supervised by Professor Somesh Jha.

T2. "Efficient Verification of Synchronous Programs," Vinod Ganapathy, Bachelor's thesis, Indian Institute of Technology Bombay, Powai, Mumbai, May 2001, Supervised by Professor S. Ramesh.

5.2 Conference Papers

C1. "Faastlane: Accelerating Function-as-a-Service Workflows," Swaroop Kotni, Ajay Nayak, Vinod Ganapathy, and Arkaprava Basu, In *Proceedings of ATC'21, the 2021 USENIX Annual Technical Conference*, Virtual event (originally: Santa Clara, California, USA), July 2021, USENIX Association, pages 957–971. Acceptance: 64/341 (18.7%).

C2. "(Mis)managed: A Novel TLB-based Covert Channel on GPUs," Ajay Nayak, B. Pratheek, Vinod Ganapathy, and Arkaprava Basu, In *Proceedings of AsiaCCS'21, the 16th ACM Asia Conference on Computer and Communications Security*, Virtual event (originally: Hong Kong), June 2021, ACM Press, pages 872–885. DOI:10.1145/3433210.3453077, Acceptance: 70/362 (19.3%).

C3. "Privaros: A Framework for Privacy-Compliant Delivery Drones," Rakesh Rajan Beck, Abishek Vijeev, and Vinod Ganapathy, In *Proceedings of CCS'20, the 27th ACM SIGSAC Conference on Computer and Communications Security*, Virtual event (originally: Orlando, Florida, USA), November 2020, ACM Press, pages 181–194. DOI:10.1145/3372297.3417858, Acceptance: 121/715 (16.9%).

C4. "An Evaluation of Methods to Port Legacy Code to SGX Enclaves," Kripa Shanker, Arun Joseph, and Vinod Ganapathy, In *Proceedings of ESEC/FSE'20, the 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, Virtual event (originally: Sacramento, California, USA), November 2020, ACM Press, pages 1077–1088, Artifact DOI: 10.5281/zenodo.3895761. DOI:10.1145/3368089.3409726, Acceptance: 101/360 (28%).

C5. "ActiveThief: Model Extraction using Active Learning and Unannotated Public Data," Soham Pal, Yash Gupta, Aditya Shukla, Aditya Kanade, Shirish Shevade, and Vinod Ganapathy, In *Proceedings of AAAI'20, the 34th AAAI Conference on Artificial Intelligence*, New York, New York, USA, February 2020, AAAI Press, pages 865–872. DOI:10.1609/aaai.v34i01.5432, Acceptance: 1591/7737 (20.6%).

C6. “Secure, Consistent, and High-Performance Memory Snapshotting,” Guilherme Cox, Zi Yan, Abhishek Bhattacharjee, and Vinod Ganapathy, In *Proceedings of CODASPY’18, the 8th ACM Conference on Data and Application Security and Privacy*, Tempe, Arizona, USA, March 2018, ACM Press, pages 236–247. DOI:10.1145/3176258.3176325, Acceptance: 23/110 (20.9%).

C7. “EnGarde: Mutually-Trusted Inspection of SGX Enclaves,” Hai Nguyen, and Vinod Ganapathy, In *Proceedings of ICDCS’17, the 37th IEEE International Conference on Distributed Computing Systems*, Atlanta, Georgia, USA, June 2017, IEEE Computer Society Press, pages 2458–2465. DOI:10.1109/ICDCS.2017.35, Acceptance: 90/531 (16.9%).

C8. “Regulating ARM TrustZone Devices in Restricted Spaces,” Ferdinand Brasser, Daeyoung Kim, Christopher Liebchen, Vinod Ganapathy, Liviu Iftode, and Ahmad-Reza Sadeghi, In *Proceedings of MobiSys’16, the 14th ACM International Conference on Mobile Systems, Applications, and Services*, Singapore, June 2016, ACM Press, pages 413–425. DOI:10.1145/2906388.2906390, Acceptance: 31/197 (15.7%).

C9. “A Novel Algorithm for Pattern Matching with Back-References,” Liu Yang, Vinod Ganapathy, Pratyusa Manadhata, and Ye Wu, In *Proceedings of IPCCC’15, the 34th IEEE International Performance Computing and Communications Conference*, Nanjing, China, December 2015, IEEE Computer Society Press, pages 1–8. DOI:10.1109/PCCC.2015.7410264, Acceptance: 88/298 (29%).

C10. “Testing Cross-Platform Mobile App Development Frameworks,” Nader Boushehrinejadmoradi, Vinod Ganapathy, Santosh Nagarakatte, and Liviu Iftode, In *Proceedings of ASE’15, the 30th IEEE/ACM International Conference on Automated Software Engineering*, Lincoln, Nebraska, USA, November 2015, IEEE Computer Society Press, pages 441–451. DOI:10.1109/ASE.2015.21, Acceptance: 60/289 (20.7%) for full papers and 77/326 (23.6%) overall.

C11. “Efficient Runtime Enforcement Techniques for Policy Weaving,” Richard Joiner, Thomas Reps, Somesh Jha, Mohan Dhawan, and Vinod Ganapathy, In *Proceedings of FSE’14, the 22nd ACM SIGSOFT International Symposium on the Foundations of Software Engineering*, Hong Kong, November 2014, ACM Press, pages 224–234, Certified by FSE’14 artifact evaluation committee. DOI:10.1145/2635868.2635907, Acceptance: 61/273 (22.3%).

C12. “On the Control Plane of a Self-service Cloud Platform,” Shakeel Butt, Vinod Ganapathy, and Abhinav Srivastava, In *Proceedings of SOCC’14, the 5th ACM Symposium on Cloud Computing*, Seattle, Washington, USA, November 2014, ACM Press, pages 128–140. DOI:10.1145/2670979.2670989, Acceptance: 29/119 (24.3%).

C13. “Retargetting Legacy Browser Extensions to Modern Extension Frameworks,” Rezwana Karim, Mohan Dhawan, and Vinod Ganapathy, In *Proceedings of ECOOP’14, the 28th European Conference on Object-Oriented Programming*, Uppasala, Sweden, July/August 2014, Volume 8586 of *Lecture Notes in Computer Science (LNCS)*, Springer, pages 463–488. DOI:10.1007/978-3-662-44202-9_19, Acceptance: 21/101 (20.8%).

C14. “Inferring Likely Mappings Between APIs,” Amruta Gokhale, Vinod Ganapathy, and Yogesh Padmanaban, In *Proceedings of ICSE’13, the 35th ACM/IEEE International Conference on Software Engineering*, San Francisco, California, USA, May 2013, IEEE Computer Society Press, pages 82–91. DOI:10.1109/ICSE.2013.6606554, Acceptance: 85/461 (18.5%).

C15. “Fast Submatch Extraction using OBDDs,” Liu Yang, Pratyusa Manadhata, William G. Horne, Prasad Rao, and Vinod Ganapathy, In *Proceedings of ANCS’12, the 8th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, Austin, Texas, USA, October 2012, ACM Press, pages 163–174. DOI:10.1145/2396556.2396594, Acceptance: 18/64 (28.1%).

C16. “Leveraging “Choice” to Automate Authorization Hook Placement,” Divya Muthukumaran, Trent Jaeger, and Vinod Ganapathy, In *Proceedings of CCS’12, the 19th ACM SIGSAC Conference on Computer and Communications Security*, Raleigh, North Carolina, USA, October 2012, ACM Press, pages 145–156. DOI:10.1145/2382196.2382215, Acceptance: 81/423 (19.1%).

C17. “Self-service Cloud Computing,” Shakeel Butt, H. Andrés Lagar-Cavilla, Abhinav Srivastava, and Vinod Ganapathy, In *Proceedings of CCS’12, the 19th ACM SIGSAC Conference on Computer and Communications Security*, Raleigh, North Carolina, USA, October 2012, ACM Press, pages 253–264. DOI:10.1145/2382196.2382226, Acceptance: 81/423 (19.1%).

C18. “Enhancing JavaScript with Transactions,” Mohan Dhawan, Chung-chieh Shan, and Vinod Ganapathy, In *Proceedings of ECOOP’12, the 26th European Conference on Object-Oriented Programming*, Beijing, China, June 2012, Volume 7313 of *Lecture Notes in Computer Science (LNCS)*, Springer, pages 383–408. DOI:10.1007/978-3-642-31057-7_18, Acceptance: 30/140 (21.4%).

C19. “An Analysis of the Mozilla Jetpack Extension Framework,” Rezwana Karim, Mohan Dhawan, Vinod Ganapathy, and Chung-chieh Shan, In *Proceedings of ECOOP’12, the 26th European Conference on Object-Oriented Programming*, Beijing, China, June 2012, Volume 7313 of *Lecture Notes in Computer Science (LNCS)*, Springer, pages 333–355. DOI:10.1007/978-3-642-31057-7_16, Acceptance: 30/140 (21.4%).

C20. “Monitoring Data Structures using Hardware Transactional Memory,” Shakeel Butt, Vinod Ganapathy, Arati Baliga, and Mihai Christodorescu, In *Proceedings of RV’11, the 2nd International Conference on Runtime Verification*, San

Francisco, California, USA, September 2011, Volume 7186 of *Lecture Notes in Computer Science (LNCS)*, Springer, pages 345–359. DOI:10.1007/978-3-642-29860-8_26, Acceptance: 32/75 (42.4%).

C21. “K2C: Cryptographic Cloud Storage With Lazy Revocation and Anonymous Access,” Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy, In *Proceedings of SecureComm’11, the 7th International ICST Conference on Security and Privacy in Communication Networks*, London, UK, September 2011, Volume 96 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST)*, Springer, pages 59–76. DOI:10.1007/978-3-642-31909-9_4, Acceptance: 23/95 (24.2%).

