

# Ankur Taly

468 Gates Building  
353 Serra Mall  
Stanford, CA 94305

Phone: (732) 513-5690  
Email: ataly@stanford.edu  
Homepage: <http://theory.stanford.edu/~ataly>

## Education

- **Stanford University** Sept 2007 - present  
Ph.D Candidate Expected Graduation: Jun 2012  
Google PhD Fellow since Jun 2010  
Master of Science in Computer Science Jun 2010  
Advisor: Prof. John C. Mitchell
- **Indian Institute of Technology (IIT), Bombay** Jul 2003 - May 2007  
Bachelor of Technology in Computer Science and Engineering  
Cumulative GPA: 8.82/10

## Research Interests

Language Security, Web Security, Program Verification and Synthesis

## Professional Experience

- **Research Assistant, Stanford Security Lab, Stanford, USA** Nov 2007 - present  
Advisor: Prof. John C. Mitchell  
Designed provably-correct language-based mechanisms for sandboxing untrusted JavaScript on a trusted web-page. Analyzed real-world sandboxing mechanisms such as Yahoo! ADSafe, Facebook FBJS and Google Caja and identified (and reported) several security vulnerabilities in them (**refer Publications [3,5,7,8,9,11,14]**).
- **Research Intern, Microsoft Research, Redmond, USA** Jun-Sept 2011  
Mentor: Dr. Patrice Godefroid  
Developed a technique for automatically synthesizing symbolic instruction encodings (used for symbolic execution) from I/O samples. Implemented the technique to automatically synthesize encodings for over 500 ALU instructions (8/16/32 bits, outputs, EFLAGS) from the x86 instruction set (**refer Publication [2]**).
- **Research Intern, Google Inc, Mountain View, USA** Jun-Sept 2010  
Mentors: Dr. Ulfar Erlingsson, Dr. Jasvir Nagra, Dr. Mark S. Miller  
Developed a provably sound technique for confinement analysis of security-critical JavaScript APIs. Implemented the technique as a fully automated tool and used it for finding a previously undiscovered vulnerability in the Yahoo! ADSafe API and subsequently proving confinement for the fixed API (**refer Publication [3]**).
- **Visiting Student Researcher, Imperial College London, London, UK** Jul 2009  
Mentor: Dr. Sergio Maffeis  
Designed an efficient proof technique for a certain class of safety properties of programs, that is amenable to incremental changes to the syntax and semantics of the underlying programming language.
- **Research Intern, SRI International, Menlo Park, USA** Jun-Sept 2008  
Mentor: Dr. Ashish Tiwari  
Developed constraint-solving based techniques for verifying and synthesizing safe hybrid systems. Extensively collaborated with Dr. Tiwari after my internship and developed deductive techniques for verifying stability and reachability properties of hybrid systems (**refer Publications [1,4,6,10]**).
- **Research Intern, Ecole Polytechnique, Paris, France** May-Jul 2005 and May-Jul 2006  
Mentors: Prof. Eric Goubault, Prof. Stephane Gaubert  
Developed a policy-iteration based fixed computation algorithm for relational abstract domains, that was faster and more precise than the classical Kleene iteration procedure with widening/narrowing. Use the algorithm to build an abstract interpretation based static analyzer for C programs (**refer Publication [12]**).

## Selected Awards and Honors

- 3<sup>rd</sup> prize for Publication [2], **AT&T Best Applied Security Paper Award** competition, Nov 2011.
- **Google PhD Fellowship in Language Security (2010-2012)**, Jun 2010.
- **Stanford Computer Forum Fellowship (2007)**, Sept 2007.
- **All India Rank 69** out of 180,000 students, IIT joint entrance examination, Jun 2003.
- **Gold Medal**, Indian National Physics Olympiad, May 2003.
- **Gold Medal**, Indian National Chemistry Olympiad, May 2003.

## Publications

### Journals:

1. Ankur Taly, Sumit Gulwani, Ashish Tiwari - “Synthesizing Switching Logic using Constraint Solving”, *Journal on Software Tools for Technology Transfer* (STTT), Springer, 2011.

