

ZHENDONG SU

(Updated: July 2010)

Department of Computer Science
3011 Kemper Hall
University of California
Davis, CA 95616-8562

Phone: 530-754-5376
Fax: 530-752-4767
e-mail: su@cs.ucdavis.edu
web: <http://www.cs.ucdavis.edu/~su>

RESEARCH INTERESTS

Software engineering, programming languages, and computer security, focusing on techniques and tools for improving software quality and programmer productivity.

PROFESSIONAL PREPARATION

- Ph.D., Computer Science (with minor in Mathematics), University of California, Berkeley, 2002
- M.S., Computer Science, University of California, Berkeley, 1997
- B.A., Mathematics (*with the Highest Honor*), University of Texas at Austin, 1995
- B.S., Computer Science (*with the Highest Honor*), University of Texas at Austin, 1995
- Undergraduate Study, Business School, University of Wisconsin, Eau Claire, 1991–1992
- Undergraduate Study, International Trade, Fudan University, Shanghai, China, 1988–1991

Names of Research Advisors

- **Ph.D.** Alex Aiken, UC Berkeley (now at Stanford), June 1996–December 2002
- **M.S.** Alex Aiken, UC Berkeley (now at Stanford), June 1996–December 1997
- **B.S.** Vladimir Lifschitz, UT Austin, August 1994–August 1995

APPOINTMENTS

- Associate Professor (with tenure), Department of Computer Science, UC Davis, 7/2007–present
- Assistant Professor, Department of Computer Science, UC Davis, 11/2002–06/2007
- Visiting Fellow, Automated Software Engineering Group, RIACS/NASA Ames, 9/2002–12/2002
- Graduate Student Instructor, Computer Science Division, UC Berkeley, 1/2000–5/2000
- Graduate Student Researcher, Computer Science Division, UC Berkeley, 6/1996–8/2002
- Research Intern, Computing Sciences Research Center, Bell Laboratories, 5/1997–8/1997

HONORS AND AWARDS

- Chancellor's Faculty Fellow Nominee, UC Davis, 2010
- ACM SIGSOFT Distinguished Paper Award (at ISSTA'10), Trento, Italy, 2010
- Top ranked paper (at ISSTA'10), Trento, Italy, 2010
- ACM SIGSOFT Distinguished Paper Award Nominee (at ICSE'10), Cape Town, South Africa, 2010
- IBM Software Quality Innovation Award, 2008
- Distinguished Visitor, IBM Thomas J. Watson Research Center, New York, 2008
- Outstanding Junior Faculty Award, College of Engineering, UC Davis, 2007
- ACM SIGSOFT Distinguished Paper Award Nominee (at ICSE'07), Minneapolis, MN, 2007

- Marquis Who's Who in America, 2007–
- Keynote, International Workshop on Software Engineering for Secure Systems, Shanghai, 2006
- NSF CAREER Award (CISE CCF “Software Engineering and Languages” Program), 2006
- UC Davis Nominee for the Microsoft New Faculty Fellowship, November 2004
- ACM SIGSOFT Distinguished Paper Award (at ICSE’04), Edinburgh, UK, 2004 (*five out of 436*)
- Award Paper selected by TACAS’04 program committee, Barcelona, Spain, 2004 (*seven out of 145*)
- The EAPLS Best Paper Award (at ETAPS’98), Lisbon, Portugal, 1998 (*one out of 290*)
- UC Regents Fellowship, UC Berkeley, 1995–1996
- Named the Dean’s Honored Graduate of the Year in Computer Science, UT Austin, 1995
- Presidential Scholarship, UT Austin, 1994–1995
- Member of 2nd Place Team in the ACM South Central Regional Programming Contest, USA, 1994
- Ranked in the Top 150 (US & Canada) in the William Lowell Putnam Math Competition, 1993
- Directly Admitted into Fudan University without College Entrance Examination, China, 1988
- First Prize Winner in the Shanghai High School Mathematics Competition, China, 1987
- Fourth Prize Winner in the Chinese National High School Mechanics Competition, China, 1987

PUBLICATIONS

Please note that in computer science, top competitive conferences are the venues of choice for the leading people in the field to publish their best work. The top conferences select their papers on a highly competitive basis, fully reviewed by three or more referees with an acceptance rate around or below 20%. Please refer to the following article for more information regarding conference and journal publishing in Computer Science:

“Best Practices Memo—Evaluating Computer Scientists and Engineers for Promotion and Tenure,” David Patterson (UC Berkeley), Lawrence Snyder (University of Washington), and Jeffrey Ullman (Stanford University), 1999. URL: http://archive.cra.org/reports/tenure_review.html. The following quote is particularly relevant:

“For experimentalists, conference publication is preferred to journal publication, and the premier conferences are generally more selective than the premier journals.”

1) Refereed Conference and Workshop Publications

Flagship: 27 **Top:** 9 **Selective:** 4 **Workshop:** 4

Flagship: ICSE (9), ISSTA (5), FSE (4), POPL (3), PLDI (2), ASPLOS (1), CCS (1), OOPSLA (1), S&P (1)

Top: ASE (2), ESOP (2), TACAS (2), ESORICS (1), FOSSACS (1), FSTTCS (1)

Selective: ACSAC (2), NOMS (1), SDM (1)

Workshop: ASID (1), ICSE Demo (1), SAVCBS (1), TIC (1)

