

**David A. Naumann**

**September 13, 2011**

Professor of Computer Science, Stevens Institute of Technology, Hoboken NJ 07030.

URL: <http://www.cs.stevens.edu/~naumann/>

### **Education**

University of Texas at Austin, Computer Science, BA 1982 and PhD 1992

### **Appointments**

Visiting Professor, IMDEA Software Institute, Madrid, Mar-May 2011 (on sabbatical leave)

Visiting Researcher, Microsoft Research Cambridge, Sept-Dec. 2010 (on sabbatical leave)

Professor of Computer Science, Stevens Institute of Technology, since 2008

Associate Professor of Computer Science, Stevens Institute of Technology, 2002–08

Assistant Professor of Computer Science, Stevens Institute of Technology, 1997–2002

Assistant Professor of Mathematics and Computer Science, Southwestern University, 1991–97

Associate Scientist, International Software Systems, Austin, 1986–91

Consultant-programmer, Renaissance Systems, Austin, 1985–86

Programmer-designer, IBM, Austin, 1982–85

### **Journal Papers**

1. A recursion theorem for predicate transformers on inductive data types. *Information Processing Letters* 50 (1994) 329–336.
2. Data refinement, call by value, and higher order programs. *Formal Aspects of Computing* 7 (1995) 652–662.
3. Predicate transformers and higher order programs. *Theoretical Computer Science* 150 (1995) 111–159.
4. A categorical model of higher order imperative programming. *Mathematical Structures in Computer Science* 8 (1998) 351–399.
5. A weakest precondition semantics for refinement of object-oriented programs (with Ana Cavalcanti). *IEEE Transactions on Software Engineering* 26 (2000) 713–728.
6. Calculating sharp adaptation rules. *Information Processing Letters* 77 (2001) 201–208.
7. Predicate transformer semantics of a higher order imperative language with record subtyping. *Science of Computer Programming* 41 (2001) 1–51.

8. Soundness of data refinement for a higher order imperative language. *Theoretical Computer Science* 278 (2002) 271–301.
9. Stack-based access control for secure information flow (with Anindya Banerjee). *Journal of Functional Programming* 15 (2005) 131–177.
10. Ownership confinement ensures representation independence for object-oriented programs (with Anindya Banerjee). *Journal of the ACM* 52 (2005) 894–960.
11. Towards imperative modules: Reasoning about invariants and sharing of mutable state (with Michael Barnett). *Theoretical Computer Science* 365 (2006) 143–168.
12. Observational purity and encapsulation. *Theoretical Computer Science* 376 (2007) 205–224.
13. On assertion-based encapsulation for object invariants and simulations. *Formal Aspects of Computing* 19 (2007) 205–224. (Coincidentally, same pages as previous item.)

### Proceedings of Refereed Conferences

§ indicates co-authors who were students at the time of submission.

LNCS = Lecture Notes in Computer Science, series published by Springer.

1. Derivation of programs for freshmen (with R. Denman, W. Potter, and G. Richter). *ACM Conference of the Special Interest Group in Computer Science Education SIGCSE* (1994) 116–120.
2. Predicate transformer semantics of an Oberon-like language. *IFIP TC2 Working Conference on Programming Concepts, Methods and Calculi* (1994) 467–487.
3. On the essence of Oberon. *International Conference on Programming Languages and System Architecture*, Zürich, Jürg Gutknecht, ed. (1994) 313–327.
4. Beyond Fun: order and membership in polytypic imperative programming. *5th International Conference on Mathematics of Program Construction*, (1998) 286–314.
5. Towards squiggly refinement algebra. *Proceedings, IFIP Programming Concepts and Methods* (1998) 346–365.
6. A weakest precondition semantics for refinement in an object-oriented language (with Ana Cavalcanti). *World Congress on Formal Methods* (1999) 1439–1459.
7. Ideal models for pointwise relational and state-free imperative programming. *ACM Principles and Practice of Declarative Programming* (2001) 4–15.
8. Representation independence, confinement, and access control (with Anindya Banerjee). *29th ACM Symposium on Principles of Programming Languages* (2002) 166–177.