### Conferences/Workshops:

2. Patrice Godefroid, Ankur Taly - “Automated Synthesis of Symbolic Instruction Encodings from I/O Samples” - Programming Languages Design and Implementation (PLDI) conference, Jun 2012 (to be published).
3. Ankur Taly, Ulfar Erlingsson, John C. Mitchell, Mark S. Miller, Jasvir Nagra - “Automated Analysis of Security-Critical JavaScript APIs”, *IEEE Symposium on Security and Privacy* (S&P), May 2011 (**Award paper**).
4. Ankur Taly, Ashish Tiwari - “Switching Logic Synthesis for Reachability”, *International Conference on Embedded Software* (EMSOFT), Oct 2010.
5. Sergio Maffeis, John C. Mitchell, Ankur Taly - “Object Capabilities and Isolation of Untrusted Web Applications”, *IEEE Symposium on Security and Privacy* (S&P), May 2010.
6. Ankur Taly, Ashish Tiwari - “Deductive Verification of Continuous Dynamical Systems”, *Foundations of Software Technology and Theoretical Computer Science* (FST&TCS), Dec 2009.
7. Sergio Maffeis, John C. Mitchell, Ankur Taly - “Isolating JavaScript with Filters, Rewriting, and Wrappers”, *European Symposium on Research in Computer Security* (ESORICS), Sept 2009.
8. Sergio Maffeis, Ankur Taly - “Language-Based Isolation of Untrusted JavaScript”, *IEEE Symposium on Computer Security Foundations* (CSF), Jul 2009.
9. Sergio Maffeis, John C. Mitchell, Ankur Taly - “Run-Time Enforcement of Secure JavaScript Subsets”, *Web 2.0 Security and Privacy* (W2SP) workshop, May 2009.
10. Ankur Taly, Sumit Gulwani, Ashish Tiwari - “Synthesizing Switching Logic using Constraint Solving”, *Verification, Model Checking and Abstract Interpretation* (VMCAI), Jan 2009.  
**Invited to: special issue of STTT journal for best papers from VMCAI 2009.**
11. Sergio Maffeis, John C. Mitchell, Ankur Taly - “An Operational Semantics for JavaScript”, *Asian Programming Languages Symposium* (APLAS), Dec 2008.
12. Stephane Gaubert, Eric Goubault, Ankur Taly, Sarah Zennou - “Static Analysis by Policy Iteration on Relational domains”, *European Symposium on Programming* (ESOP), Mar 2007.
13. Sudeep Juvekar, Ankur Taly, Varun Kanade, Supratik Chakraborty - “Efficient Symbolic Reachability of Networks of Transition Systems”, *General Motors Workshop on Next Generation Design and Verification Methodologies for Distributed Embedded Control Systems*, Jan 2007.

### Manuscripts:

14. Ankur Taly - “Separation Logic and the Mashup Isolation Problem”, Technical report, Apr 2010.

## Other Research Literature

- Ankur Taly - “Efficient Guided Symbolic Reachability Analysis”, Undergraduate thesis, May 2007.
- Ankur Taly - “Automata on Infinite Inputs”, Junior thesis, Dec 2006.

## Selected Invited Talks

- **Sandboxing Untrusted JavaScript**  
Dagstuhl Workshop on Foundations of Scripting Languages, Schloss Dagstuhl, Germany Jan 2012  
Research in Software Engineering (RiSE) group, Microsoft Research Redmond Aug 2011  
Logic and Semantics group, Queen Mary College London Feb 2011
- **Automated Analysis of Security-Critical JavaScript APIs**  
Computer Security Awareness Week (CSAW), NYU-Polytechnique Nov 2011
- **Isolating JavaScript with Filters, Rewriting, and Wrappers**  
Software Validation group, Fujitsu Labs America Feb 2010  
Rigorous Software Engineering (RSE) group, Microsoft Research Bangalore Dec 2009
- **Structural Operational Semantics and JavaScript**  
Stanford Computer Security Workshop Apr 2009  
Guest lecture in the Stanford course “CS 258: Programming Language Theory” Feb 2009
- **Automatic Verification and Synthesis of Hybrid systems**  
Stanford Software Lunch Jan 2010  
Computer Systems Laboratory (CSL), SRI International Sept 2008
- **Static Analysis by Policy Iteration on Relational domains**  
Formal Verification group, French Atomic Energy Commission (CEA) Jul 2006

## Programming Skills

- **Programming Languages:** JavaScript, ML, C/C++, Ruby.
- **Tools:** Z3 (SMT solver), bddbddb (Datalog engine), NuSMV (Model Checker), Matlab.

## Activities

- Finalist at the 2011 CSAW Applied Security Quiz competition.
- Course Assistant at Stanford University for the courses:  
CS242: “Programming Languages”, Sept-Nov 2008.  
CS155: “Computer and Network Security”, Mar-May 2011.
- Reviewed papers for conferences: CCS 2011, IEEE S&P 2011, POPL 2011, IEEE S&P 2010, ESORICS 2009.
- Coordinator of the Stanford security seminar since Sept 2008.
- Was part of IIT Bombay’s “tech team”, responsible for organizing various robotics competitions.
- Was one of the organizers of IIT Bombay’s annual cultural festival “Mood Indigo”.