1. M. Gabel, J. Yang, Y. Yu, M. Goldszmidt, and Z. Su. Scalable and Systematic Detection of Buggy Inconsistencies in Source Code. To appear in the *ACM SIGPLAN Conference on Object-Oriented Programming Systems, Languages and Applications (OOPSLA’10)*, Reno/Tahoe, NV, October 2010. **(27%)**
2. M. Gabel and Z. Su. A Study of the Uniqueness of Source Code. To appear in the *18th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 18)*, Santa Fe, NM, November 7-11, 2010. **(20%)**
3. E. Tang, E. Barr, X. Li, and Z. Su. Perturbing Numerical Calculations for Statistical Analysis of Floating-Point Program (In)Stability. To appear in the *International Symposium on Software Testing and Analysis (ISSTA’10)*, Trento, Italy, July 2010. **(23%)**

4. T. Kwon and Z. Su. Automatic Detection of Unsafe Component Loadings. To appear in the *International Symposium on Software Testing and Analysis (ISSTA'10)*, Trento, Italy, July 2010 (**Top ranked submission; ACM SIGSOFT Distinguished Paper Award**). (23%)
5. Z. Gu, E.T. Barr, D.J. Hamilton, and Z. Su. Has the Bug Really Been Fixed? In *the 32nd International Conference on Software Engineering (ICSE'10)*, Cape Town, South Africa, May 2010. (14%)
6. M. Gabel and Z. Su. Online Inference and Enforcement of Temporal Properties. Mark Gabel and Zhendong Su. In *the 32nd International Conference on Software Engineering (ICSE'10)*, Cape Town, South Africa, May 2010 (**ACM SIGSOFT Distinguished Paper Award Nominee**). (14%)
7. A. Saebjoernsen, L. Jiang, D. Quinlan, and Z. Su. Static Validation of C Preprocessor Macros. In *the 24th IEEE/ACM International Conference on Automated Software Engineering (ASE'09)*, Auckland, New Zealand, November 2009. (17%)
8. F. Sun, L. Xu, and Z. Su. Client-Side Detection of XSS Worms by Monitoring Payload Propagation. In *the European Symposium on Research in Computer Security (ESORICS'09)*, Saint Malo, France, September 2009. (19%)
9. L. Jiang and Z. Su. Automatic Mining of Functionally Equivalent Code Fragments via Random Testing. In *the International Symposium on Software Testing and Analysis (ISSTA'09)*, Chicago, IL, July 2009. (27%)
10. A. Saebjoernsen, J. Willcok, T. Panas, D. Quinlan, and Z. Su. Detecting Code Clones in Binary Executables. In *the International Symposium on Software Testing and Analysis (ISSTA'09)*, Chicago, IL, July 2009. (27%)
11. C. Bird, E. Barr, A. Nash, P. Devanbu, V. Filkov, and Z. Su. Structure and Dynamics of Research Collaboration in Computer Science. In *the SIAM International Conference on Data Mining (SDM'09)*, Sparks, Nevada, April 2009. (30%)
12. L. Jiang and Z. Su. Profile-Guided Program Simplification for Effective Testing and Analysis. In *the 16th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 16)*, Atlanta, GA, November 2008. (20%)
13. M. Gabel and Z. Su. Javert: Fully Automatic Mining of General Temporal Properties from Dynamic Traces. In *the 16th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 16)*, Atlanta, GA, November 2008. (20%)
14. G. Wassermann, D. Yu, A. Chander, D. Dhurjati, H. Inamura, and Z. Su. Dynamic Test Input Generation for Web Applications. In *the International Symposium on Software Testing and Analysis (ISSTA'08)*, Seattle, WA, July 2008. (26%)
15. M. Gabel, L. Jiang, and Z. Su. Scalable Detection of Semantic Clones. In *the 30th International Conference on Software Engineering (ICSE'08)*, Leipzig, Germany, May 2008. (15%)
16. M. Gabel and Z. Su. Symbolic Mining of Temporal Specifications. In *the 30th International Conference on Software Engineering (ICSE'08)*, Leipzig, Germany, May 2008. (15%)
17. G. Wassermann and Z. Su. Static Detection of Cross-Site Scripting Vulnerabilities. In *the 30th International Conference on Software Engineering (ICSE'08)*, Leipzig, Germany, May 2008. (15%)
18. D. A. S. de Oliveria, J. R. Crandall, G. Wassermann, S. Ye, S. F. Wu, Z. Su, and F. T. Chong. Bezoar: Automated Virtual Machine-based Full-System Recovery from Control-Flow Hijacking Attacks. In *the IEEE/IFIP Network Operations and Management Symposium (NOMS'08)*, Salvador, Bahia, Brazil, April 2008. (27%)
19. M. Van Gundy, H. Chen, Z. Su, and G. Vigna. Feature Omission Vulnerabilities: Thwarting Signature Generation for Polymorphic Worms. In *the Annual Computer Security Applications Conference (ACSAC'07)*, Miami Beach, Florida, December 2007. (22%)
20. L. Jiang and Z. Su. Context-Aware Statistical Debugging: From Bug Predictors to Faulty Control Flow Paths. In *the 22nd IEEE/ACM International Conference on Automated Software Engineering (ASE'07)*, Atlanta, Georgia, November 2007. (12%)

