Vinod Ganapathy

Department of Computer Science	Tel: (732) 445-2001 x5027
Rutgers, the State University of New Jersey	Fax: (732) 445-0537
110 Frelinghuysen Road (Office: CoRE 309)	E-mail: `vinodg@cs.rutgers.edu`
Piscataway, New Jersey 08854-8019, USA	`http://www.cs.rutgers.edu/~vinodg`

1 Research Interests

Computer security and reliability with a focus on improving software quality. Specific research topics include techniques to retrofit legacy software for security, novel security enforcement mechanisms, Web and browser security, operating system security, and malware detection.

2 Academic Appointments

- **Rutgers University**, New Brunswick, New Jersey, USA ..... September 2007 onwards
  Assistant Professor of Computer Science.

3 Education

- **University of Wisconsin**, Madison, Wisconsin, USA.
  - ***Ph.D. in Computer Science*** ..... August 2007
    Thesis: "Retrofitting Legacy Code for Authorization Policy Enforcement" [1]
    Advisor: Professor Somesh Jha.
    Minor degree: Mathematics (Algebra and Logic).
  - ***M.S. in Computer Science*** ..... May 2003
- **Indian Institute of Technology Bombay**, Mumbai, India.
  - ***B.Tech. in Computer Science & Engineering*** ..... August 2001
    Thesis: "Efficient Verification of Synchronous Programs" [2]
    Advisor: Professor S. Ramesh.

4 Previous Work Experience

- University of Wisconsin, Madison, Wisconsin, USA .....September 2001–August 2007
  Graduate Research Assistant
- IBM T.J. Watson Research Center, Hawthorne, New York, USA .....May 2005–August 2005
  Intern (Secure Systems Department)
- Microsoft Research, Redmond, Washington, USA .....May 2004–August 2004
  Intern (Runtime Analysis and Design Group)
- Indian Institute of Technology Bombay, Mumbai, India .....July 2000–May 2001
  Undergraduate Research Assistant

- Tata Institute of Fundamental Research, Mumbai, India .....May 2000–July 2000
  Intern (Visiting Students' Research Program)

5 Distinctions

- Best Student Paper Award at ACSAC 2008 (for conference paper [4]).
- Visiting Students' Research Scholarship, awarded by Tata Institute of Fundamental Research, Mumbai (May 2000).

6 Scientific Publications

Electronic copies of these papers are available at `http://www.cs.rutgers.edu/~vinodg/papers`

Theses

[1] "Retrofitting Legacy Code for Authorization Policy Enforcement," Vinod Ganapathy, PhD dissertation, University of Wisconsin-Madison, Madison, Wisconsin, USA, August 2007.

[2] "Efficient Verification of Synchronous Programs," Vinod Ganapathy, Senior thesis, Indian Institute of Technology Bombay, Powai, Mumbai, May 2001.

Refereed Conference Papers

[3] "OMOS: A Framework for Secure Communication in Mashup Applications," Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy, In *ACSAC'08: Proceedings of the 24th Annual Computer Security Applications Conference*, Anaheim, California, USA, December 2008, IEEE Computer Society Press, pages TBD. Accepted 42 out of 173 papers (24.8%).

[4] "Automatic Inference and Enforcement of Kernel Data Structure Invariants," Arati Baliga, Vinod Ganapathy, and Liviu Iftode, In *ACSAC'08: Proceedings of the 24th Annual Computer Security Applications Conference*, Anaheim, California, USA, December 2008, IEEE Computer Society Press, pages TBD, **Awarded Best Student Paper**. Accepted 42 out of 173 papers (24.8%).

[5] "Enforcing Authorization Policies using Transactional Memory Introspection," Arnar Birgisson, Mohan Dhawan, Úlfar Erlingsson, Vinod Ganapathy, and Liviu Iftode, In *ACM CCS'08: Proceedings of the 15th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, October 2008, ACM Press, pages 223–234. Accepted 51 out of 281 submissions (18.1%).

[6] "The Design and Implementation of Microdrivers," Vinod Ganapathy, Matthew J. Renzelmann, Arini Balakrishnan, Michael M. Swift, and Somesh Jha, In *ASPLOS'08: Proceedings of the Thirteenth International Conference on Architectural Support for Programming Languages and Operating Systems*, Seattle, Washington, USA, March 2008, ACM Press, pages 168–178. Accepted 31 out of 127 submissions (24.4%).

