David A. Naumann **March 18, 2018**

Professor of Computer Science, Stevens Institute of Technology, Hoboken NJ 07030.
http://www.cs.stevens.edu/~naumann/ naumann@cs.stevens.edu

Education

University of Texas at Austin, Computer Science, BA 1982 and PhD 1992
Dissertation advisors: Professors Edsger W. Dijkstra and C.A.R. Hoare

Appointments

Visiting Fellow, Department of Computer Science, Princeton University (DeepSpec project), Sept. 2017–May 2018 (on sabbatical leave)

Visiting Professor, Madrid Institute for Advanced Studies in Software Development Technologies (IMDEA), 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

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

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.)

14. Refactoring and representation independence for class hierarchies (with Augusto Sampaio and Leila Silva). *Theoretical Computer Science* 433 (2012) 60–97.

15. Local reasoning for global invariants, Part I: Region logic (with Anindya Banerjee and Stan Rosenberg[§]). *Journal of the ACM* 60 (2013) 18:1–18:56.

16. Local reasoning for global invariants, Part II: Dynamic boundaries (with Anindya Banerjee). *Journal of the ACM* 60 (2013) 19:1–19:73.

17. Guiding a general-purpose C verifier to prove cryptographic protocols (with François Dupressoir[§], Andrew D. Gordon, and Jan Jürjens). *Journal of Computer Security* 22 (2014) 823–866.

18. Behavioral subtyping, specification inheritance, and modular reasoning (with Gary Leavens). *ACM Transactions on Programming Languages and Systems* 37 (2015) 13:1–13:88.

19. Towards Patterns for Heaps and Imperative Lambdas. *Journal of Logical and Algebraic Methods in Programming* 85 (2016) 1038–1056.

20. A Logical Analysis of Framing for Specifications with Pure Method Calls (with Anindya Banerjee and Mohammad Nikouei[§]). *ACM Transactions on Programming Languages and Systems* (2018) accepted for publication, 92pp.

Proceedings of Refereed Conferences

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*[1] (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[§], Michael Chladil[§], Natalie Vanatta[§], Susanne Wetzel, Farooq Anjum, and Ravi Jain). *IEEE Global Telecommunications Conference* (2003) 2814–2818.

[1]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*.

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[§] 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. *I8th 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[§]). *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.

23. Closing internal timing channels by transformation (with Alejandro Russo[§], 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[§]). 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 Mathmatical 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[§] 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[§]). 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[§]). 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 *Programming Languages and Systems, 19th European Symposium on Programming (ESOP)* LNCS 6012 (2010) 2–22.

32. Information flow monitor inlining (with Andrey Chudnov[§]). 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[§]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[§], 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[§] and Susanne Wetzel). In *ICST Conference on Security and Privacy in Communication Networks* (2011) 480–490.

36. Decision procedures for region logic (with Stan Rosenberg[§] and Anindya Banerjee). In *13th International Conference on Verification, Model Checking, and Abstract Interpretation* LNCS 7148 (2012) 379–395.

37. Laws of programming for references (with Giovanny Lucero[§] and Augusto Sampaio). In *11th Asian Symposium on Programming Languages and Systems* LNCS 8301 (2013) 124–139.

38. Analysis of authentication and key establishment in inter-generational mobile telephony (with Chunyu Tang[§] and Susanne Wetzel). In *IEEE International Conference on High Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing* (2013) 1605–1614 (see www.iacr.org/2013/227).

39. A logical analysis of framing for specifications with pure method calls (with Anindya Banerjee). In post-proceedings of *Verified Software: Theories, Tools, Experiments* LNCS 8471 (2014) 3–20.

40. Information flow monitoring as abstract interpretation for relational logic (with Andrey Chudnov[§] and George Kuan). In *IEEE Computer Security Foundations Symposium* (2014) 48–62.

41. Inlined information flow monitoring for JavaScript (with Andrey Chudnov[§]). In *ACM Conference on Computer and Communication Security* (2015) 629–643.

42. Calculational design of information flow monitors (with Mounir Assaf). In *IEEE Computer Security Foundations Symposium* (2016) 210–224.

43. Specifying and verifying advanced control features (with Gary T. Leavens, Hridesh Rajan, Tomoyuki Aotani). In *7th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation* (2016).

44. Relational logic with framing and hypotheses (with Anindya Banerjee and Mohammad Nikouei[§]). In *36th Conference on Foundations of Software Technology and Theoretical Computer Science* (2016) 11:1–11:16.

45. Hypercollecting semantics and its application to static analysis of information flow (with Mounir Assaf, Julien Signoles, Éric Totel, Frédéric Tronel). In *44th ACM Symposium on Principles of Programming Languages* (2017) 874–887.

Book chapters

1. State Based Encapsulation for Modular Reasoning about Behavior-Preserving Refactorings (with Anindya Banerjee). Invited chapter in *Aliasing in Object-oriented Programming*, Dave Clarke and James Noble and Tobias Wrigstad, eds., Springer State-of-the-art Surveys, 2013, LNCS 7850, pages 319–365.

2. A Simple Semantics and Static Analysis for Stack Inspection (with Anindya Banerjee). In *Semantics, Abstract Interpretation, and Reasoning about Programs: Essays Dedicated to David A. Schmidt on the Occasion of his Sixtieth Birthday*, EPTCS 129 (2013) 284–308 (DOI: 10.4204/EPTCS.129, ISSN: 2075-2180).