21. L. Jiang, Z. Su, and E. Chiu. Context-Based Detection of Clone-Related Bugs. In the *Sixth Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE'07)*, Dubrovnik, Croatia, September 2007. (17%)
22. G. Wassermann and Z. Su. Sound and Precise Analysis of Web Applications for Injection Vulnerabilities. In *ACM SIGPLAN 2007 Conference on Programming Language Design and Implementation (PLDI'07)*, San Diego, CA, June 2007. (25%)
23. L. Jiang, G. Mishherghi, Z. Su, and S. Glondu. DECKARD: Scalable and Accurate Tree-based Detection of Code Clones. In the *29th International Conference on Software Engineering (ICSE'07)*, Minneapolis, MN, May 2007 (ACM SIGSOFT Distinguished Paper Award Nominee). (15%)
24. F. Hsu, H. Chen, T. Ristenpart, J. Li, and Z. Su. Back to the Future: A Framework for Automatic Malware Removal and System Repair. In *Annual Computer Security Applications Conference (ACSAC'06)*, Miami Beach, Florida, December 2006. (30%)
25. G. Wassermann and Z. Su. Validity Checking for Finite Automata over Linear Arithmetic Constraints. In the *26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)*, Kolkata, India, December 2006. (22%)
26. J. Crandall, G. Wassermann, D. de Oliveira, Z. Su, S. F. Wu, and F. Chong. Temporal Search: Detecting Hidden Malware Timebombs with Virtual Machines. In *Twelfth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'06)*, San Jose, California, October 2006. (22%)
27. D. de Oliveira, J. Crandall, G. Wassermann, S. F. Wu, Z. Su, and F. Chong. ExecRecorder: VM-Based Full-System Replay for Attack Analysis and System Recovery (*short paper, 6 pages*). In the *Workshop on Architectural and System Support for Improving Software Dependability (ASID'06)*, San Jose, California, October 2006.
28. L. Yuan, J. Mai, Z. Su, H. Chen, C. Chuah, and P. Mohapatra. FIREMAN: A Toolkit For FIREwall Modeling and ANalysis. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Oakland, California, May 2006. (9%)
29. L. Jiang and Z. Su. Osprey: A Practical Type System for Validating Dimensional Unit Correctness of C Programs. In the *28th International Conference on Software Engineering (ICSE'06)*, Shanghai, China, May 2006. (9%)
30. G. Mishherghi and Z. Su. HDD: Hierarchical Delta Debugging. In the *28th International Conference on Software Engineering (ICSE'06)*, Shanghai, China, May 2006. (9%)
31. Z. Su and G. Wassermann. The Essence of Command Injection Attacks in Web Applications. In *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'06)*, Charleston, South Carolina, January 2006. (19%)
32. J. Crandall, Z. Su, S. F. Wu, F. Chong. On Deriving Unknown Vulnerabilities from Zero-Day Polymorphic and Metamorphic Worm Exploits. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, Alexandria, Virginia, November 2005. (15%)
33. J. Niehren, T. Priesnitz, and Z. Su. Complexity of Subtype Satisfiability over Posets. In *Proceedings of European Symposium On Programming (ESOP'05)*, Edinburgh, Scotland, UK, April 2005. (24%)
34. G. Wassermann and Z. Su. An Analysis Framework for Security in Web Applications. In *Proceedings of the Workshop on Specification and Verification of Component-Based Systems (SAVCBS)*, November 2004. (43%)
35. C. Gould, Z. Su, and P. Devanbu. JDBC Checker: A Static Analysis Tool for SQL/JDBC Applications. Formal Research Demonstrations Track, in *Proceedings of the 26th International Conference on Software Engineering (ICSE'04)*, Edinburgh, Scotland, UK, May 2004. (35%)
36. C. Gould, Z. Su, and P. Devanbu. Static Checking of Dynamically Generated Queries in Database Applications. In *Proceedings of the 26th International Conference on Software Engineering (ICSE'04)*, Scotland, UK, May 23-28, 2004 (ACM SIGSOFT Distinguished Paper Award). (13%)

37. Z. Su and D. Wagner. A Class of Polynomially Solvable Range Constraints for Interval Analysis without Widening and Narrowing. In *Proceedings of the 10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'04)*, Barcelona, Spain, March 29-April 2, 2004. Among **Best Papers** of TACAS'04 (7/145, **4.8%**), invited paper in Theoretical Computer Science). (**25%**)
38. Z. Su, A. Aiken, J. Niehren, T. Priesnitz, and R. Treinen. The First-Order Theory of Subtyping Constraints. In *Proceedings of the 29th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'02)*, pages 203–216, Portland, USA, January 16–18, 2002.
39. Z. Su and A. Aiken. Entailment with Conditional Equality Constraints. In *Proceedings of European Symposium On Programming (ESOP'01)*, pages 170–189, Genova, Italy, April 2–6, 2001.
40. Z. Su, M. Fähndrich, and A. Aiken. Projection Merging: Reducing Redundancies in Inclusion Constraint Graphs. In *Proceedings of the 27th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'00)*, pages 81–95, Boston, USA, January 19–21, 2000.
41. M. Fähndrich, J.S. Foster, Z. Su, and A. Aiken. Partial Online Cycle Elimination in Inclusion Constraint Graphs. In *Proceedings of the 1998 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'98)*, pages 85–96, Montreal, Canada, June 1998.
42. A. Aiken, M. Fähndrich, and Z. Su. Detecting Races in Relay Ladder Logic Programs. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'98)*, pages 184–200, Lisbon, Portugal, March 1998. **EAPLS Best Paper Award at ETAPS'98.**
43. A. Aiken, M. Fähndrich, J.S. Foster, and Z. Su. A Toolkit for Constructing Type- and Constraint-Based Program Analyses. In *Proceedings of the Second International Workshop on Types in Compilation (TIC'98)*, pages 78–96, Kyoto, Japan, March 1998.
44. A. Muscholl, D. Peled, and Z. Su. Deciding Properties for Message Sequence Charts. In *Proceedings of the International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'98)*, pages 226–242, Lisbon, Portugal, March 1998.