C22. “Security versus Energy Tradeoffs in Host-based Mobile Malware Detection,” Jeffrey Bickford, H. Andrés Lagar-Cavilla, Alexander Varshavsky, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of MobiSys’11, the 9th ACM International Symposium on Mobile Systems, Applications, and Services*, Bethesda, Maryland, USA, June/July 2011, ACM Press, pages 225–238. DOI:10.1145/1999995.2000017, Acceptance: 25/141 (17.7%).

C23. “Improving NFA-based Signature Matching using Ordered Binary Decision Diagrams,” Liu Yang, Rezwana Karim, Vinod Ganapathy, and Randy Smith, In *Proceedings of RAID’10, the 13th International Symposium on Recent Advances in Intrusion Detection*, Ottawa, Canada, September 2010, Volume 6307 of *Lecture Notes in Computer Science*, Springer, pages 58–78, Journal version: [J5]. DOI:10.1007/978-3-642-15512-3_4, Acceptance: 24/102 (23.5%).

C24. “Protecting Commodity Operating System Kernels from Vulnerable Device Drivers,” Shakeel Butt, Vinod Ganapathy, Michael M. Swift, and Chih-Cheng Chang, In *Proceedings of ACSAC’09, the 25th Annual Computer Security Applications Conference*, Honolulu, Hawaii, USA, December 2009, IEEE Computer Society Press, pages 301–310. DOI:10.1109/ACSAC.2009.35, Acceptance: 44/226 (19.6%).

C25. “Analyzing Information Flow in JavaScript-based Browser Extensions,” Mohan Dhawan, and Vinod Ganapathy, In *Proceedings of ACSAC’09, the 25th Annual Computer Security Applications Conference*, Honolulu, Hawaii, USA, December 2009, IEEE Computer Society Press, pages 382–391, **Outstanding Student Paper Award**. DOI:10.1109/ACSAC.2009.43, Acceptance: 44/226 (19.6%).

C26. “Detecting Identity Spoofs in 802.11e Wireless Networks,” Gayathri Chandrashekaran, John Austen Francisco, Vinod Ganapathy, Marco Gruteser, and Wade Trappe, In *Proceedings of GLOBECOM’09, the IEEE Global Communications Conference*, Honolulu, Hawaii, USA, November/December 2009, IEEE Press, pages 1–6. DOI:10.1109/GLOCOM.2009.5426152, Acceptance:: 34.8%.

C27. “Privately Querying Location-based Services with SybilQuery,” Pravin Shankar, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of UbiComp’09, the 11th International Conference on Ubiquitous Computing*, Orlando, Florida, USA, September/October 2009, ACM Press, pages 31–40. DOI:10.1145/1620545.1620550, Acceptance: 31/251 (12.35%).

C28. “Working Set-Based Access Control for Network File Systems,” Stephen Smaldone, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of SACMAT’09, the 14th ACM Symposium on Access Control Models and Technologies*, Stresa, Italy, June 2009, ACM Press, pages 207–216. DOI:10.1145/1542207.1542241, Acceptance: 24/75 (32%).

C29. “OMOS: A Framework for Secure Communication in Mashup Applications,” Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy, In *Proceedings of ACSAC’08, the 24th Annual Computer Security Applications Conference*, Anaheim, California, USA, December 2008, IEEE Computer Society Press, pages 355–364. DOI:10.1109/ACSAC.2008.25, Acceptance: 42/173 (24.8%).

C30. “Automatic Inference and Enforcement of Kernel Data Structure Invariants,” Arati Baliga, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of ACSAC’08, the 24th Annual Computer Security Applications Conference*, Anaheim, California, USA, December 2008, IEEE Computer Society Press, pages 77–86, **Outstanding Student Paper Award**. Journal version: [J6]. DOI:10.1109/ACSAC.2008.29, Acceptance: 42/173 (24.8%).

C31. “Enforcing Authorization Policies using Transactional Memory Introspection,” Arnar Birgisson, Mohan Dhawan, Úlfar Erlingsson, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of CCS’08, the 15th ACM SIGSAC Conference on Computer and Communications Security*, Alexandria, Virginia, USA, October 2008, ACM Press, pages 223–234. DOI:10.1145/1455770.1455800, Acceptance: 51/281 (18.1%).

C32. “The Design and Implementation of Microdrivers,” Vinod Ganapathy, Matthew J. Renzelmann, Arini Balakrishnan, Michael M. Swift, and Somesh Jha, In *Proceedings of ASPLOS’08, the Thirteenth International Conference on Architectural Support for Programming Languages and Operating Systems*, Seattle, Washington, USA, March 2008, ACM Press, pages 168–178. DOI:10.1145/1346281.1346303, Acceptance: 31/127 (24.4%).

C33. “Mining Security-Sensitive Operations in Legacy Code using Concept Analysis,” Vinod Ganapathy, David King, Trent Jaeger, and Somesh Jha, In *Proceedings of ICSE’07, the 29th ACM/IEEE International Conference on Software Engineering*, Minneapolis, Minnesota, USA, May 2007, IEEE Computer Society Press, pages 458–467. DOI:10.1109/ICSE.2007.54, Acceptance: 50/334 (15%).

C34. “NetSpy: Automatic Generation of Spyware Signatures for NIDS,” Hao Wang, Somesh Jha, and Vinod Ganapathy, In *Proceedings of ACSAC’06, the 22nd Annual Computer Security Applications Conference*, Miami Beach, Florida, USA, December 2006, IEEE Computer Society Press, pages 99–108. DOI:10.1109/ACSAC.2006.34, Acceptance: 40/132 (30.3%).

C35. “HeapMD: Identifying Heap-based Bugs using Anomaly Detection,” Trishul M. Chilimbi, and Vinod Ganapathy, In *Proceedings of ASPLOS’06, the Twelfth International Conference on Architectural Support for Programming Languages and Operating Systems*, San Jose, California, USA, October 2006, ACM Press, pages 219–228. DOI:10.1145/1168857.1168885, Acceptance: 38/158 (24%).

C36. “Retrofitting Legacy Code for Authorization Policy Enforcement,” Vinod Ganapathy, Trent Jaeger, and Somesh Jha, In *Proceedings of IEEE S&P’06, the 2006 IEEE Symposium on Security and Privacy*, Berkeley/Oakland, California, USA, May 2006, IEEE Computer Society Press, pages 214–229. DOI:10.1109/SP.2006.34, Acceptance: 32/251 (12.7%).

C37. “An Auctioning Reputation System Based on Anomaly Detection,” Shai Rubin, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin, Louis Kruger, Hao Wang, and Nicholas Kidd, In *Proceedings of CCS’05, the 12th ACM SIGSAC Conference on Computer and Communications Security*, Alexandria, Virginia, USA, November 2005, ACM Press, pages 270–279. DOI:10.1145/1102120.1102156, Acceptance: 38/250 (15.2%).

C38. “Automatic Placement of Authorization Hooks in the Linux Security Modules Framework,” Vinod Ganapathy, Trent Jaeger, and Somesh Jha, In *Proceedings of CCS’05, the 12th ACM SIGSAC Conference on Computer and Communications Security*, Alexandria, Virginia, USA, November 2005, ACM Press, pages 330–339. DOI:10.1145/1102120.1102164, Acceptance: 38/250 (15.2%).

C39. “Automatic Discovery of API-Level Exploits,” Vinod Ganapathy, Sanjit A. Seshia, Somesh Jha, Thomas W. Reps, and Randal E. Bryant, In *Proceedings of ICSE’05, the 27th ACM/IEEE International Conference on Software Engineering*, St. Louis, Missouri, USA, May 2005, ACM Press, pages 312–321. DOI:10.1145/1062455.1062518, Acceptance: 44/313 (14%).

C40. “Buffer Overrun Detection using Linear Programming and Static Analysis,” Vinod Ganapathy, Somesh Jha, David Chandler, David Melski, and David Vitek, In *Proceedings of CCS’03, the 10th ACM SIGSAC Conference on Computer and Communications Security*, Washington, DC, USA, October 2003, ACM Press, pages 345–354. DOI:10.1145/948109.948155, Acceptance: 35/253 (13.8%).

5.3 Journal Articles

J1. “SG^{XL}: Security and Performance for Enclaves using Large Pages,” Sujay Yadalam, Vinod Ganapathy, and Arkaprava Basu, *ACM Transactions on Architecture and Code Optimization*, Volume 18, Number 1, December 2020, pages 12:1–12:25, ACM Press. DOI:10.1145/3433983.

J2. “Exploring Infrastructure Support for App-based Services on Cloud Platforms,” Hai Nguyen, Vinod Ganapathy, Abhinav Srivastava, and Shivaramakrishnan Vaidyanathan, *Computers and Security*, Volume 62, Number 1, September 2016, pages 177–192, Elsevier. DOI:10.1016/j.cose.2016.07.009.

J3. “Detecting Plagiarized Mobile Apps using API Birthmarks,” Daeyoung Kim, Amruta Gokhale, Vinod Ganapathy, and Abhinav Srivastava, *Automated Software Engineering*, Volume 23, Number 4, December 2016, pages 591–618, Springer. DOI:10.1007/s10515-015-0182-6.

J4. “Monitoring Integrity using Limited Local Memory,” Yuki Kinebuchi, Shakeel Butt, Vinod Ganapathy, Liviu Iftode, and Tatsuo Nakajima, *IEEE Transactions on Information Forensics and Security*, Volume 8, Number 7, July 2013, pages 1230–1242, IEEE Signal Processing Society. DOI:10.1109/TIFS.2013.2266095.

J5. “Fast, Memory-efficient Regular Expression Matching with NFA-OBDDs,” Liu Yang, Rezwana Karim, Vinod Ganapathy, and Randy Smith, *Computer Networks*, Volume 55, Number 15, October 2011, pages 3376–3393, Elsevier BV, Extends [C23]. DOI:10.1016/j.comnet.2011.07.002.

J6. “Detecting Kernel-Level Rootkits using Data Structure Invariants,” Arati Baliga, Vinod Ganapathy, and Liviu Iftode, *IEEE Transactions on Dependable and Secure Computing*, Volume 8, Number 5, September/October 2011, pages 670–684, IEEE Computer Society Press, Extends [C30]. DOI:10.1109/TDSC.2010.38.