9. Forward simulation for data refinement of classes (with Ana Cavalcanti). *International Symposium of Formal Methods Europe* (2002) 471–490.
10. On a specification-oriented model for object-orientation (with Ana Cavalcanti). *6th Brazilian Symposium on Programming Languages* (2002) 114–127.
11. Secure information flow and pointer confinement in a Java-like language (with Anindya Banerjee). *15th IEEE Computer Security Foundations Workshop*<sup>1</sup> (2002) 253–270.
12. Using access control for secure information flow in a Java-like language (with Anindya Banerjee). *16th IEEE Computer Security Foundations Workshop* (2003) 155–169.
13. CodeBLUE: a Bluetooth interactive dance club system (with Dennis Hromin<sup>§</sup>, Michael Chladil<sup>§</sup>, Natalie Vanatta<sup>§</sup>, Susanne Wetzel, Farooq Anjum, and Ravi Jain). *IEEE Global Telecommunications Conference* (2003) 2814–2818.
14. Towards imperative modules: Reasoning about invariants and sharing of mutable state, extended abstract (with Mike Barnett). *19th IEEE Symposium on Logic in Computer Science* (2004) 313–323.
15. Friends need a bit more: Maintaining invariants over shared state (with Mike Barnett) *7th International Conference on Mathematics of Program Construction* (2004) 54–84.
16. Modular and constraint-based information flow inference for an object-oriented language (with Qi Sun<sup>§</sup> and Anindya Banerjee). *11th International Static Analysis Symposium*, LNCS 3148 (2004) 84–99.
17. Assertion-based encapsulation, object invariants and simulations (invited survey paper), in post-proceedings, *Formal Methods for Components and Objects*, LNCS 3657 (2004) 251–273.
18. Observational purity and encapsulation. *Fundamental Aspects of Software Engineering* (2005) 190–204. Awarded Best Software Sciences Paper of ETAPS 2005.
19. State based ownership, reentrance, and encapsulation (with Anindya Banerjee). *19th European Conference on Object-Oriented Programming* (2005) 387–411.
20. Verifying a secure information flow analyzer. *18th International Conference on Theorem Proving in Higher Order Logics* (2005) 211–226.
21. Deriving an information flow checker and certifying compiler for Java (with Gilles Barthe and Tamara Rezk<sup>§</sup>). *27th IEEE Symposium on Security and Privacy* (2006) 230–242.
22. From coupling relations to mated invariants for checking secure information flow. *11th European Symposium on Research in Computer Security* (2006) 279–296.

---

<sup>1</sup>Nominally this was a refereed workshop, not a conference, but at the quality standard of a symposium—indeed, in 2007 it was renamed to the *20th Computer Security Foundations Symposium*.

23. Closing internal timing channels by transformation (with Alejandro Russo<sup>§</sup>, John Hughes, and Andrei Sabelfeld). In *11th Asian Computing Science Conference* (2006).
24. Allowing state changes in specifications (with Michael Barnett, Wolfram Schulte, and Qi Sun<sup>§</sup>). In *International Conference on Emerging Trends in Information and Communication Security LNCS 3995* (2006) 321–336, invited paper.
25. Category theoretic models of data refinement (with Michael Johnson and John Power). In *Irish Conference on Mathematical Foundations of Computer Science and Information Technology* (2006), invited paper. In *Springer Electronic Notes in Theoretical Computer Science 225(2)* (2009) 21–38.
26. Beyond stack inspection: a unified access-control and information-flow security model (with Marco Pistoia and Anindya Banerjee). In *28th IEEE Symposium on Security and Privacy* (2007) 149–163.
27. Modular verification of higher-order methods with mandatory calls specified by model programs (with Steve M. Shaner<sup>§</sup> and Gary T. Leavens). In *22d International Conference on Object Oriented Programming, Languages, and Systems* (2007) 351–368. Awarded Best Student Paper.
28. Expressive declassification policies and modular static enforcement (with Anindya Banerjee and Stan Rosenberg<sup>§</sup>). In *29th IEEE Symposium on Security and Privacy* (2008) 339–353.
29. Regional logic for local reasoning about global invariants (with Anindya Banerjee and Stan Rosenberg<sup>§</sup>). In *European Conference on Object Oriented Programming* (2008) 387–411. Awarded Distinguished Paper.
30. Boogie meets regions: a verification experience report (with Anindya Banerjee and Mike Barnett). In *Verified Software: Theories, Tools, Experiments LNCS 5295* (2008) 177–191.
31. Dynamic boundaries: Information hiding by second order framing with first order assertions (with Anindya Banerjee). In the *19th European Symposium on Programming (ESOP) LNCS 6012* (2010) 2–22.
32. Information flow monitor inlining (with Andrey Chudnov<sup>§</sup>). In *IEEE Computer Security Foundations Symposium* (2010) 200–214.
33. Local reasoning and dynamic framing for the composite pattern and its clients (with Stan Rosenberg<sup>§</sup> and Anindya Banerjee). In proceedings of 3d International Conference on *Verified Software: Theories, Tools, Experiments (VSTTE) LNCS 6217* (2010) 183–198.