2) Journal Publications

1. G. Misherghi, L. Yuan, Z. Su, C. Chuah, and H. Chen. A General, Formal Framework for Evaluating Firewall Optimization Techniques. In the *IEEE Transactions on Network and Service Management (TNSM)*, 2009.
2. J. R. Crandall, J. Brevik, S. Ye, G. Wassermann, D. A.S. de Oliveira, Z. Su, S. F. Wu, and F. T. Chong. Putting Trojans on the Horns of a Dilemma: Redundancy for Information Theft Detection. In the *Special Issue on Security in Computing of the Transactions on Computational Sciences Journal (Springer LNCS)*, 2009.
3. G. Wassermann, C. Gould, Z. Su, and P. Devanbu. Static Checking of Dynamically Generated Queries in Database Applications. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 16(4), 2007 (**invited paper**).
4. Z. Su and D. Wagner. A Class of Polynomially Solvable Range Constraints for Interval Analysis without Widening. In *Theoretical Computer Science (TCS)*, 345(1), 122–138, 2005 (**invited paper**).
5. A. Aiken, M. Fähndrich, and Z. Su. Detecting Races in Relay Ladder Logic Programs. In *Springer International Journal on Software Tools for Technology Transfer (STTT)*, 3(1), pages 93–105, Springer Verlag, 2000 (**invited paper**).

3) Edited Books and Conference Proceedings

1. J. Palsberg and Z. Su (Eds). *Proceedings of SAS'09, International Static Analysis Symposium*, LNCS 5673, 361 pages, Springer 2009. ISBN: 978-3-642-03236-3.

4) Recent Drafts (under submission/to be submitted)

1. L. Xu, F. Sun, and Z. Su. Constructing Precise Control Flow Graphs from Binaries. July 2010. (12 pages)
2. M. Marron, C. Sanchez, and Z. Su. High-Level Heap Abstractions for Debugging Programs. July 2010. (12 pages)
3. E. Barr, D. Hamilton, M. Gabel, and Z. Su. Prodromoi: Scouting the State-Space with Idle Cores. March 2010. (15 pages)
4. T. Kwon and Z. Su. Modeling High-Level Behavior Patterns for Precise Similarity Analysis of Software. March 2010. (10 pages)

5) Dissertations, Theses, Technical Reports, and Unpublished Manuscripts

1. T. Kwon and Z. Su. Automatic Detection of Vulnerable Dynamic Component Loadings. Technical Report UCD//CSE-2010-2, UC Davis, 2010. (*Revision to appear in ISSTA 2010*)
2. L. Xu, F. Sun, and Z. Su. Constructing Precise Control Flow Graphs from Binaries. Technical Report UCD//CSE-2009-27, UC Davis, 2009.
3. L. Xu and Z. Su. Dynamic Detection of Process-Hiding Kernel Rootkits. Technical Report UCD//CSE-2009-24, UC Davis, 2009.
4. L. Jiang. Scalable Detection of Similar Code: Techniques and Applications. Ph.D. Dissertation, University of California, Davis, October 2009.
5. G. Wassermann. Techniques and Tools for Engineering Secure Web Applications. Ph.D. Dissertation, University of California, Davis, September 2008.
6. J. Crandall. Capturing and Analyzing Internet Worms. Ph.D. Dissertation, University of California, Davis, May 2007.
7. G. Misherghi. Hierarchical Delta Debugging. Master's Thesis, University of California, Davis, May 2007.
8. G. Wassermann and Z. Su. Validity Checking for Finite Automata over Linear Arithmetic Constraints. Technical Report UCD//CSE-2006-16, UC Davis, 2006. (*Revision appeared in FSTTCS 2006*)
9. L. Jiang and Z. Su. Automatic Isolation of Cause-Effect Chains with Machine Learning. Technical Report UCD//CSE-2005-32, UC Davis, 2005. (*Revision appeared in ASE 2007*)
10. H. Chen, F. Hsu, J. Li, T. Ristenpart, and Z. Su. Back to the Future: A Framework for Automatic Malware Removal and System Repair. Technical Report UCD//CSE-2005-6, UC Davis, 2005. (*Revision appeared in ACSAC 2006*)
11. Z. Su and G. Wassermann. Type-based Inference of Size Relationships for XML Transformations. Technical Report UCD//CSE-2004-8, UC Davis, April 2004.
12. Z. Su and D. Wagner. Polynomial Time Algorithms for Solving Integer Range Constraints. Computer Science Technical Report UCD//CSE-2003-5, UC Davis, February 2003. (*Revisions appeared in TACAS and TCS*)
13. Z. Su. Algorithms for and the Complexity of Constraint Entailment. Ph.D. Dissertation, University of California, Berkeley, December 2002.
14. Z. Su and A. Aiken. Entailment with Conditional Equality Constraints. Computer Science Division Tech Report UCB//CSD-00-1113 University of California at Berkeley, October 2000. (*Revision appeared in ESOP 2001*)
15. Z. Su. Stutter Equivalence for Infinite State Systems. Unpublished manuscript, May 1998.
16. Z. Su. Automatic Analysis of Relay Ladder Logic Programs. Computer Science Division Tech Report UCB//CSD-97-969 University of California at Berkeley, September 1997. (*Revisions appeared in TACAS and STTT*)
17. Z. Su and M. Zhou. A Comparative Analysis of Branch Prediction Schemes. Unpublished manuscript, December 1995.
18. Z. Su. Automating the Computation of Nested Abnormality Theories. Undergraduate Honor's Thesis, Department of Computer Sciences The University of Texas at Austin, June 1995.