5.4 Workshop Papers

W1. “Regulating Drones in Restricted Spaces,” Abhishek Vijeev, Vinod Ganapathy, and Chiranjib Bhattacharyya, In *Proceedings of HotMobile’19, the 20th International Workshop on Mobile Computing Systems and Applications*, Santa Cruz, California, USA, February 2019, ACM Press, pages 27–32. DOI:10.1145/3301293.3302370, Acceptance: 26/57 (45.6%). One of 20 selected for full oral presentation.

W2. “Short Paper: Compiler Optimizations with Retrofitting Transformations: Is there a Semantic Mismatch?,” Jay Lim, Vinod Ganapathy, and Santosh Nagarakatte, In *Proceedings of PLAS’17, the 12th ACM SIGSAC Workshop on Programming Languages and Analysis for Security*, Dallas, Texas, USA, October 2017, ACM Press, pages 1–7. DOI:10.1145/3139337.3139343, Acceptance: 10/16 (62.5%).

W3. “Assurance for Defense-in-Depth via Retrofitting,” Vinod Ganapathy, Trent Jaeger, Gang Tan, and Christian Skalka, In *Proceedings of LAW’14, the 8th Layered Assurance Workshop*, New Orleans, Louisiana, USA, December 2014, ACM Press, pages 1–10.

W4. “Data-Driven Inference of API Mappings,” Amruta Gokhale, Daeyoung Kim, and Vinod Ganapathy, In *Proceedings of PROMOTO’14, the 2nd Workshop on Programming for Mobile and Touch*, Portland, Oregon, USA, October 2014, ACM Press, pages 29–32. DOI:10.1145/2688471.2688480.

W5. “Short Paper: Enhancing Users’ Comprehension of Android Permissions,” Liu Yang, Nader Boushehrinejadmoradi, Pallab Roy, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of SPSM’12, the 2nd ACM CCS Workshop on Security and Privacy in Mobile Devices*, Raleigh, North Carolina, USA, October 2012, ACM Press, pages 21–26. DOI:10.1145/2381934.2381940, Acceptance: 11/30 (36%).

W6. “Towards a Richer Model of Cloud App Markets,” Abhinav Srivastava, and Vinod Ganapathy, In *Proceedings of CCSW’12, the 4th ACM Cloud Computing Security Workshop*, Raleigh, North Carolina, USA, October 2012, ACM Press, pages 25–30. DOI:10.1145/2381913.2381918, Acceptance: 13/52 (25%).

W7. “The Case for Energy-aware Trust Establishment in Dynamic Networks of Cyber Physical Devices,” Amruta Gokhale, John McCabe, Vinod Ganapathy, and Ulrich Kremer, In *TrustED’11, the First International Workshop on Trustworthy Embedded Devices*, Leuven, Belgium, September 2011.

W8. “Position Paper: The Case for JavaScript Transactions,” Mohan Dhawan, Chung-chieh Shan, and Vinod Ganapathy, In *Proceedings of PLAS’10, the ACM SIGPLAN 5th Workshop on Programming Languages and Analysis for Security*, Toronto, Canada, June 2010, ACM Press, pages 1–7. DOI:10.1145/1814217.1814223.

W9. “Rootkits on Smart Phones: Attacks, Implications and Opportunities,” Jeffrey Bickford, Ryan O’Hare, Arati Baliga, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of HotMobile’10, the 11th International Workshop on Mobile Computing Systems and Applications*, Annapolis, Maryland, USA, February 2010, ACM Press, pages 49–54. DOI:10.1145/1734583.1734596, Acceptance: 15/62 (25%).

W10. “Privacy-aware Identity Management for Client-side Mashup Applications,” Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy, In *Proceedings of DIM’09, the 5th ACM Workshop on Digital Identity Management*, Chicago, Illinois, USA, November 2009, ACM Press, pages 21–30. DOI:10.1145/1655028.1655036.

W11. “Evaluating Attack Amplification in Online Social Networks,” Blase E. Ur, and Vinod Ganapathy, In *W2SP’09, the Web 2.0 Security and Privacy Workshop*, Oakland, California, USA, May 2009.

W12. “Microdrivers: A New Architecture for Device Drivers,” Vinod Ganapathy, Arini Balakrishnan, Michael M. Swift, and Somesh Jha, In *Proceedings of HotOS’07, the 11th Workshop on Hot Topics in Operating Systems*, San Diego, California, USA, May 2007, USENIX Association, pages 85–90. Acceptance: 21/104 (20%).

W13. “Towards Automated Authorization Policy Enforcement,” Vinod Ganapathy, Trent Jaeger, and Somesh Jha, In *Proceedings of SELinux’06, the Second Annual Security Enhanced Linux Symposium*, Baltimore, Maryland, USA, March 2006, pages 7–11.

W14. “Slicing Synchronous Reactive Programs,” Vinod Ganapathy, and S. Ramesh, In *Proceedings of the 1st Workshop on Synchronous Languages, Applications and Programming*, Grenoble, France, July 2002, Volume 65(5) of *Electronic Notes in Theoretical Computer Science (ENTCS)*, Elsevier Press, pages 50–64. DOI:10.1016/S1571-0661(05)80440-2.

5.5 Invited Papers

I1. “Reflections on the Self-service Cloud Computing Project,” Vinod Ganapathy, In *Proceedings of ICISS’15, the 11th International Conference on Information Systems Security*, Kolkata, India, December 2015, Volume 9478 of *Lecture Notes in Computer Science*, Springer, pages 36–57, Invited paper to accompany keynote presentation. DOI:10.1007/978-3-319-26961-0_4.

5.6 Books and Book Chapters

B1. “Proceedings of the 14th International Conference on Information Systems Security, December 17-19, 2018, Bangalore, India,” Vinod Ganapathy, Trent Jaeger, and R. K. Shyamasundar (editors), Volume 11281 of *Lecture Notes in Computer Science*. Springer, December 2018.

B2. “Dynamic Analysis,” Mihai Christodorescu, and Vinod Ganapathy, In *Encyclopedia of Cryptography and Security (2nd Edition)*, H. C. A. van Tilborg and S. Jajodia, editors. Springer, 2011, pages 365–367. DOI:10.1007/978-1-4419-5906-5_836.

B3. “Identifying Systemic Threats to Kernel Data: Attacks and Defense Techniques,” Arati Baliga, Pandurang Kamat, Vinod Ganapathy, and Liviu Iftode, In *Advanced Operating Systems and Kernel Applications: Techniques and Technologies*, Y. Wiseman and S. Jiang, editors. Information Science Reference (IGI Global), September 2009, Chapter 3, pages 46–70. DOI:10.4018/978-1-60566-850-5.ch003.

B4. "Analysis of COTS for Security Vulnerability Remediation," Gogul Balakrishnan, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin, Shai Rubin, Hao Wang, Somesh Jha, Barton P. Miller, and Thomas Reps, In *Department of Defence Sponsored Information Security Research: New Methods for Protecting against Cyber Threats*, C. Wang, S. King, R. Wachter, R. Herklotz, C. Arney, G. Toth, D. Hislop, S. Heise, and T. Combs, editors. Wiley Publishing Inc., July 2007, pages 375–380.

5.7 Patents

P1. "A Method and System For Implementing Privacy Compliance Associated with Host Areas on Agent Devices," Vinod Ganapathy, Rakesh Rajan Beck, and Abhishek Vijeev, Indian Patent Application No. 202141006477, filed on February 14, 2022.

P2. "System and Method for Protection against Side Channel Attacks," Sujay Yadalam Sudarshan, Vinod Ganapathy, and Arkaprava Basu, United States Patent Application Number 17/092,471, filed on November 9, 2020.

P3. "Richer Model of Cloud App Markets," Abhinav Srivastava, and Vinod Ganapathy, United States Patent 9,542,216 B2, issued on January 10, 2017.

P4. "Balancing Malware Rootkit Detection with Power Consumption on Mobile Devices," Horacio Andres Lagar-Cavilla, Jeffrey Bickford, Vinod Ganapathy, Liviu Iftode, and Alexander Varshavsky, United States Patent 8,566,935 B2, issued on October 22, 2013.

P5. "Heap-Based Bug Identification using Anomaly Detection," Trishul M. Chilimbi, and Vinod Ganapathy, United States Patent 7,770,153 B2, issued on August 3, 2010.

5.8 Refereed Posters

O1. "User Request as a means to Automate Authorization Hook Placement (poster)," Divya Muthukumaran, Trent Jaeger, and Vinod Ganapathy, In *2012 IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2012.

O2. "Enhancing Mobile Malware Detection with Social Collaboration (poster paper)," Liu Yang, Vinod Ganapathy, and Liviu Iftode, In *Proceedings of SocialCom'11, the 3rd International Conference on Social Computing*, Boston, Massachusetts, USA, October 2011, IEEE Press, pages 572–576. DOI:10.1109/PASSAT/SocialCom.2011.176.

O3. "Analyzing Information Flow in JavaScript-based Browser Extensions (poster)," Mohan Dhawan, and Vinod Ganapathy, In *2009 IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2009.

O4. "Rootkits: Now a Threat to Smart Phones (poster)," Ryan O'Hare, Jeffrey Bickford, Arati Baliga, Vinod Ganapathy, and Liviu Iftode, In *Spring Undergraduate Research Symposium: sponsored by Columbia Undergraduate Science Journal and Engineering Student Council*, New York, New York, USA, April 2009, **Best Poster Award**.

O5. "Automatic Inference and Enforcement of Kernel Data Structure Invariants (poster)," Arati Baliga, Vinod Ganapathy, and Liviu Iftode, In *17th USENIX Security Symposium*, San Jose, California, USA, July 2008.