34. Guiding a general-purpose C verifier to prove cryptographic protocols (with François Dupressoir<sup>§</sup>, Andrew D. Gordon, and Jan Jürjens). In *IEEE Computer Security Foundations Symposium* (2011) 3–17.
35. Symbolic analysis for security of roaming protocols in mobile networks (with Chunyu Tang<sup>§</sup> and Susanne Wetzel). To appear in *ICST Conference on Security and Privacy in Communication Networks (SecureComm)* 2011.

### Edited collections

Proceedings of the ACM SIGPLAN Fourth Workshop on Programming Languages and Analysis for Security, 2009, Dublin, Ireland. Co-editor with Stephen Chong (Harvard). Published by ACM Press, 131 pages, ISBN 978-1-60558-645-8

VSTTE 2010 Workshop Proceedings (119 pages). Co-editor with Rajeev Joshi (NASA), Tiziana Margaria (Potsdam), Peter Mller (ETH), and Hongseok Yang (U. London). Technical Reports 676, ETH Zurich, Computer Science.

### Selected awards

Best Software Science Paper, ETAPS 2005 (European Association of Software Sciences and Technology).

Davis Memorial Award for Research Excellence, Stevens Institute of Technology, 2006.

Best Student Paper, OOPSLA 2008 (well, the student is Steven M. Shaner and the third coauthor is his advisor, Gary T. Leavens).

Distinguished Paper Award, ECOOP 2008 (with coauthors Anindya Banerjee and Stan Rosenberg).

### Selected recent activities

Co-organizer and co-editor of proceedings, first Dagstuhl seminar on Language Based Security (Seminar 03411, October 5–10, 2003, <http://www.dagstuhl.de/03411/>) with Anindya Banerjee, Heiko Mantel, and Andrei Sabelfeld.

Co-editor of *Concurrency and Computation: Practice and Experience*, June 2004, special issue on formal methods for Java programs.

Co-author, *Verified Software Initiative: grand challenge roadmap* 2007.

Corresponding member, Verified Software Repository Network (<http://vsr.sourceforge.net/>)

Visiting Researcher, Microsoft Research Cambridge (Fall 2010).

Visiting Researcher, the IMDEA Software Institute, Madrid (Spring 2011).

*Chair of Theory Working Group*, Verified Software Initiative,<sup>2</sup> 2005–2007.

---

<sup>2</sup><http://vstte.ethz.ch/index.html> and <http://qpq.csl.sri.com/vsr/>, <http://www.dagstuhl.de/06281/>

*Co-chair of Theory Workshop* in connection with International Conference on *Verified Software: Theory, Tools, Experiments* 2010 (with Hongseok Yang), and 2008 (with Peter O’Hearn).

*Co-chair of 4th ACM Workshop on Programming Languages and Analysis for Security* in connection with International Conference on *Programming Language Design and Implementation* 2009 (with Stephen Chong).

*Co-organizer of the IBM Programming Languages Day* 2009 (with Rajesh Bordawekar, IBM, and Riccardo Pucella, Northeastern U.)

*Co-organizer of the New Jersey Programming Languages Seminar* April 2010 (with Adriana Compagnoni and Dominic Duggan).

*Co-chair of the 15th Brazilian Symposium on Formal Methods* (SBMF) 2012; also member of steering committee.

*Program committee member, refereed conferences:*

ACM Principles of Programming Languages (POPL) 2011;  
ACM Computer and Communication Security (CCS) 2010;  
European Symposium on Programming (ESOP) 2004, 2008;  
IFIP Formal Methods for Open Object-based Distributed Systems (FMOODS) 2007, 2008;  
International Conference on Formal Engineering Methods (ICFEM) 2005, 2009;  
Verified Software: Theories, Tools, Experiments (VSTTE) 2008, 2010;  
TOOLS Europe 2008;  
European Symposium on Research in Computer Security (ESORICS) 2007;  
14th International Symposium on Formal Methods (FM) 2006;  
International Conference on Mathematics of Program Construction 2000, 2002, 2004, 2010, 2012;  
Brazilian Symposium on Formal Methods 2004, 2007, 2008, 2009, 2010, 2011;  
Brazilian Symposium on Programming Languages 2004, 2005, 2006, 2007, 2008;  
Brazilian Symposium on Software Engineering 2002, 2003, 2005;  
International Symposium on Unifying Theories of Programming (UTP) 2006, 2008, 2010.