Edited collections

1. Proceedings of Seminar 03411 on Language Based Security, 2005, Dagstuhl, Germany. Co-editor with Anindya Banerjee, Heiko Mantel, and Andrei Sabelfeld (http://www.dagstuhl.de/03411/).

2. 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.

3. 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.

4. Formal Methods: Foundations and Applications – Proceedings of 15th Brazilian Symposium, 2012. Co-editor with Rohit Gheyi. LNCS 7498.

5. Fifth International Symposium on Unifying Theories of Programming (UTP 2014), Revised Selected Papers. Editor. LNCS 8963.

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

Chair of the 5th International Symposium on Unifying Theories of Programming 2014, co-located with FM2014 in Singapore.

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

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

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); also member of the steering committee.

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

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).

Chair of Theory Working Group, Verified Software Initiative,[2] 2005–2007.

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

Co-organizer and co-editor of proceedings, first Dagstuhl seminar on Language Based Security (Seminar 03411, Oct. 5–10, 2003), with Anindya Banerjee, Heiko Mantel, and Andrei Sabelfeld.

Editorial board member:
Formal Aspects of Computing
Journal of Object Technology

Program committee member, refereed conferences:

ACM Principles of Programming Languages (POPL) 2019;
5th International Conference on Runtime Verification (RV) 2014, 2016;
28th IEEE Computer Security Foundations Symposium (CSF) 2015;
20th International Symposium on Formal Methods (FM) 2015;
4th Conference Principles of Security and Trust (POST) 2015;
Verified Software: Theories, Tools, Experiments (VSTTE) 2016, 2013, 2010, 2008;
International Conference on Mathematics of Program Construction (MPC) 2015, 2012, 2010, 2004, 2002, 2000;
ACM Principles of Programming Languages (POPL) 2011;
ACM Computer and Communication Security (CCS) 2010;
European Symposium on Programming (ESOP) 2008, 2004;
Brazilian Symposium on Formal Methods (SBMF) 2018, 2017, 2016, 2015, 2014, 2013, 2012 (co-chair), 2011, 2010, 2009, 2008, 2007, 2004;
IFIP Formal Methods for Open Object-based Distributed Systems (FMOODS) 2008, 2007;
International Conference on Formal Engineering Methods (ICFEM) 2009, 2005;
TOOLS Europe 2008;
European Symposium on Research in Computer Security (ESORICS) 2007;
14th International Symposium on Formal Methods (FM) 2006;
7th IFIP International Conference on Theoretical Computer Science 2012;
Brazilian Symposium on Programming Languages 2008, 2007, 2006, 2005, 2004;
Brazilian Symposium on Software Engineering 2005, 2003, 2002;
International Symposium on Unifying Theories of Programming (UTP) 2014, 2012, 2010, 2008, 2006.

[2] http://vstte.ethz.ch/index.html and http://www.dagstuhl.de/06281/

Advisees and mentees

Postdoc: Mounir Assaf (2015–2017)

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): *Region Logic: Local Reasoning for Java Programs and its Automation.*

Chunyu Tang (defended December 2013): *Modeling and Analysis of Mobile Telephony Protocols.*

Andrey Chudnov (defended April 2015, now at Galois Inc.): *Inlined Information Flow Monitoring for Web Applications in JavaScript.*

Mohammad Nikouei (expected 2018): *A Logical Analysis of Relational Program Correctness*

Masters theses advised:

Dylan Hutchison (2015, now PhD student at U. Washington): *ModelWizard: Toward Interactive Model Construction*

Julian Sexton (2016, now at MITRE): *Information Flow Control for Android Applications with Embedded WebPages*

Undergraduate theses advised: Lam Nguyen, Elizabeth Taylor, and Dustin Long.

Other PhDs:

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.

Opponent and PhD examiner for Musard Balliu, *Logics for information flow security: from specification to verification*, KTH Royal Institute of Technology, Stockholm, supervisor Mads Dam, 2014.

PhD examiner for José Fragoso Santos, *Enforcing secure information flow in client-side web applications*, University of Nice (INRIA), Sophia Antipolis, supervisors Tamara Rezk and Ana Almeida Matos, 2014.

PhD co-advisor for Giovanny Lucero, *Algebraic laws for object oriented programming with references*, Federal University of Pernambuco, Brazil, supervisor Augusto Sampaio, 2015.

PhD committee member for Yuyan Bao, *Reasoning about frame properties in object-oriented programs*, University of Central Florida, supervisor Gary Leavens, 2017.

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

Supervised research internship (Mar 2013–July 2013) Guillaume Bury, *Automating relational verification in Why3*, École Normale Supérieure (ENS), Paris, supervisor Xavier Rival.

PhD committee member: *At Stevens*: Mark Wolfskehl (1999), Tendü Yogurtcu (2000), Ricardo Medel (2007), Uma Batchu (2007), Ye Wu (2010), Yifei Bao (2013), Yidi Zhang (2014), Ruilin Yang (2015), Walter Krawec (2015), Hesham Mansour (2015), Boxiang Dong (2016), Michael Engling (2017). *Elsewhere*: Rohit Gheyi, Federal University of Pernambuco, Brazil (2007).

Consulting

Microsoft; Vulcan Inc.; Galois Inc.