O6. "Enforcing Authorization Policies using Transactional Memory Introspection (poster)," Arnar Birgisson, Mohan Dhawan, Úlfar Erlingsson, Vinod Ganapathy, and Liviu Iftode, In *17th USENIX Security Symposium*, San Jose, California, USA, July 2008.

5.9 Selected Technical Reports

TR1. "Remote Driving: A Ready-to-go Approach to Autonomous Cars? Opportunities and Challenges," Ruilin Liu, Kostas Bekris, Ahmed Elgammal, Vinod Ganapathy, Mario Gerla, Liviu Iftode, Melchi Michel, and Jingang Yi, Technical Report DCS-TR-712, Department of Computer Science, Rutgers University, Piscataway, New Jersey, USA, February 2015.

6. Research Funding

6.1 Funded Projects at the Indian Institute of Science

Share of total grant funding acquired at IISc: Rs. 7,93,76,100.

- "*Security and Privacy for Smart Cities*," National Security Council; Participant in the effort led by the Indian Urban Data Exchange (IUDX) at IISc (project sanctioned in August 2021); Personal share: **Rs. 1,75,95,000** (effective August 2021-August 2024).

- "*Technology Innovation Hub in Cyber-security for Cyber-physical Infrastructure*," National Mission on Interdisciplinary Cyber Physical Systems (NM-ICPS); Department of Science and Technology, Government of India; Participant in the effort led by the Indian Institute of Technology, Kanpur (project sanctioned in March 2020); **IISc PIs**: Vinod Ganapathy, Arpita Patra; Total grant amount is approximately Rs. 100 crores; IISc's share: **Rs. 5,19,23,000** (effective July 2021-July 2026).
- "*Obfuscating Page Accesses to Defend Against Page Address-based Side-channel Attacks on Intel SGX*," Intel Technology India Pvt. Ltd.; PIs: Vinod Ganapathy, Arkaprava Basu; December 2019 onwards; **Rs. 14,16,000**.
- "*Systems Support for Reliable, Secure and High-performance Autonomous Navigation*," Robert Bosch Centre for Cyber-Physical Systems Grant; PIs: Vinod Ganapathy, Arkaprava Basu, Deepak D'Souza; April 2019-March 2020; **Rs. 22,00,000**.
- "*Mobile Payment Systems for the Internet of Things Era*," Interdisciplinary Cyber Physical Systems (ICPS) Programme, Department of Science and Technology; PI: Kanchi Gopinath, **co-PI**: Vinod Ganapathy; March 2019-March 2022; **Rs. 24,42,100**.
- "*Regulating Smart Devices in Restricted Spaces*," Ramanujan Fellowship, Department of Science and Technology/Science and Engineering Research Board; **PI**: Vinod Ganapathy; October 2017-October 2022; **Rs. 38,00,000**.

6.2 Funded Projects at Rutgers University

Total grant funding acquired at Rutgers University: US $3,732,547.

- "*SaTC:STARSS: Hardware-assisted Methods for Operating System Integrity*," NSF Secure and Trustworthy Cyberspace Program—Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (CNS-1441724); **PI**: Vinod Ganapathy; co-PIs: Santosh Nagarakatte and Liviu Iftode; October 2014-September 2017; **$499,988**.
- "*TWC:Small: Self-service Cloud Computing*," NSF Secure and Trustworthy Cyberspace Program (CNS-1420815); **PI**: Vinod Ganapathy; October 2014-September 2017; **$499,880**.
- "*Secure Computation*," Microsoft Research India, October 2014; **$25,000**.
- "*TWC:Medium:Collaborative Research: Retrofitting Software for Defense-in-Depth*," NSF Secure and Trustworthy Cyberspace Program (CCF-1408803); PI: Trent Jaeger (Pennsylvania State University), **co-PIs**: Vinod Ganapathy (Rutgers University), Christian Skalka (University of Vermont), and Gang Tan (Lehigh University); September 2014-August 2018; **$300,000** (Rutgers share; total grant amount was $1,200,000).
- Rutgers Board of Trustees Fellowship for Scholarly Excellence, May 2013; **$1,500**.
- "*Information Flow Integrity for Systems of Independently-Developed Components*," US Air Force Office of Scientific Research (AFOSR) Multi-University Research Initiative (FA9550-12-1-0166); PI: Trent Jaeger (Pennsylvania State University), **co-PIs**: Vinod Ganapathy, Patrick McDaniel (Pennsylvania State University), and Somesh Jha (University of Wisconsin-Madison); April 2012-March 2015; **$265,000** (Rutgers share; total grant amount was $729,466).
- "*STIR: Detecting Malicious Software on Mobile Devices*," US Army RDECOM: Research, Development, and Engineering Command (60583-CS-II); **PI**: Vinod Ganapathy, co-PI: Liviu Iftode; December 2011-September 2012; **$50,000**.
- "*TC:Small: Exploring Malware Detection on Mobile Platforms*," NSF Cross-Cutting Program on Trustworthy Computing (CNS-1117711); PI: Liviu Iftode, **co-PI**: Vinod Ganapathy; September 2011-August 2015; **$457,750**.
- Participant in Microsoft Research Project Hawaii: received ten AT&T Samsung Focus phones for instructional use in the Fall 2011 semester.
- "*Research on Privacy, Security, and Mobile Computing*," NEC Laboratories America, jointly with Liviu Iftode, October 2010; **$40,000**.
- "*CAREER: Improving Software Assurance using Transactions*," NSF Faculty Early-Career Development Program (CNS-0952128); **PI**: Vinod Ganapathy; September 2010-August 2015; **$400,000**.
- "*Advanced Techniques to Detect Emerging Threats from Rootkit-based Malware*," Grant from the US Army Research, Development, and Engineering Command (RDECOM)/Communications-Electronics Research, Development and Engineering Center (CERDEC)/Space and Terrestrial Communications Directorate (STCD)

Cyber Security and Information Assurance Division; September 2009-August 2010; Funding for one graduate student for one calendar year; Value: **$91,428**.

- "*CPS:Small:Collaborative Research: Establishing Integrity in Dynamic Networks of Cyber Physical Devices*," NSF Cyber Physical Systems Program (CNS-0931992); **PI**: Vinod Ganapathy, co-PIs: Ulrich Kremer and Trent Jaeger (Pennsylvania State University); September 2009-August 2013; **$355,000** (Rutgers share; total grant amount was $540,000).
- "*TC:Small:Collaborative Research: Protecting Commodity Operating Systems from Vulnerable Device Drivers*," NSF Cross-Cutting Program on Trustworthy Computing (CNS-0915394); **PI**: Vinod Ganapathy, co-PI: Michael M. Swift (University of Wisconsin); September 2009-August 2013; **$250,000** (Rutgers share; total grant amount was $500,000).
- "*Energy-Efficient Security for Dynamic Networks of Resource-Constrained Devices*," Rutgers University Computing Coordination Council (CCC) Green Computing Initiative; **PI**: Vinod Ganapathy, co-PI: Ulrich Kremer; September 2009-August 2010; **$40,000**.
- Sun Microsystems, equipment donation: one Sun T5220 (Niagara 2) machine, July 2009.
- "*CT-ISG: Advanced Techniques to Detect Kernel-Level Rootkits*," NSF Cyber Trust Program (CNS-0831268); **PI**: Vinod Ganapathy, co-PI: Liviu Iftode; September 2008-August 2012; **$450,001**. (Original grant amount of $400,000 for CNS-0831268 was supplemented by $50,001 via grant CNS-1063674 in September 2010).
- "*Security Enforcement using Transactional Memory*," Rutgers University School of Arts and Sciences, Grant Proposal Development Competition; **PI**: Vinod Ganapathy; July 2008-May 2009; **$3,000**.
- "*Security Enforcement using Transactional Memory*," Rutgers University Research Council Grants Program; **PI**: Vinod Ganapathy; July 2008-May 2009; **$4,000**.

7. Presentations

7.1 Presentations at Universities and Industrial Laboratories

- "*Delivery Drones and Citizen Privacy*,"
  - ▷ Conference on Artificial Intelligence, Plaksha University, Mohali, India, April 28, 2022.
  - ▷ Communications of the ACM India Region Workshop, March 23, 2022.
- "*Regulating Smart Devices in Restricted Spaces*,"
  - ▷ CSAW'19 Workshop, Indian Institute of Technology, Kanpur, India, November 6, 2019.
  - ▷ Volvo India, Bangalore, India, August 1, 2019.
  - ▷ Sonata Software, Bangalore, India, April 11, 2019.
  - ▷ IISc AI day, Bangalore, India, March 13, 2019.
  - ▷ Air Force Technical College, Bangalore, India, August 2, 2018.
  - ▷ Indian National Academy of Engineering (INAE) Engineers' Conclave, Bangalore, India, September 15, 2017.
  - ▷ Microsoft Research India, Bangalore, India, August 5, 2016.
  - ▷ CSA Dept., Indian Institute of Science, Bangalore, India, December 10, 2015.
- "*How to Securely Snapshot Memory*,"
  - ▷ EECS Symposium, Indian Institute of Science, Bangalore, India, March 2, 2018,
- "*Policies and Mechanisms for Operating System Security*,"
  - ▷ CSA Dept., Indian Institute of Science, Bangalore, India, August 8, 2016.
- "*Self-service Cloud Computing*,"
  - ▷ Keynote address at the 11th International Conference on Information Systems Security (ICISS), Kolkata, India, December 19, 2015.
  - ▷ Professor R. Narasimhan Memorial Lecture, Tata Institute of Fundamental Research, Mumbai, India, December 17, 2015.