[7] "Mining Security-Sensitive Operations in Legacy Code using Concept Analysis," Vinod Ganapathy, David King, Trent Jaeger, and Somesh Jha, In *ICSE'07: Proceedings of the 29th ACM/IEEE International Conference on Software Engineering*, Minneapolis, Minnesota, USA, May 2007, IEEE Computer Society Press, pages 458–467. Accepted 50 out of 334 submissions (15%).

[8] "NetSpy: Automatic Generation of Spyware Signatures for NIDS," Hao Wang, Somesh Jha, and Vinod Ganapathy, In *ACSAC'06: Proceedings of the 22nd Annual Computer Security Applications Conference*, Miami Beach, Florida, USA, December 2006, IEEE Computer Society Press, pages 99–108. Accepted 40 out of 132 submissions (30.3%).

[9] "HeapMD: Identifying Heap-based Bugs using Anomaly Detection," Trishul M. Chilimbi, and Vinod Ganapathy, In *ASPLOS'06: Proceedings of the Twelfth International Conference on Architectural Support for Programming Languages and Operating Systems*, San Jose, California, USA, October 2006, ACM Press, pages 219–228. Accepted 38 out of 158 submissions (24%).

[10] "Retrofitting Legacy Code for Authorization Policy Enforcement," Vinod Ganapathy, Trent Jaeger, and Somesh Jha, In *IEEE S&P'06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, Berkeley/Oakland, California, USA, May 2006, IEEE Computer Society Press, pages 214–229. Accepted 32 out of 251 submissions (12.7%).

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

[12] "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 *ACM CCS'05: Proceedings of the 12th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, November 2005, ACM Press, pages 270–279. Accepted 38 out of 250 submissions (15.2%).

[13] "Automatic Placement of Authorization Hooks in the Linux Security Modules Framework," Vinod Ganapathy, Trent Jaeger, and Somesh Jha, In *ACM CCS'05: Proceedings of the 12th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, November 2005, ACM Press, pages 330–339. Accepted 38 out of 250 submissions (15.2%).

[14] "Automatic Discovery of API-Level Exploits," Vinod Ganapathy, Sanjit A. Seshia, Somesh Jha, Thomas W. Reps, and Randal E. Bryant, In *ICSE'05: Proceedings of the 27th ACM/IEEE International Conference on Software Engineering*, St. Louis, Missouri, USA, May 2005, ACM Press, pages 312–321. Accepted 44 out of 313 submissions (14%).

[15] "Buffer Overrun Detection using Linear Programming and Static Analysis," Vinod Ganapathy, Somesh Jha, David Chandler, David Melski, and David Vitek, In *ACM CCS'03: Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington, DC, USA, October 2003, ACM Press, pages 345–354. Accepted 35 out of 253 submissions (13.8%).

Refereed Workshop Papers

[16] "Microdrivers: A New Architecture for Device Drivers," Vinod Ganapathy, Arini Balakrishnan, Michael M. Swift, and Somesh Jha, In *HotOS'07: Proceedings of the 11th Workshop on Hot Topics in Operating Systems*, San Diego, California, USA, May 2007, USENIX Association, pages 85–90. Accepted 21 out of 104 submissions (20%).

[17] "Slicing Synchronous Reactive Programs," Vinod Ganapathy, and S. Ramesh, In *Electronic Notes in Theoretical Computer Science (Proceedings of the 1st Workshop on Synchronous Languages, Applications and Programming, Grenoble, France)*, F. Maraninchi, A. Girault, and E. Rutten, editors, Volume 65. Elsevier Press, April 2002.

Book Chapters

[18] "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.

Patents

[19] "System for Automatic Detection of Spyware," Somesh Jha, Hao Wang, and Vinod Ganapathy, Patent Application filed with the United States Patent Office, November 29, 2006.

[20] "Heap-Based Bug Identification using Anomaly Detection," Trishul M. Chilimbi, and Vinod Ganapathy, Patent Application Number 20060265694, filed with the United States Patent Office, May 20, 2005.

Posters

[21] "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.

[22] "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.

Technical Reports (not published elsewhere)

[23] "Working Set-Based Access Control for Network File Systems," Stephen Smaldone, Vinod Ganapathy, and Liviu Iftode, Technical Report DCS-TR-643, Department of Computer Science, Rutgers University, Piscataway, New Jersey, USA, November 2008.