FUNDING (AWARDED)

- **[Current]** NSF, Software and Hardware Foundations (SHF) Medium Grant CCF-0964703, “SHF:Medium:How Do Static Analysis Tools Affect End-user Quality?,” \$700,118, 2010-2013, **co-PI** (with PI: P. Devanbu, UCD; co-PI: E. Barr, UCD; and co-PI: V. Filkov, UCD).
- **[Current]** AFOSR, DURIP, “Helix Project Testbed: Towards the Self-Regenerative Incorruptible Enterprise,” \$240,000 (UCD portion: \$60,000), 2010–2011, **co-PI** (with PI: John Knight, University of Virginia and co-PIs from University of Virginia, UC Davis, UCSB, and University of New Mexico).
- **[Current]** NSF, Trustworthy Computing (TC) Grant CNS-0917392, “ TC: Small: Runtime and Static Analysis for Web Application Security,” \$423,967, 2009–2012, **sole PI**.
- **[Current]** DHS, I3P Research Fellowship, “Understanding the Malware Arms Race,” \$150,000, 2009-2010, **PI** (I3P Postdoctoral Fellow supported: E. Barr, UCD).
- **[Current]** IBM Software Quality Innovation Award, “Precise and Scalable Static Analysis of Web Applications,” \$25,000, 2008, **sole PI**.
- **[Current]** NSF-China, “A Unified Analysis, Testing, and Verification Framework for Evaluating Software Dependability,” RMB 3,000,000 (approx. \$440,000), 2008-2011, **International Co-PI** (joint project with Nanjing University, China).
- **[Past]** Intel, California Public Affairs Higher Education Equipment Grant, “Bringing Multi-core Technologies to the Classrooms,” 15 dual-core workstations with an approximated value of \$50,000, 2007–2008, **PI**.
- **[Current]** NSF, Computing Processes and Artifacts (CPA) Grant CCF-0702622, “Program Analysis for Reliable Numerical Software,” \$400,000, 2007–2010, **sole PI**.
- **[Current]** AFOSR, MURI, “Helix: A Self-Regenerative Architecture for the Incorruptible Enterprise,” \$4,589,449 (UCD portion: \$1,621,605), 2007–2012, **co-PI** (with PI: John Knight, University of Virginia and co-PIs from University of Virginia, UC Davis, UCSB, and University of New Mexico).
- **[Past]** UCD College of Engineering, Outstanding Junior Faculty Award, \$2,500, 2007.
- **[Past]** DOE LLNL subcontract to UC Davis, “Software Security Analysis,” \$280,000 (total award approx. \$1,500,000), 2006-2009, **sole PI** (LLNL PI: Daniel J. Quinlan).
- **[Current]** NSF, CyberTrust Team Grant, “Collaborative Research: CT-T: A Vertical Systems Framework for Effective Defense against Memory-based Attacks,” \$750,000, 2006-2010, **PI** (with co-PI: S. Felix Wu, UCD and co-PI: Frederic Chong, UCSB).
- **[Current]** NSF, CAREER Grant CCF-0546844, “CAREER: Reliability and Security of Database and Web Applications,” \$450,000, 2006–2010, **sole PI**.
- **[Past]** NSF NeTS-NBD Grant CNS-0520320, “Automatic Validation, Optimization, and Adaptation of Distributed Firewalls for Network Performance and Security,” \$400,000, 2005–2009, **co-PI** (with PI: C-N. Chuah and co-PI: H. Chen).
- **[Past]** Intel, “Containing Malicious Software,” \$50,000, gift, 2005 (with H. Chen).
- **[Past]** DARPA, Self Regenerative Systems (BAA03-44), Subcontract from Global Infotek, Inc. (GITI), \$400,000, 2004–2006, **co-PI** (with PI: K. Levitt and co-PI: J. Rowe).
- **[Past]** HP, Education Grant, “Proposal for Bringing the Power of Itanium 2 to the Classroom,” \$127,141, 2004, **co-PI** (with PI: Z. Bai, other co-PIs include M. Farrens, R. Olsson, R. Pandey, K. Wilken, and K. Jones).
- **[Past]** UC Davis, Junior Faculty Research Grant, \$2,500, 2003–2006, **sole PI**.

FUNDING (PENDING)

- NSF, Software Infrastructure for Sustained Innovation, “Collaborative Research: SI2-SSI: Modeling Software for Regional Climate Prediction,” \$720,000 (total award requested: \$4,163,863; with NCAR, Colorado-Boulder, Toronto), 2011-2014, **PI** (co-PI: P. Devanbu), June 2010.
- DOE, X-Stack Software Research, “Scalable Numerical Computing Primitives for Manycore Architectures,” \$1,952,495, 2010-2013, **co-PI** (PI: J. Owens, UCD; co-PI: Z. Bai, UCD; co-PI: F. Gygi, UCD), March 2010.
- DARPA, Cyber Genome Program, “Cybernomics: Discovering Malware Lineage Using Software Genotypes and Phenotypes,” \$3,360,054, 2010-2014, **co-PI** (PI: T. Heberlein, Net Squared, Inc.; co-PI: K. Levitt, UCD; co-PI: E. Barr, UCD; co-PI: J. Rowe, UCD), March 2010.