  - ▷ Microsoft Research India, Bangalore, India, May 26, 2014.
  - ▷ CSA Dept., Indian Institute of Science, Bangalore, India, May 22, 2014.
  - ▷ Trusted Infrastructure Workshop, Pennsylvania State University, State College, Pennsylvania, June 6, 2013.
  - ▷ CS Dept., Rutgers University, Piscataway, New Jersey, September 6, 2012.
- "*Rootkit-based Attacks and Defenses: Past, Present, and Future*,"
  - ▷ Pennsylvania State University, State College, Pennsylvania, October 27, 2011.
  - ▷ IEEE North Jersey Chapter, Teaneck, New Jersey, September 29, 2011.
  - ▷ Columbia University, New York, New York, September 21, 2011.
- "*The Mobile Malware Landscape: A Survey of the Past, Present, and Future of Malicious Software on Smart Phones*," Verizon Wireless, Warren, New Jersey, October 18, 2012.
- "*Detecting Kernel-Level Rootkits using Data Structure Invariants*,"
  - ▷ Symantec Research Laboratories, August 17, 2010.
  - ▷ NEC Laboratories America, Princeton, New Jersey, June 15, 2010.
  - ▷ Security and Privacy Day, Brooklyn Polytechnic Institute, New York, December 4, 2009.
  - ▷ CS Dept., Rutgers University, Piscataway, New Jersey, November 30, 2009.
- "*Analyzing Information Flow in JavaScript-based Browser Extensions*,"
  - ▷ Microsoft Research, Redmond, Washington, February 25, 2010.
  - ▷ 2nd ICT FORWARD Workshop, Saint-Jean-Cap-Ferrat, France, May 4, 2009.
- "*Enforcing Security Policies using Transactional Memory Introspection*,"
  - ▷ CSA Dept., Indian Institute of Science, Bangalore, India, August 12, 2009.
  - ▷ NEC Laboratories America, Princeton, New Jersey, February 13, 2009.
  - ▷ NYC area S&P day, IBM TJ Watson Research Center, Hawthorne, New York, December 5, 2008.
  - ▷ UCLA-IPAM Workshop on Applications of Internet Multi-Resolution Analysis to Cyber-Security, Los Angeles, California, October 13, 2008.
  - ▷ State University of New York, Stony Brook, New York, May 16, 2008.
- "*Retrofitting Legacy Code for Security*,"
  - ▷ Summer School on Cryptography and Software Security, Pennsylvania State University, State College, Pennsylvania, May 30-June 1, 2012.
  - ▷ DIMACS Mixer Series, Bell Labs, Murray Hill, New Jersey, October 23, 2007.
  - ▷ Ph.D. thesis defense, Madison, Wisconsin, July 12, 2007.
  - ▷ Rutgers University, Piscataway, New Jersey, April 10, 2007.
  - ▷ North Carolina State University, Raleigh, North Carolina, March 30, 2007.
  - ▷ Microsoft Research India, Bangalore, India, March 22, 2007.
  - ▷ Purdue University, West Lafayette, Indiana, February 26, 2007.
  - ▷ Pennsylvania State University, University Park, Pennsylvania, February 21, 2007.
  - ▷ IBM T.J. Watson Research Center, Hawthorne, New York, February 8, 2007.
  - ▷ IBM Research India, Bangalore, India, July 7, 2006.
  - ▷ Google, Bangalore, India, June 28, 2006.
  - ▷ CSA Dept., Indian Institute of Science, Bangalore, India, June 19, 2006.
  - ▷ First Midwest Security Workshop, Chicago, Illinois, May 6, 2006.

7.2 Conference Presentations

- "*On the Control Plane of a Self-service Cloud Platform*," 5th ACM Symposium on Cloud Computing, Seattle, Washington, November 4, 2014.

- "*The Case for JavaScript Transactions*," 5^{th} ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, Toronto, Canada, June 10, 2010.
- "*Mining Security-Sensitive Operations in Legacy Code using Concept Analysis*," 29^{th} International Conference on Software Engineering, Minneapolis, Minnesota, May 25, 2007.
- "*Microdrivers: A New Architecture for Device Drivers*," 11^{th} International Workshop on Hot Topics in Operating Systems, San Diego, California, May 8, 2007.
- "*HeapMD: Identifying Heap-based Bugs using Anomaly Detection*," Twelfth International Conference on Architectural Support for Programming Languages and Operating Systems, San Jose, California, October 24, 2006.
- "*Retrofitting Legacy Code for Authorization Policy Enforcement*," 2006 IEEE Symposium on Security and Privacy, Oakland, California, May 23, 2006.
- "*Towards Automated Authorization Policy Enforcement*," Second Annual Security-enhanced Linux Symposium, Baltimore, Maryland, March 1, 2006.
- "*Automatic Placement of Authorization Hooks in the Linux Security Modules Framework*," 12^{th} ACM Conference on Computer and Communications Security, Alexandria, Virginia, November 10, 2005.
- "*Automatic Discovery of API-Level Exploits*," 27^{th} International Conference on Software Engineering, St. Louis, Missouri, May 19, 2005.
- "*Buffer Overrun Detection Using Linear Programming and Static Analysis*," 10^{th} ACM Conference on Computer and Communications Security, Washington, DC, October 30, 2003.

8. Publicly-released Software and Research Artifacts

Links to these artifacts are available at: `http://www.csa.iisc.ac.in/~vg/software`

- **Privaros**. A mandatory access control framework for ROS2-based platforms, such as drones. *Related papers:* [C3].
- **Porpoise**. A toolkit to port applications to SGX enclaves. *Related papers:* [C4].
- **AndroCrypt**. An encrypting obfuscator for Android Apps. *Related papers:* [J3].
- **JAMScript** and **JAMWeave**. Transactional policy-enforcement system for JavaScript code, built atop Firefox-17.0.5esr. *Related papers:* [C11], [C18].
- **Self-service Cloud Platform**. A set of enhancements to the Xen 3.4.0 hypervisor to implement virtual machine abstractions and a hypervisor privilege model that protects client code and data from untrusted cloud administrators. *Related papers:* [C12], [C17].
- **NFA-OBDDs**. Code and data for an implementation of NFA-based regular expression matching using ordered binary-decision diagrams (OBDDs). *Related papers:* [J5], [C23].
- **Sabre**. A JavaScript information-flow tracking system tailored for the analysis of Firefox extensions, built atop Firefox-2.0.0.9. *Related papers:* [C25].
- **Gibraltar**. A Xen-based kernel rootkit detection system that uses data structure invariants, built atop Xen-3.4.2. *Related papers:* [J6], [C22], [C30].
- **Microdrivers**. Benchmark device drivers used in the evaluation sections of our paper on Microdrivers. *Related papers:* [C32].
- **Authorization hook mining.** Datasets reported in our work on automated mining of security-sensitive operations to be mediated by authorization hooks. *Related papers:* [C33].

9. Media Coverage and Appearances

- Research on privacy-compliant delivery drones covered in:
  - ▷ "*Eyes on the Skies*," ACM News, February 2, 2021.
  - ▷ "*Enabling Privacy-Compliant Drones*," Featured article on the Indian Institute of Science main page, February 2021.
  - ▷ "*Drone delivery: IISc devises privacy aid*," Times of India, February 8, 2021.

  - ▷ Indian Institute of Science Annual Report 2018-19, page 108.

- Research on smart phone rootkits covered in over 90 media outlets, including:
  - ▷ "*Can clever hackers target smart phones?*," NSF Press Release 10-052 and Webcast, April 2, 2010.
  - ▷ "*Rutgers researchers show new security threat against smart phone users*," Rutgers University News Release, February 22, 2010.
  - ▷ "*Smart phones expose users to clever attacks*," National Science Foundation (NSF) News, February 22, 2010.
  - ▷ "*Predicting smart phone attacks*," MIT Technology Review, February 22, 2010.
  - ▷ "*Hacked smart phones could be used to spy on you*," TechNewsDaily, February 22, 2010.
  - ▷ "*New smart phone security threat identified*," United Press International, February 24, 2010.
  - ▷ "*Is it time to start thinking about smart phone viruses?*," Los Angeles Times, February 24, 2010.
  - ▷ "*Is your mobile phone spying on you?*," National Geographic News, February 22, 2010.
  - ▷ "*Software turns your cell phone against you*," ABC News and Discovery News, March 14, 2010.
- Research on device driver security mentioned in the MIT Technology Review: "*The Achilles' Heel of Your Computer*," MIT Technology Review, June 30, 2010.
- Statement on a security breach in an US Army database: "*CECOM data breach may not be last. Expert: CECOM attack ongoing 'game'*," Asbury Park Press, January 7, 2013.
- Radio interview: "*Internet Safety*," WVPH 90.3 FM "The Core," (a Rutgers and Piscataway-based radio station) June 27, 2015.

10. Instructional Experience

10.1 Courses Taught at the Indian Institute of Science

Semester	Course	Course Title	Students	Student Evaluation	
				Instructor	Course
Fall 2021	E0-359	Topics in Computer Systems Security	11	4.50/5	4.00/5
Spring 2021	E0-253	Operating Systems	13	4.71/5	4.86/5
Autumn 2020	E0 256	Computer Systems Security	37	5.00/5	5.00/5
Spring 2020	E0 253	Operating Systems	19	4.25/5	4.38/5
Autumn 2019	E0 256	Computer Systems Security	60	4.48/5	4.27/5
Spring 2019	E0 253	Operating Systems	26	4.40/5	4.21/5
Autumn 2018	E0 256	Computer Systems Security	44	4.61/5	4.52/5
Spring 2018	E0 253	Operating Systems	15	4.62/5	4.62/5
Autumn 2017	E0 256	Computer Systems Security	12	4.80/5	4.75/5

Note: All courses taught at IISc are graduate-level courses. Course evaluations were collected by IISc's Digital Campus and Information Technology Services using anonymous surveys.