7 Research Grants

- "NSF 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 2011; $400,000.
- "Security Enforcement using Transactional Memory," Rutgers University School of Arts and Sciences Grant Proposal Development Competition; PI: Vinod Ganapathy; July 2008-May 2009; $3000.
- "Security Enforcement using Transactional Memory," Rutgers University Research Council Grants Program; PI: Vinod Ganapathy; July 2008-May 2009; $4000.

8 Presentations

Conference Presentations

- "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.

Invited Presentations

- "Enforcing Security Policies using Transactional Memory Introspection,"
  - NYC area Security and Privacy 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.
  - CS Dept., State University of New York, Stony Brook, New York, May 16, 2008.
- "Retrofitting Legacy Code for Security,"

- DIMACS Mixer Series, Bell Labs, Murray Hill, New Jersey, October 23, 2007.
- CS Dept., Rutgers University, New Brunswick, New Jersey, April 10, 2007.
- CS Dept., North Carolina State University, Raleigh, North Carolina, March 30, 2007.
- Microsoft Research India, Bangalore, India, March 22, 2007.
- CS Dept., Purdue University, West Lafayette, Indiana, February 26, 2007.
- CSE Dept., Pennsylvania State University, University Park, Pennsylvania, February 21, 2007.
- IBM T.J. Watson Research Center, Hawthorne, New York, February 8, 2007.

Other Presentations to the Research Community

- "Retrofitting Legacy Code for Authorization Policy Enforcement,"
  - Ph.D. thesis defense, Madison, Wisconsin, July 12, 2007.
  - IBM Research India, Bangalore, India, July 7, 2006.
  - Google Inc., Bangalore, India, June 28, 2006.
  - CSA Dept., Indian Institute of Science, Bangalore, India, June 19, 2006.
  - Microsoft Research India, Bangalore, India, June 15, 2006.
  - First Midwest Security Workshop, Chicago, Illinois, May 6, 2006.
- "Creating and Operating Security-Aware Code," Ph.D. Thesis Proposal, Computer Sciences Department, University of Wisconsin, Madison, Wisconsin, January 20, 2006.
- "Enabling Application-Level Authorization Policy Enforcement," IBM T.J. Watson Research Center, Hawthorne, New York, August 25, 2005.
- "Automatic Placement of Authorization Hooks in the Linux Security Modules Framework," IBM T.J. Watson Research Center, Hawthorne, New York, August 3, 2005.

Presentations to Funding Agencies

- "Automatic Discovery of API-Level Exploits," ONR MURI Workshop, Arlington, Virginia, February 14, 2005.
- "Buffer Overrun Detection Using Linear Programming and Static Analysis,"
  - ONR MURI Workshop, Pittsburgh, Pennsylvania, July 23, 2003.
  - ONR MURI Workshop, Williamsburg, Virginia, January 28, 2003.
  - ONR MURI Workshop, Harpers Ferry, West Virginia, July 12, 2002.
  - ONR MURI Workshop, Washington, DC, January 15, 2002.
  - ONR Site Visit, Madison, Wisconsin, November 10, 2001.

9 Teaching and Advising Experience

Teaching at Rutgers University

Term	Topic	Size	Rating
Fall'08	*Introduction to Computer Security* (01:198:442:01).	19	TBD
Fall'08	*Light Seminar: Browser and Web Security* (01:198:500).	16	TBD
Spring'08	*Introduction to Computer Security* (01:198:442:01).	16	4.78
Fall'07	*Introduction to Software Security* (16:198:673:01).	20	4.78
Fall'07	*Light Seminar: Systems, Networking, and Security Isues in Mobile Personal Computing* (16:198:500:01), with Liviu Iftode.	16	4.80

Notes: (1) The rating field shows the average score, out of a maximum of 5, based upon student evaluations to the question "I rate the teaching effectiveness of the instructor as". (2) 01:198:442 is a senior-level undergraduate course on the basic principles of computer security. (3) 16:198:673 is an advanced graduate course on computer security with a focus on state-of-the-art techniques in software security. (4) 16:198:500 is a light seminar on topics in computer security.