SELECTED INVITED PRESENTATIONS

1. Keynote, Internetware 2010, the Second Asia-Pacific Symposium on Internetware, Suzhou, China, November 2010.
2. Emerging Faculty Symposium, ICSE 2010, Invited Presenter, Cape Town, South Africa, May 2010.
3. How to Work Through the PhD Process? Doctoral Symposium, ICSE 2010, Cape Town, South Africa, May 2010.
4. Fully Automatic Mining of General Temporal Properties.
 - Department of Computer Science, Shanghai Jiaotong University, China, January 2010.
 - Department of Computer Science, Nanjing University, China, July 2009.
 - School of Computer Science, Georgia Institute of Technology, March 2009.
5. Techniques and Tools for Engineering Secure Web Applications. Computer Science Department, University of Southern California, February 2009.
6. New Software Engineering Faculty and Researchers Symposium at ACM SIGSOFT 2008 / FSE 16, Invited Presenter, Atlanta, Georgia, November 10, 2008.
7. Techniques and Tools for Detecting Clones and Clone-related Defects. School of Computer Science, Georgia Institute of Technology, September 2008.
8. Web Application Security. Distinguished Visitor, IBM Thomas J. Watson Research Center, New York, August 4-6, 2008.
9. Web and Database Application Security. Invited Lecturer, International Summer School on Language-Based Techniques for Integrating with the External World, University of Oregon, Eugene, Oregon, July 18–26, 2007.
10. Static and Dynamic Analysis for Web Application Security. Google Inc., February 20, 2007.
11. Scalable and Accurate Tree-based Detection of Code Clones. Stanford Software Seminar, Computer Science Department, Stanford University, October 16, 2006.
12. Syntactic Prevention of Command Injection Attacks in Web Applications. State of the Art in Software Engineering, Rutgers University, June 16, 2006.
13. Web Application Security: Software Engineering Challenges and Opportunities. Keynote Speaker, International Workshop on Software Engineering for Secure Systems (SESS), In conjunction with ICSE'06, Shanghai, China, May 2006.
14. Research on Software Reliability and Security. Presented at the CASC/ISCR Seminar at LLNL, California, May 2005.

PROFESSIONAL ACTIVITIES

• Editorial Board:

- Associate Editor, ACM Transactions on Software Engineering and Methodology (TOSEM), 2008–present
- Editorial Board, ICST Transactions on Security and Privacy, 2009–present

• Conference/Program (Co-)Chair:

- Program Chair, International Conference on Software Testing and Analysis (ISSTA), 2012
- Program Co-chair, the 16th International Static Analysis Symposium (SAS), Los Angeles, CA, 2009

• Program Committee:

- European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering, Hungary, 2011
- International Static Analysis Symposium (SAS), Italy, 2011
- Mentor, International Conference on Software Engineering Mentoring Program, 2011.

- ACM Workshop on Programming Languages and Analysis for Security (PLAS), Canada, 2010
- International Conference on Software Testing and Analysis (ISSTA), Italy, 2010
- International Static Analysis Symposium (SAS), France, 2010
- ACM SIGSOFT Symposium on Foundations of Software Engineering (FSE), New Mexico, 2010
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), 2010
- International Conference on Software Engineering (ICSE), Cape Town, South Africa, 2010
- International Conference on Software Engineering (ICSE), Doctoral Symposium, Cape Town, South Africa, 2010
- International Conference on Software Testing and Analysis (ISSTA), Chicago, IL, July 2009
- International Conference on Software Engineering (ICSE), Vancouver, Canada, 2009
- The 18th International World Wide Web Conference (WWW), Madrid, Spain, 2009
- International Conference on Compiler Construction (CC), York, UK, 2009
- The 16th Annual Network & Distributed System Security Symposium (NDSS), 2009
- ASIAN Symposium on Programming Language and Systems (APLAS), India, 2008
- 11th IEEE High Assurance Systems Engineering Symposium (HASE), Nanjing, China, 2008
- International Conference on Security and Privacy in Communication Networks (SecureComm), Istanbul, Turkey, 2008
- International Workshop on Compiler and Architectural Techniques for Application Reliability and Security (CATARS), Anchorage, AL, 2008
- International Symposium on Theoretical Aspects of Software Engineering, China, 2008
- International Conference on Software Engineering (ICSE), Leipzig, Germany, 2008
- The 17th International World Wide Web Conference (WWW), Beijing, China, 2008
- The 15th Annual Network & Distributed System Security Symposium (NDSS), 2008
- ASIAN Symposium on Programming Language and Systems (APLAS), Singapore, 2007
- Eclipse Technology eXchange (ETX) Workshop (with OOPSLA'07), Montreal, Canada, 2007
- International Static Analysis Symposium (SAS), Seoul, Korea, 2006
- ACM SIGSOFT Symposium on Foundations of Software Engineering (FSE), Oregon, 2006
- Tools and Algorithms for the Construction and Analysis of Systems (TACAS), Austria, 2006
- International Workshop on Remote Analysis and Measurement of Software Systems (RAMSS'05)

- **Journal and Conference Reviewer:**

- Information and Computation (I&C)
- Journal of Functional Programming (JFP)
- ACM Transactions on Programming Languages and Systems (TOPLAS)
- ACM Transactions on Software Engineering and Methodology (TOSEM)
- IEEE Transactions on Software Engineering (TSE)
- Higher-Order and Symbolic Computation (HOSC)
- Symposium on Principles of Programming Languages (POPL)
- ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)
- International Conference on Software Engineering (ICSE)
- Foundations of Software Engineering (FSE)
- Static Analysis Symposium (SAS)
- Conference on Rewriting Techniques and Applications (RTA)
- International Colloquium on Automata, Languages and Programming (ICALP)
- International Conference on Computer Aided Verification (CAV)
- Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- IEEE INFOCOM Conference on Computer Communications (INFOCOM)
- Annual Network and Distributed System Security Symposium (NDSS)

- Annual Computer Security Applications Conference (ACSAC)

- **Proposal Reviewer:**

- National Science Foundation (NSF) Panelist (2005, 2006, 2008).
- Air Force Office of Scientific Research (AFOSR) Proposal Reviewer (2007).
- Army Research Office (ARO) Proposal Reviewer (2010).