10.2 Courses Taught at Rutgers University

Semester	Course	Course Title	Students	Student Evaluation	
				Instructor	Course
Fall 2016	16:198:546	Computer Systems Security	14	5.00/5	4.83/5
Spring 2016	01:198:419	Computer Security	65	4.27/5	4.22/5
Fall 2015	16:198:546	Computer Systems Security	26	4.58/5	4.63/5
Spring 2015	01:198:419	Computer Security	40	4.93/5	4.60/5
Spring 2015	01:198:416	Operating System Design	51	(Substitute for L. Iftode)	
Spring 2015	16:198:518	Operating System Design	17	(Substitute for L. Iftode)	

Fall 2014	16:198:546	Computer Systems Security	15	4.40/5	4.20/5
Fall 2014	01:198:416	Operating System Design	57	3.81/5	3.81/5
Fall 2014	16:198:518	Operating System Design	20	3.73/5	4.00/5
Spring 2014	01:198:419	Computer Security	35	4.20/5	4.07/5
Fall 2013	16:198:546	Computer Systems Security	16	4.58/5	4.58/5
Spring 2013	01:198:419	Computer Security	39	4.69/5	4.56/5
Fall 2012	16:198:671	Topics in Mobile App Development and Analysis	4	3.75/5	3.75/5
Spring 2012	01:198:419	Computer Security	31	4.63/5	4.63/5
Fall 2011	16:198:671	Computer Systems Security	10	4.80/5	4.60/5
Spring 2011	*Pre-tenure teaching relief*				
Fall 2010	01:198:419	Computer Security	14	4.67/5	4.67/5
Spring 2010	16:198:500	Light Seminar in Mobile Computing	10	-	-
Spring 2010	01:198:419	Computer Security	27	4.65/5	4.65/5
Fall 2009	01:198:416	Operating System Design	48	3.85/5	3.91/5
Spring 2009	16:198:671	Introduction to Software Security	18	4.80/5	4.70/5
Fall 2008	01:198:442	Introduction to Computer Security	18	4.07/5	3.67/5
Fall 2008	01:198:500	Browser and Web Security	16	4.57/5	4.62/5
Spring 2008	01:198:442	Introduction to Computer Security	16	4.78/5	4.56/5
Fall 2007	16:198:673	Introduction to Software Security	20	4.78/5	4.61/5
Fall 2007	16:198:500	Light Seminar: Systems and Security Issues in Mobile Personal Computing	16	4.80/5	4.18/5

Note: 01:198:... are undergraduate-level courses and 16:198:... are graduate-level courses. All student evaluations were collected by the Rutgers Center for Teaching Advancement and Assessment Research using anonymous surveys.

10.3 Courses Taught Elsewhere

- Lecturer, online course on Computer Systems Security, offered by the Karnataka State Centre of Excellence in Cyber Security (CySecK), May 1-July 31, 2021.
- Coordinator and Lecturer, 2019 ACM India Summer School on Detection and Analysis of Malware, Pune, June 17-28, 2019.
- Lecturer, 7th CSA Undergraduate Summer School, Indian Institute of Science, Bangalore, July 17, 2019.
- Lecturer, 5th CSA Undergraduate Summer School, Indian Institute of Science, Bangalore, July 7, 2017.
- Course content creator, Cyber Security program, JerseySTEM, February 2017. Designed and created the syllabus and teaching materials for a Cyber Security mini-course targetted towards middle-school and high-school children. The course is to be offered by JerseySTEM, a non-profit organization aimed at disseminating science, technology, engineering and mathematics courses to school children in Chatham, Newark and Elizabeth, New Jersey.
- Lecturer, Summer School on Cryptography and Software Security, Pennsylvania State University, State College, Pennsylvania, May 30-June 1, 2012.
- Keynote speaker, 2010 Northern New Jersey JSHS: Junior Science and Humanities Symposium (March 2010). Lectured to a group of about 100 high-school students on the threat of malware and malware detection technologies.

11. Student Supervision and Mentoring Experience

11.1 Post-doctoral Research Supervision

- Arati Baliga, postdoctoral scholar at Rutgers University during May 2009–September 2009. I also helped supervise a part of the research that went into Arati's Ph.D. dissertation, "*Automated Detection and Containment of Stealth Attacks on the Operating System Kernel*," DOI: 10.7282/T33B60FK.

  - External recognition during Ph.D. study and postdoc: Outstanding student paper award at ACSAC'08; Significant coverage in the popular press and by the NSF for work on smartphone rootkits (HotMobile'10).
  - First employment: AT&T Security Research Center, New York City.

11.2 Ph.D. Degree Supervision as Thesis Advisor

- Daeyoung Kim, Ph.D. degree in Computer Science, Rutgers University, granted January 2019.
  - Ph.D. dissertation: "*Regulating Smart Devices in Restricted Spaces.*" DOI: 10.7282/t3-c6kf-j713
  - First employment: Assistant Professor, Montclair State University, Montclair, New Jersey, USA.
- Hai Nguyen, Ph.D. degree in Computer Science, Rutgers University, granted October 2018.
  - Ph.D. dissertation: "*Exploring Security Support for Cloud-based Services.*" DOI: 10.7282/t3-dre3-gm67
  - First employment: Bloomberg, Princeton, New Jersey, USA.
- Rezwana Karim, Ph.D. degree in Computer Science, Rutgers University, granted October 2015.
  - Ph.D. dissertation: "*Techniques and Tools for Secure Web Browser Extension Development.*" DOI: 10.7282/T3000433.
  - External recognition during Ph.D. study: Best paper award at ISEC'15.
  - First employment: Samsung Research America, Mountain View, California, USA.
- Amruta Gokhale, Ph.D. degree in Computer Science, Rutgers University, granted October 2015.
  - Ph.D. dissertation: "*Similarity Detection Techniques for Mobile Platform Artifacts.*" DOI: 10.7282/T3J38VJN.
  - First employment: Teradata Hadapt, Cambridge, Massachusetts, USA.
- Shakeel Butt, Ph.D. degree in Computer Science, Rutgers University, granted January 2015.
  - Ph.D. dissertation: "*Self-service Cloud Computing.*" DOI: 10.7282/T3930VWX.
  - First employment: NVidia, Santa Clara, California, USA.
- Liu Yang, Ph.D. degree in Computer Science, Rutgers University, granted May 2013.
  - Ph.D. dissertation: "*New Pattern Matching Algorithms for Network Security Applications.*" DOI: 10.7282/T3513WS6.
  - First employment: HP ArcSight, Sunnyvale, California, USA.
- Mohan Dhawan, Ph.D. degree in Computer Science, Rutgers University, granted May 2013.
  - Ph.D. dissertation: "*Rethinking Web Platform Extensibility.*" DOI: 10.7282/T38P5Z39.
  - External recognition during Ph.D. study: Outstanding student paper award at ACSAC'09; Best paper nominee at IMC'12.
  - First employment: IBM Research – India, New Delhi, India.
- Saman Zarandioon (co-advised with Professor Danfeng Yao), Ph.D. degree in Computer Science, Rutgers University, granted May 2012.
  - Ph.D. dissertation: "*Improving the Security and Usability of Cloud Services with User-Centric Security Models.*" DOI: 10.7282/T3PC31B4.
  - First employment: Amazon.com, Seattle, Washington, USA.
- *Current students.*
  - Kripa Shanker (August 2017-now): Ph.D. Comprehensive Examination completed in August 2019.
  - Arun Joseph (January 2019-now): Ph.D. Comprehensive Examination completed in April 2021.
  - Nikita Yadav (October 2020-now).

11.3 Masters Degree Supervision

11.3.1 Research-based Masters Students

The following students completed their masters research under my supervision. A masters-by-research degree requires the student to submit a thesis that will be reviewed by an external committee member, and the student defends this thesis in a Ph.D.-thesis-defense-like oral presentation.

- Nikhil Agrawal, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted October 2022.
    - M.Tech. thesis: "*An Evaluation of Basic Protection Mechanisms in Financial Apps on Mobile Devices.*"
    - First employment: CradleWise, Bangalore, India.
- Rounak Agarwal, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted October 2021.
    - M.Tech. thesis: "*A Trusted Hardware-Backed Secure Payments Platform for Android.*" Archival copy: IISc Library 2005/5439.
    - First employment: NVidia, Bangalore, India.
- Rakesh Rajan Beck, M.Tech. degree in Computer Science and Engineering, Indian Insitute of Science, granted October 2021.
    - M.Tech. thesis: "*A Framework for Privacy-Compliant Delivery Drones.*" Archival copy: IISc Library 2005/5223.
    - First employment: Citrix Systems, Bangalore, India.
- Ajay Ashok Nayak, M.Tech. degree in Computer Science and Engineering, Indian Insitute of Science, granted June 2021.
    - M.Tech. thesis: "*Design, Implementation, and Analysis of a TLB-based Covert Channel on GPUs.*"
    - First employment: Ph.D. Candidate, Department of Computer Science and Automation, Indian Institute of Science, Bangalore.
- Aditya Shukla, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2020.
    - M.Tech. thesis: "*Model Extraction and Active Learning.*" Archival copy: IISc Library 2005/4420.
    - First employment: ShareChat, Bangalore, India.
- Subhendu Malakar, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted April 2020.
    - M.Tech. thesis: "*Experiences in Using Reinforcement Learning for Directed Fuzz Testing.*" Archival copy: IISc Library 2005/5130.
    - First employment: Cohesity India, Bangalore, India.
- Yogesh Padmanabhan, M.S. degree in Computer Science, Rutgers University, granted January 2013.
    - M.S. thesis: "*Learning API Mappings Between Programming Platforms.*" DOI: 10.7282/T3GX498K.
    - First employment: Microsoft Corporation, Redmond, Washington, USA.
- Jeffrey Bickford, M.S. degree in Computer Science, Rutgers University, granted January 2012.
    - M.S. thesis: "*Rootkits on Smart Phones: Attacks, Implications, and Energy-Aware Defense Techniques.*" DOI: 10.7282/T3RJ4HHW.
    - External recognition during M.S. study: Significant coverage in the popular press and by the NSF for work on smartphone rootkits (HotMobile'10).
    - First employment: AT&T Security Research Center, New York City.
- *Current students.* Chinmay Gameti (January 2020-now), Gokulnath Pillai (January 2021-now), Nikhil Agrawal (January 2020-now).