Ph.D. Candidate Supervision

- Shakeel Butt (CS, Rutgers University); Spring 2008 onwards.
- Chih-Cheng Chang (CS, Rutgers University); Spring 2008 onwards.
- Mohan Dhawan (CS, Rutgers University), co-advised by Professor Liviu Iftode; Fall 2007 onwards.
- Saman Zarandioon (CS, Rutgers University), co-advised by Professor Danfeng Yao; Summer 2008 onwards.

Masters Candidate Supervision

- Linda Yaeger, (CS, Rutgers University); Spring 2008.

Ph.D. Qualifying Exam/Thesis Defense Committees

- Arati Baliga (CS, Rutgers University), Thesis Defense in December 2008; Advisor: Professor Liviu Iftode.
- Gang Xu (CS, Rutgers University), Thesis Defense in August 2008; Advisor: Professor Liviu Iftode.
- Xiaoxu Wang (CS, Rutgers University), Qualifying Exam in July 2008; Advisor: Professor Dimitris Metaxas.
- Bruno Dufour (CS, Rutgers University), Qualifying Exam June 2008; Advisor: Professor Barbara Ryder.
- Weiqing Sun (CS, State University of New York-Stony Brook), Thesis Defense in May 2008; Advisor: Professor R. Sekar.
- Yuchi Huang (CS, Rutgers University), Qualifying Exam in May 2008; Advisor: Professor Dimitris Metaxas.
- Stephen Smaldone (CS, Rutgers University), Qualifying Exam in September 2007; Advisor: Professor Liviu Iftode.

Other Pedagogical Activities

- Participant, New Jersey Governor's School for Engineering and Technology (July 2008). Supervised four high-school students from New Jersey in their research on malware analysis.

10 Professional Activities

Program Committee Member

- SESS 2009: 5^{th} International Workshop on Software Engineering for Secure Systems, Vancouver, Canada, May 19, 2009.
- 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.
- CSAW 2008: 2^{nd} Computer Security Architecture Workshop, Fairfax, Virginia, October 31, 2008.
- CCS 2008: 15^{th} ACM Conference on Computer and Communications Security, Alexandria, Virginia, October 27-31, 2008.
- SUTC 2008: 2^{nd} IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (Reliable Software Systems track), Taichung, Taiwan, June 11-13, 2008.
- SESS 2008: 4^{th} International Workshop on Software Engineering for Secure Systems, Leipzig, Germany, May 17-18, 2008.
- NDSS 2008: 15^{th} Annual Networked and Distributed Systems Security Symposium, San Diego, California, February 11-13, 2008.

Reviewing

- *Journals:* Journal of Computer Security (JCS), ACM Transactions on Internet Technology (TOIT), ACM Transactions on Information and System Secutity (TISSEC), IEEE Transactions on Software Engineering (TSE).
- *Conferences:* IEEE Symposium on Security and Privacy (2007), IEEE Computer Security Foundations Symposium (2008), ACM Conference on Computer and Communications Security (2005, 2006, 2007), USENIX Security Symposium (2005, 2006), ISOC Symposium on Networked and Distributed Systems Security (2005, 2007), USENIX Annual Technical Conference (2004, 2008), International Symposium on High-Performance Computer Architecture (2008), International World Wide Web Conference (2004, 2005), International Conference on Computer-Aided Verification (2005, 2006), International Conference on Tools and Algorithms for the Construction and Analysis of Systems (2007), ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming (2008), ACM SIGSOFT International Symposium on Foundations of Software Engineering (2008), ACM SIGSOFT International Symposium on Software Testing and Analysis (2004), Formal Methods and Models for Codesign (2004).
- *Workshops:* Workshop on Software Engineering for Secure Systems (2005).
- *Other:* ARO Proposal Reviewer (2008).

University and Departmental Service

- Graduate student admissions committee, Department of Computer Science, Rutgers University (Spring 2008).
- Incoming graduate student transition committee (constituted by students' chapter of the ACM); University of Wisconsin, Madison (2002).

Collaboration with Industry

- Technology transfer to Grammatech Inc., Ithaca, New York. Lead the design, implementation and evaluation of a buffer overrun detection tool using CodeSurfer^{tm} (September 2001–August 2003).

Professional Societies

- Member of the ACM.
- Member of DIMACS, the Center for Discrete Mathematics and Theoretical Computer Science.

11 Personal Information

- **Nationality:** Indian.
- **Visa status:** H-1B work permit.
- **Other:** Date and place of birth—September 1979, Bangalore, India.

Piscataway, NJ, November 29, 2008