*Program committee member, refereed workshops:*

IEEE/ACM Workshop on Automated Formal Methods (AFM) 2007, 2008, 2009;  
ECOOP International Workshop on Aliasing, Confinement and Ownership in object-oriented programming (IWACO) 2003, 2008;  
ACM Workshop on Program Analysis and Security (PLAS) 2008, 2009 (co-chair);  
NIST Static Analysis Summit (SAS II) 2008;  
Workshop on Specification and Verification of Component-Based Systems, 2007;  
ACM/CCS Workshop on Formal Methods in Security Engineering (FMSE) 2007, 2008;  
LICS/ICALP Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA) 2007;  
ESEC/FSE Workshop on Specification and Verification of Component-Based Systems (SAVCBS)

2007;

ECOOP Workshop on Program Analysis for Security and Safety (PASSWORD) 2006;

ECOOP Workshop on Formal Techniques for Java-like Languages 2003, 2004, 2005;

UN International Institute for Software Technology Workshop on Formal Aspects of Component Software 2005.

## PhD students

*My PhD Students:*

- Qi Sun (defended October 2007, now at Google): *Constraint-based Secure Information Flow Inference for Object-oriented Programs*.
- Stan Rosenberg (defended June 2011, now at Proclivity Systems): *Region Logic: Local Reasoning for Java Programs and its Automation*.
- Chunyu Tang (expected 2011): *Tools for Security Modeling and Analysis*.
- Andrey Chudnov (expected 2011): *Information Flow Security of JavaScript*.

Opponent and PhD examiner for Leonid Mikhajlov, *Software reuse mechanisms and techniques: safety versus flexibility*, Turku University, Finland, supervisor Ralph Back, 1999.

PhD examiner for Hongseok Yang, *Local reasoning for stateful programs*, University Illinois, supervisor Uday Reddy, 2001 (student was supported by my award INT-9813854).

PhD examiner for Noah Torp-Smith, *Advances in Separation Logic*, IT University of Copenhagen, supervisor Lars Birkedal, 2005.

PhD examiner for Yannis Kassios, *A theory of object-oriented refinement*, University of Toronto, supervisor Eric Hehner, 2006.

PhD examiner for Mariela Pavlova, *Framework for formal verification of Java bytecode against functional and security policies*, University of Nice, supervisor Gilles Barthe, 2007.

Opponent and PhD examiner for Daniel Hedin, *Program analysis issues in language based security*, Chalmers University of Technology, Gothenberg, supervisor David Sands, 2008.

Supervised research internship (Oct 2010–Feb 2011) of Mehdi Bouaziz, *Symbolic execution for JavaScript*, École Normale Supérieure (ENS), Paris, supervisor Patrick Cousot.

PhD committee member: *At Stevens*: Mark Wolfskehl (1999), Tendü Yogurtcu (2000), Ricardo Medel (2007), Uma Batchu (2007), Ye Wu (2010), Jared Cordasco (in progress), Hesham Mansour (in progress). *Elsewhere*: Rohit Gheyi, Federal University of Pernambuco, Brazil (2007).

## Undergraduate honors theses supervised

Lam Nguyen, Elizabeth Taylor, and Dustin Long.

## Associates

**Thesis Supervisors:** Edsger W. Dijkstra (University of Texas at Austin; deceased) and C. A. R. Hoare (Oxford University, now Microsoft, Cambridge, UK)

**Recent Collaborators:** Anindya Banerjee (Kansas State University), Mike Barnett and Wolfram Schulte (Microsoft Research, Redmond), Gilles Barthe and Tamara Rezk (INRIA, Sophia-Antipolis), Paulo Borba and Augusto Sampaio (Federal University of Pernambuco, Brazil), Ana Cavalcanti (University of Kent), Andrew Gordon and François Dupressoir (Microsoft Research, Cambridge), John Hughes, Andrei Sabelfeld, and Alejandro Russo (Chalmers University of Technology), Gary T. Leavens and Steve Shaner (Iowa State University), Marco Pistoia (IBM Research), Leila Silva (Federal University of Sergipe, Brazil), Werner Backes, Antonio Nicolosi, Wendy Hui Wang, and Susanne Wetzels (Stevens)