11.3.2 Masters Project Students

- A. Akash, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2021.
    - M.Tech. project: "*Studies on Multi-Cloud FaaS Applications.*"
    - First employment: AMD India, Bangalore, India.

- Sreepada Abhinivesh, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2020.
  - ▷ M.Tech. project: "*Anomaly Detection with Sparse Training Data.*"
  - ▷ First employment: Wells Fargo, Bangalore, India.
- Nikita Yadav, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2020.
  - ▷ M.Tech. project: "*Bug-Finding Methods for Permissioned Blockchain Implementations.*"
  - ▷ First employment: Ph.D. Candidate, Department of Computer Science and Automation, Indian Institute of Science, Bangalore.
- Rishabh Ravindra Meshram, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2020.
  - ▷ M.Tech. project: "*Analysis of the SAFE Remote Proctoring System.*"
  - ▷ First employment: Mindtree, Bangalore, India.
- Zad Basheer, M.Tech. degree in Computer Science and Engineering, Indian Institute of Science, granted July 2018.
  - ▷ M.Tech. project: "*Security Analysis of Mobile Payment Applications.*"
  - ▷ First employment: Walmart Labs, Bangalore, India.
- *Current students.* Eikansh Gupta (May 2021-now), Isha Bansal (May 2021-now), Himanshu Kumar (May 2022-now), Vivek Kumar (May 2022-now), Dhruv Shah (May 2022-now).

11.4 Undergraduate Student Supervision

- *Rutgers University Independent Study Supervision.* Arman Shanjani (Fall 2014), Michael Verderese (Summer 2013), Vaibhav Verma (Fall 2012), Jerry Reptak (Fall 2012), Tyler Neely (Fall 2011-Spring 2012), Kanwar Gill (Fall 2011), David Wong (Spring 2011), Jeffrey Bickford (Fall 2008-Spring 2009), Ryan O'Hare (Fall 2008-Spring 2009), Jan Jajalla (Spring 2009).
- *DIMACS Summer Project Students.* Nathan Harper (CS, Vassar College, DIMACS REU student, Summer 2009).

11.5 Other Student Supervision

Participated in the New Jersey Governor's School for Engineering and Technology at Rutgers University and supervised the following high-school students from New Jersey:

- July 2013, Supervised Rohan Mathur, Vivian Mo, Kavinayan Sivakumar, and Jonathan Vielstich for the project "*Exploring methods to develop cross-platform mobile apps.*"
- July 2012, Supervised Emily Bridges, Dhriti Kishore and Joeseph Pedo for the project "*Android app security analysis.*"
- July 2011, Supervised Sydney Becker, Karan Hiremath, and Robert Zhao for the project "*A study of Android permissions and how applications use them.*"
- July 2010, Supervised Caleb Levine, Reid McKenzie, Matthew Mikolay, Tara Nealon, and Vincent Sparacio for the project "*Extension-based security exploits in Firefox.*"
- July 2008, Supervised Mitchell Dorrell, Layal Rustom, Jed Schmidt, and Steven Tricanowicz for the project "*A multidimensional analysis of malicious software.*"

11.6 Ph.D. and Masters Thesis Defense Committee Membership

- Guilherme Mota Cavalcanti De Albuquerque Cox, Ph.D. in Computer Science, Rutgers University, "*Improving and Complementing Virtual Memory using Hardware Techniques*," September 2018, advisor: Professor Abhishek Bhattacharjee.
- Ruilin Liu, Ph.D. in Computer Science, Rutgers University, "*Capturing and Analyzing Human Driving Behavior to Improve Road Travel Experience*," September 2017, advisor: Professor B. R. Badrinath.

- Daehan Kwak, Ph.D. in Computer Science, Rutgers University, "*Supporting Route Choice via Real-time Visual Traffic Information and Counterfactual Arrival Times*," May 2017, advisor: Professor B. R. Badrinath.
- Andrey Chudnov, Ph.D. in Computer Science, Stevens Institute of Technology, "*Inlined Information Flow Monitoring for Web Applications in JavaScript*," April 2016, advisor: Professor David Naumann.
- Jason Perry, Ph.D. in Computer Science, Rutgers University, "*Putting Secure Computation to Work*," May 2015, advisor: Professor Rebecca Wright.
- Parveen Sevusu, M.S. in Computer Science, Rutgers University, "*Real-time Air Quality Measurements using Mobile Platforms*," December 2014, advisors: Professors Liviu Iftode and Badri Nath.
- Andrew Tjang, Ph.D. in Computer Science, Rutgers University, "*Model-based Validation for Operator Mistakes*," June 2014, advisor: Professor Thu Nguyen.
- Pravin Shankar, Ph.D. in Computer Science, Rutgers University, "*Improving Performance, Privacy and Relevance of Location-based Services for Mobile Users*," May 2011, advisor: Professor Liviu Iftode.
- Stephen Smaldone, Ph.D. in Computer Science, Rutgers University, "*Improving the Performance, Availability and Security of Data Access for Opportunistic Mobile Computing*," April 2011, advisor: Professor Liviu Iftode.
- Gayathri Chandrashekaran, Ph.D. in Computer Science, Rutgers University, "*Direct Inference of Location-related Context from Wireless Signal Strength*," April 2011, advisor: Professor Richard Martin.
- Nitya Vyas, M.S. in Computer Science, Rutgers University, "*Usable We 2.0 Privacy Management and Medical Imaging Search: An Ontological Approach*," March 2010, advisor: Professor Danfeng Yao.
- Bruno Dufour, Ph.D. in Computer Science, Rutgers University, "*Practical Analysis of Framework-intensive Applications*," December 2009, advisor: Professor Barbara Ryder.
- Arati Baliga, Ph.D. in Computer Science, Rutgers University, "*Automated Detection and Containment of Stealth Attacks on the Operating System Kernel*," December 2008, advisor: Professor Liviu Iftode.
- Gang Xu, Ph.D. in Computer Science, Rutgers University, "*Trusted Application Centric Ad Hoc Network*," August 2008, advisor: Professor Liviu Iftode.
- Weiqing Sun, Ph.D. in Computer Science, State University of New York (SUNY) Stony Brook, "*Practical Information Flow Based Techniques to Safeguard Host Integrity*," May 2008, advisor: Professor R. Sekar.

11.7 Other Committees (Ph.D. Qualifying Exams, etc.)

P. Habeeb (Advisor: Professor Deepak D'Souza), Ullas Aparanji (Advisor: Professor Y. N. Srikant), Divya Ravi (Advisor: Professor Arpita Patra), Bo Liu (advisor: Professor Dimitris Metaxas), Fatma Betül Durak (advisor: Professor David Cash), David Menendez (advisor: Professor Santosh Nagarakatte), Nader Boushehrinejadmoradi (advisor: Professor Liviu Iftode), Lin Zhong (advisor: Professor Dimitris Metaxas), Kevin Sanik (advisor: Professor Doug DeCarlo), Joseph Wegehaupt (advisor: Professor Chung-chieh Shan), John Asmuth (advisor: Professor Michael Littman), Xiaoxu Wang (advisor: Professor Dimitris Metaxas), Vivek Pathak (advisor: Professor Liviu Iftode), Yuchi Huang (advisor: Professor Dimitris Metaxas).

12. Service to the Profession and University

12.1 Conference and Workshop Organization

- Program Committee chair, ICISS 2018: 14th International Conference on Information Systems Security, Bangalore, India, December 16-20, 2018.
- Co-organizer, with Thomas Ristenpart and Ari Juels, of the DIMACS Workshop on Secure Cloud Computing, organized as part of the DIMACS Special Focus on CyberSecurity, Piscataway, New Jersey, March 27-28, 2014.
- Workshops chair, ASIACCS 2014: 9th ACM Symposium on Information, Computer and Communications Security, Kyoto, Japan, June 2-6, 2014.

12.2 Journal Editorial Boards

- Associate Editor, IEEE Transactions on Dependable and Secure Computing (TDSC), 2018-2020.
- Associate Editor, Sadhana—Academy Proceedings in Engineering Sciences, Indian Academy of Sciences.

12.3 Conference Program Committee Membership

- Usenix Security 2022: 31st USENIX Security Symposium, Boston, Massachusetts, August 10-12, 2022.
- EMSOFT 2020: 20th International Conference on Embedded Software, Shanghai, China, October 11-16, 2020.
- ASIACCS 2020: 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, June 2-5, 2020.
- NDSS 2020: 27th Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 20-23, 2020.
- SysTEX 2019: 4th Workshop on System Software for Trusted Execution, Huntsville, Ontario, Canada, October 27, 2019.
- EMSOFT 2019: 19th International Conference on Embedded Software, New York City, USA, October 13-18, 2019.
- ASIACCS 2019: 14th ACM Asia Conference on Computer and Communications Security, Auckland, New Zealand, July 7-12, 2019.
- ASIACCS 2018: 13th ACM Asia Conference on Computer and Communications Security, Incheon, South Korea, June 4-8, 2018.
- ASIACCS 2017: 12th ACM Asia Conference on Computer and Communications Security, Abu Dhabi, April 2-6, 2017.
- ICISS 2016: 12th International Conference on Information Systems Security, Jaipur, India, December 16-20, 2015.
- CCS 2016: 23rd ACM Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016.
- ICISS 2015: 11th International Conference on Information Systems Security, Kolkata, India, December 16-20, 2015.
- CCS 2015: 22nd ACM Conference on Computer and Communications Security, Denver, Colorado, October 12-16, 2015.
- SecureComm 2015: 11th International Conference on Security and Privacy in Communication Networks, Dallas, Texas, October 26-29, 2015.
- SPACE 2015: 5th International Conference on Security, Privacy, and Applied Cryptography Engineering, Jaipur, India, October 3-7, 2015.
- ISEC 2015: 8th India Software Engineering Conference, Bangalore, India, February 18-20, 2015.
- ICISS 2014: 10th International Conference on Information System Security, Hyderabad, India, December 16-20, 2014.
- CCS 2014: 21st ACM Conference on Computer and Communications Security, Scottsdale, Arizona, November 3-7, 2014.
- SACMAT 2014: 19th ACM Symposium on Access Control Models and Technologies, London, Ontario, Canada, June 25-27, 2014.
- CCGrid 2014: Workshop on Assured Cloud Computing, at the 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Chicago, Illinois, May 26-29, 2014.
- NDSS 2014: 21st Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 23-26, 2014.
- ICISS 2013: 9th International Conference on Information System Security, Kolkata, India, December 16-20, 2012.
- SecureComm 2013: 9th International Conference on Security and Privacy in Communication Networks, Sydney, Australia, September 25-27, 2013.
- Oakland-W2SP 2013: 2013 Workshop on Web 2.0 Security and Privacy, San Francisco, California, May 24, 2013.
- PLAS 2013: 8th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, Seattle, Washington, June 20, 2013.