- **Dissertation Award Committee:**

- ACM SIGPLAN Best Dissertation Award, 2007–2008

ADVISING AND MENTORING

1) Postdoctoral Researcher Mentoring

- E. Barr (UC Davis), August 2009–present
Awards: I3P Fellowship (2009-2010)
Accomplishments: Co-author on two publications in flagship venues (ICSE'10 and ISSTA'10)
Co-PI on two funded grants (NSF and AFOSR, 2010)

2) Graduate Student (co-)Advising

- J. Apple (UC Davis), September 2007–2009
- I. Balepin (UC Davis), September 2003–2007 (co-advisor)
- J. Crandall (UC Davis), 2004–June 2007 (co-advisor)
- M. Gabel (UC Davis), September 2006–present
- C. Gould (UC Davis), September–November 2004
- Z. Gu (UC Davis), August 2008–present
- L. Jiang (UC Davis), September 2003–September 2009
- T. Kwon (UC Davis), September 2007–present
- V. Le (UC Davis), September 2009–present
- G. Misherghi (UC Davis), March 2005–June 2007
- A. Nash (UC Davis), September 2007–2009
- D. Pallas (UC Davis), March 2004–June 2005 (co-advisor)
- A. Saebjoernsen (UC Davis), September 2006–present
- F. Sun (UC Davis), September 2007–present
- M. Van Gundy (UC Davis), September 2006–2008 (co-advisor)
- T. Vo (UC Davis), September 2009–present
- G. Wassermann (UC Davis), June 2003–July 2008
- L. Xu (UC Davis), September 2007–present
- J. Yuen (UC Davis), January 2008–2009
- D. Zinn (UC Davis), January 2007–2009 (co-advisor)

3) Undergraduate Student (co-)Advising

- Y. Xiao (UC Davis), June 2009–present
- M. Velez (UC Davis), June 2009–present
- S. Hillman (UC Davis), June 2009–present
- S. Peterson (UC Davis), July 2007–March 2008
- S. Shepard (UC Davis), August 2007–December 2007
- E. Chiu (UC Davis), January 2007–June 2007
- M. Byrd (UC Davis), June 2004–December 2004
- C. Gould (UC Davis), March 2003–June 2004
- A. Singh (UC Davis), January–June 2005

4) Visiting Scholars

- E. Tang (Nanjing University, China), September 2008–September 2009
- S. Glondu (ENS Cachan, France), June–August 2005
- K. Doh (Hanyang University, South Korea), February 2005–August 2006
- C. David (ENS Cachan, France), June–August 2002
- T. Priesnitz (Universität des Saarlandes, Germany), September–October 2001

DISSERTATION, THESIS, AND EXAM COMMITTEE

1) Doctoral Dissertation Committee

1. Jed Crandall (Computer Science; **co-advisor**), Advisor: Prof. Fred Chong [**graduated**]
Current employment: Assistant Professor, University of New Mexico
Awards: UCD CS Best Graduate Student Researcher (2007)
UCD CS Best Dissertation Award (2007)
NSF CAREER Award (2009)
2. O. Erdem Demir (Computer Science), Advisor: Prof. Prem Devanbu [**graduated**]
3. Mark Gabel (Computer Science)
Awards: ARCS Fellowship (2008, 2009)
UCD CS Best Graduate Student Researcher (2010)
4. Zhongxian Gu (Computer Science)
5. Lingxiao Jiang (Computer Science; **major advisor**) [**graduated**]
Current employment: Assistant Professor, Singapore Management University
Awards: UCD CS Best Graduate Student Researcher (2008)
UCD CS Best Dissertation Award (2009)
Honorable Mention, UCD CoE Zuhair A. Munir Dissertation Award (2009)
6. Taeho Kwon (Computer Science)
Awards: ACM SIGSOFT Distinguished Paper Award (ISSTA 2010)
7. Vu Minh Le (Computer Science)
8. Andreas Saebjoernsen (Computer Science)
9. Nija Shi (Computer Science), Advisor: Prof. Ron Olsson [**graduated**]
10. Ghassan Shobaki (Computer Science), Advisor: Prof. Ken Wilken [**graduated**]
11. Till Stegers (Computer Science), Advisor: Prof. Philip Rogaway
12. Fangqi Sun (Computer Science)
13. Thanh Vo (Computer Science)

14. Gary Wassermann (Computer Science; **major advisor**) [**graduated**]
Current employment: HP Inc.
Awards: UCD CS Best Dissertation Award (2008)
Honorable Mention, UCD CoE Zuhair A. Munir Dissertation Award (2008)
CS faculty position offers: Ohio State, NCSU, and Iowa State
15. Liang Xu (Computer Science)
16. Daniel Zinn (Computer Science), Advisor: Prof. Bertram Ludascher [**graduated**]

2) M.S. Thesis Committee

1. David Hamilton (Computer Science), *In Progress*, **Chair**
2. Jeffrey Yuen (Computer Science), *Exam Option*
3. Ghassan Mishserghi (Computer Science), *HDD: Hierarchical Delta Debugging*, 2007, **Chair**
Current employment: Google Inc.
4. Ryan Iwahashi (Computer Science), *Defining and Detecting Software Vulnerabilities that Allow Control Flow Hijack Attacks using Vulnerability-Based Signatures*, 2006, Advisor: Prof. Felix Wu
5. Tom Ristenpart (Computer Science), *Time Stamp Synchronization of Distributed Sensor Logs: Impossibility Results and Approximation Algorithms*, 2005, Advisor: Prof. Matt Bishop
6. Chad Stirling (Computer Science), *Automated Bug Isolation via Program Chipping*, 2005, Advisor: Prof. Ron Olsson