- CCGrid 2013: Workshop on Assured Cloud Computing, at the 13^{th} IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Delft, The Netherlands, May 13-16, 2013.
- ICISS 2012: 8^{th} International Conference on Information System Security, Guwahati, India, December 15-19, 2012.
- SecureComm 2012: 8^{th} International Conference on Security and Privacy in Communication Networks, Padua, Italy, September 3-6, 2012.
- Oakland-W2SP 2012: 2012 Workshop on Web-2.0 Security and Privacy, San Francisco, California, May 2012.
- CCS-SSPM 2011: 1^{st} ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Chicago, Illinois, October 17, 2011.
- SecureComm 2011: 7^{th} International Conference on Security and Privacy in Communication Networks, London, UK, September 7-9, 2011.
- ICDCS 2011: 31^{st} International Conference on Distributed Computing Systems – Security and Privacy Track, Genoa, Italy, June 21-25, 2010.
- ESSoS 2011: 3^{rd} International Symposium on Engineering Secure Software and Systems, Madrid, Spain, February 9-10, 2011.
- CCS 2010: 17^{th} ACM Conference on Computer and Communications Security, Chicago, Illinois, October 4-8, 2010.
- Usenix Security 2010: 19^{th} USENIX Security Symposium, Washington, DC, August 9-13, 2010.
- ICDCS 2010: 30^{th} International Conference on Distributed Computing Systems – Security and Privacy Track, Genoa, Italy, June 21-25, 2010.
- NDSS 2010: 17^{th} Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 28-March 3, 2010.
- ICISS 2009: 5^{th} International Conference on Information System Security, Calcutta, India, December 14-18, 2009.
- ACSAC 2009: 25^{th} Annual Computer Security Applications Conference, Honolulu, Hawaii, December 7-11, 2009.
- ASIAN 2009: 13^{th} Annual Asian Computing Science Conference, Urumqi, China, October 8-10, 2009.
- ICSE-SESS 2009: 5^{th} International Workshop on Software Engineering for Secure Systems, Vancouver, Canada, May 19, 2009.
- Usenix Security 2009: 18^{th} USENIX Security Symposium, Montreal, Canada, August 10-14, 2009.
- ASIACCS 2009: 4^{th} ACM Symposium on Information, Computer and Communication Security, Sydney, Australia, March 17-19, 2009.
- NDSS 2009: 16^{th} Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 8-11, 2009.
- ICISS 2008: 4^{th} International Conference on Information Systems Security, Hyderabad, India, December 16-20, 2008.
- ACSAC 2008: 24^{th} Annual Computer Security Applications Conference, Anaheim, California, December 8-12, 2008.
- CCS 2008: 15^{th} ACM Conference on Computer and Communications Security, Alexandria, Virginia, October 27-31, 2008.
- NDSS 2008: 15^{th} Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 11-13, 2008.

12.4 Membership in Panels and Other Community Forums

- Member, cybersecurity course curriculum design committee, All India Council for Technical Education, October 2021 onwards.
- Member of Expert Committee, Phase-II of the Indo-Max Planck Centre for Computer Science (IMPECS), IIT-Delhi, 2017-2020.
- Panelist for National Science Foundation (NSF) proposal reviews, 2012, 2013, 2015, 2016.

- Invited Speaker, Summer Schools on Cryptography and Software Security, Pennsylvania State University, State College, Pennsylvania, May 30-June 1, 2012.
- Invited Participant, INCO-TRUST Workshop on International Cooperation in Security and Privacy—International Data Exchange with Security and Privacy: Applications, Policy, Technology and Use, New York City, New York, May 3-5, 2010.
- Invited Participant, 2nd ICT-FORWARD Workshop, Saint-Jean-Cap-Ferrat, France, May 4-5, 2009.

12.5 Other Reviewing Activities

- *Journals, as a referee:* Journal of Computer Security (JCS), Communications of the ACM (CACM), ACM Computing Surveys, ACM Transactions on Internet Technology (TOIT), ACM Transactions on Information and System Secutity (TISSEC), IEEE Transactions on Software Engineering (TSE), IEEE Transactions on Cloud Computing (TCC), IEEE Transactions on Parallel and Distributed Systems (TPDS)–special issue on Trust, Security and Privacy in Parallel and Distributed Systems, IEEE Pervasive Computing, Computer Networks–The International Journal of Computer and Telecommunications Networks (COMNET).
- *Conferences and Workshops, as an external reviewer:* IEEE Symposium on Security and Privacy, IEEE Computer Security Foundations Symposium, ACM Conference on Computer and Communications Security, USENIX Security Symposium, ISOC Symposium on Networked and Distributed Systems Security, USENIX Annual Technical Conference, International Symposium on High-Performance Computer Architecture, International World Wide Web Conference, International Conference on Computer-Aided Verification, International Conference on Tools and Algorithms for the Construction and Analysis of Systems, ACM SIGPLAN SIGACT Symposium on the Principles of Programming Languages, ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, ACM SIGSOFT International Symposium on Foundations of Software Engineering, Workshop on Software Engineering for Secure Systems, ACM SIGSOFT International Symposium on Software Testing and Analysis, Formal Methods and Models for Codesign.
- *Other:* Proposal reviewer for the Army Research Office (ARO), 2008.

12.6 Governmental Service

- Co-chair of Technical Committee and Member of Standing Committee, Karnataka State Centre of Excellence in Cybersecurity (CySecK), September 2018 onwards.

12.7 University and Departmental Service

- At the Department of Computer Science and Automation, Indian Institute of Science:
  - ▷ Chair, Examination Committee, Programming Test for M.Tech. (CSE) Admissions, April 2022–May 2022.
  - ▷ Project PI, Wells Fargo Corporate Social Responsibility grant (Rs. 1,09,00,000) to set up a departmental laboratory for security, intelligent systems and computer systems-related instructional activities, March 2021–March 2022.
  - ▷ Chair, Cyber Security Committee, to investigate a cyber security incident on campus, and to provide recommendations to the IISc IT team on cyber safety moving forward, September 2020–June 2021.
  - ▷ Co-organizer, IISc + CySecK H.A.C.K. "Meet the startups" day, September 11, 2020.
  - ▷ Secured funding from McAfee India (Rs. 45,000) to sponsor the Best M.Tech. project award in the CSA department, July 2020.
  - ▷ Prime Minister's Research Fellowship selection committee, June 2020–January 2021.
  - ▷ Member, Faculty Search Committee, September 2020–now.
  - ▷ Member, Departmental Finance Committee, September 2019–now.
  - ▷ Member, Departmental Curriculum Committee, May 2019–August 2020.
  - ▷ Coordinator, International Student Admission, March 2019.
  - ▷ Member, EECS Research Performance Evaluation Committee, Autumn 2018.
  - ▷ Coordinator and Chair, Narendra Summer Internship program, Summer 2018.
  - ▷ Coordinator, Systems Stream, Mid-year Research Interviews, November 2017.

- ▷ Faculty Coordinator, Global Cyber Challenge Peace-a-thon (sponsored by the Ministry of Electronics and Information Technology), November 2017.

- At the Department of Computer Science, Rutgers University:
  - ▷ Web committee (chair, 2012-2016). Responsible for overseeing all aspects of the Rutgers Department of Computer Science Web site.
  - ▷ Undergraduate advising committee (2008-2015).
  - ▷ Graduate committee (2010-2012).
  - ▷ Graduate admissions committee (2007-2009).
  - ▷ MS admissions committee (2016-2017).
  - ▷ Merit increase review committee (2015-2016).
  - ▷ Faculty hiring committee (2009-2012, 2015-2016).
  - ▷ Faculty advisor to RuSec, the Rutgers Students in Cyber Security club (2015-2017).
  - ▷ Co-organizer, New York area Security and Privacy day (May 2009).
- Member, Board of Trustees, Rutgers-Livingston Day Care Center, September 2014-August 2016.
- At the Department of Computer Science, University of Wisconsin: Incoming graduate student transition committee, constituted by students' chapter of the ACM (Spring 2002).

12.8 Collaboration with Industry

- Research consultancy agreement with Pulse Secure, Bangalore, India. Joint work on network anomaly detection (October 2018–September 2019).
- Research collaboration agreement with AT&T Research, Florham Park, New Jersey. Joint work on security and privacy in cloud computing (July 2011-March 2016).
- Joint study agreement with IBM Thomas J. Watson Research Center, Hawthorne, New York. Collaboration on the design and implementation of security monitors using transactional memory introspection (January 2009-January 2010).
- Technology transfer to Grammatech Inc., Ithaca, New York. Lead the design, implementation and evaluation of a buffer overrun detection tool using CodeSurfer™ (September 2001–August 2003).

12.9 Society Memberships

- Member of the IEEE and ACM.
- Member of the IIT Bombay Alumni Association (lifetime member from 2015 onwards).

13. Personal Information

- **Particulars**: Born September 1979 in Bangalore, India. Married, one son.
- **Nationality**: Citizen of India.
- **Spoken Languages**: Native/bilingual in English and Tamil, fluent in Hindi and Kannada, conversant in Malayalam.