3) Qualifying Examination Committee

1. Daryl Posnett (Computer Science), *TBA*, Date: TBD
2. Mohammad Foyzur Rahman (Computer Science), *Understanding and Minimizing Software Failures*, Date: May 28, 2010
3. Michael Ogawa (Computer Science), *Visualizing the Open Source World*, Date: February 5, 2010
4. Liang Xu (Computer Science), *Binary Analyses for Detecting and Analyzing Evasive Malware*, Date: November 24, 2009
5. Taeho Kwon (Computer Science), *Detecting Unsafe Software Component Interoperation*, Date: October 20, 2009
6. Fangqi Sun (Computer Science), *Advanced Program Analyses for Web Application Security*, Date: September 18, 2009
7. Xiaoheng Chen (Electrical & Computer Engineering), *Decoder Architectures and Implementations for Structured Low-Density Parity-Check Codes*, Date: March 11, 2009
8. Robert Heath (Electrical & Computer Engineering), *Efficient Techniques for Tightening Instruction Scheduling Bounds*, Date: March 11, 2009
9. Daniel Zinn (Computer Science), *Design and Optimization of Scientific Workflows—A New Approach for Developing Coarse-Grained Parallel Applications*, Date: May 27, 2008 (**committee chair**)
10. Christian Bird (Computer Science), *Sociotechnical Collaboration and Coordination in Open Source Software*, Date: May 5, 2008
11. Matin Hashemi (Electrical & Computer Engineering), *Embedded Software Synthesis for Multi-Core Architectures*, Date: September 20, 2007
12. Jingyu Kang (Electrical & Computer Engineering), *Constructions, Applications, and Decoder Implementation of Low-Density Parity-Check Codes*, Date: September 11, 2007
13. Jeffrey Wu (Computer Science), *BOTS: A Constraint-based System for Composing Component Software Targeting Embedded Systems*, Date: June 1, 2007
14. Till Stegers (Computer Science), *Formal Indistinguishability Relations*, Date: March 23, 2007

15. Payman Mohassel (Computer Science), *Efficiency of Secure Multiparty Protocols*, Date: March 22, 2007
16. Liping Guo (Electrical & Computer Engineering), *An Energy Scalable Computational Array for Energy Harvesting Sensors*, Date: November 15, 2006
17. Lynn Nguyen (Computer Science), *Approaches to Secure Code In Same Privilege Mode As Malicious Code*, Date: September 5, 2006
18. Sophie Engle (Computer Science), *Vulnerability Analysis*, Date: September 5, 2006
19. Po-Kuan Huang (Electrical & Computer Engineering), *Efficient and Scalable Energy Optimization for Embedded System*, Date: September 5, 2006
20. Lingxiao Jiang (Computer Science), *Reliability for Numerical Software Systems*, Date: August 7, 2006
21. Chris Lupo (Electrical & Computer Engineering), *Hierarchical Selection of Spill Candidates and Spill-Code Placement in a Graph-Coloring Register Allocator*, Date: June 6, 2006
22. Gary Wassermann (Computer Science), *Security and Reliability of Web Application Metaprogramming*, Date: March 9, 2006
23. Jed Crandall (Computer Science), *Containing Rapid Polymorphic and Metamorphic Worms with Network Content Filtering*, Date: October 19, 2005 (**committee chair**)
24. Yu-Cheng Chou (Mechanical Engineering), *Dynamic Parallel Processing with Mobile Agents for Distributed Systems*, Date: September 2, 2005
25. Nija Shi (Computer Science), *Reverse Engineering of Design Patterns from Java Source Code*, Date: June 16, 2005
26. Anant Chaudhary (Computer Science), *Formal Reasoning for Intrusion Detection Systems*, Date: March 15, 2005
27. Tufan Demir (Computer Science), *Application of Biologically Inspired Diversity Ideas to Create Heterogeneous Environments for Malicious Code*, Date: March 9, 2005
28. Erdem Demir (Computer Science), *Cross Layer Adaptations*, Date: February 23, 2005
29. Tamara Dahlgren (Computer Science), *Self-Adaptive Enforcement of Interface Assertions*, Date: February 7, 2005
30. Martin Gagne (Computer Science), *A Study of Random Oracles*, Date: November 16, 2004
31. Jingmin (Jimmy) Zhou (Computer Science), *Modeling Intrusion Detection Alerts for Correlation*, Date: June 2, 2004
32. Mark Heffernan (Electrical & Computer Engineering), *Improved Instruction Scheduling*, Date: December 2, 2003
33. Tao Song (Computer Science), *Verification of Intrusion Detection Systems*, Date: September 18, 2003
34. Ghassan Shobaki (Computer Science), *Optimal Global Instruction Scheduling*, Date: June 16, 2003

TEACHING

- Software Development and OO Programming (ECS 40), UC Davis [F'07, W'11]
- Programming Languages (ECS 140A), UC Davis [S'04, S'07, S'08, F'08, S'09]
- Compilers (ECS 142), UC Davis, [W'03, W'05, F'06] q
- Formal Semantics of Programming Languages (ECS 240), UC Davis [W'06, S'07, S'08, S'09, W'11]
- Seminar on Program Analysis (ECS 289C), UC Davis [S'03, W'04, W'05]

UNIVERSITY SERVICE ACTIVITIES

- Chair, Computer Science Graduate Admissions Committee, UC Davis, 2007–2009
- Computer Science Department Personnel Committee, UC Davis, 2007-2009
- Computer Science Department Faculty Search Committee, UC Davis, 2008-2009
- Computer Science Department Colloquium Organizer, UC Davis, 2007-2008
- Reviewer, Graduate Internal Fellowship Applications, UC Davis, 2007
- Graduate Advisor, Department of Computer Science, UC Davis, 2005–2007
- CS Representative to the Academic Senate, UC Davis, 2005–2007
- College of Engineering Research and Library Committee, 2005–2006
- GGCS Graduate Admissions Committee, 2004–2006
- Faculty Advisor of the Student Workshop on Computing, July–October 2004
- Faculty Representatives Committee, Computer Science, UC Davis, 2004–2005
- Undergraduate Affairs Committee, Computer Science, UC Davis, 2003–2004
- CS Representative to the PSE Library Committee, Computer Science, UC Davis, 01/2003–06/2003