

Ankur Taly

1600 Amphitheatre Pkwy
Mountain View, CA 94043

Email: ankur.taly@gmail.com

Employment

- **Google Inc., Mountain View, CA, USA**

Staff Research Scientist, Aug. 2012 — present

Current work (May 2016—present)

- Working on deep learning approaches to automated program synthesis.
- Working on debugging and understanding deep neural networks using techniques from programming languages, logic, and mathematical analysis. (refer **Publication [3]**)

Prior work (Aug. 2012 — May 2016)

- Designed and implemented the security model for the *Vanadium* application framework; the model supports fully decentralized identities, mutual authentication and authorization, fine-grained delegation, and end-to-end encryption. (refer **Publications [1, 4, 5]**, **Patents [2—4]**)
- Developed the core technology for *Macaroons* — a flexible authorization credential for decentralized and controlled delegation of authority among principals in the Web, Cloud and other distributed systems. (refer **Publication [6]**, **Patent [1]**)

Education

- **Stanford University**

Ph.D. in Computer Science, Jun. 2012

Thesis title: *Sandboxing Untrusted JavaScript*

Advisor: Prof. John C. Mitchell

Google Ph.D. Fellow

M.S. in Computer Science, Jun. 2010

- **Indian Institute of Technology (IIT), Bombay**

B. Tech in Computer Science and Engineering, May 2007

Professional Activities

- **Teaching:**

- Taught a **short course** on “Distributed Authorization” at the International summer school on Foundations of Security, Analysis and Design (FOSAD), held at Bertinoro, Italy, in Sep. 2016.
- **Guest lectures in graduate courses:**
 - * CS223: “Advanced Computer Security”, UC Santa Cruz, USA Oct. 2012
 - * CS258: “Programming Language Theory”, Stanford University, USA Mar. 2009
 - * CS242: “Programming Languages”, Stanford University, USA Oct. 2008

- **Google Research outreach:**

- Reviewer for several Faculty Research Award (FRA) and Google PhD fellowship proposals in Security and Programming languages.
- Official FRA liaison for:

- * 2013 FRA in Security to Prof. David Evans' group (University of Virginia).
- * 2015 FRA in Security to Prof. Stephen Chong's group (Harvard University).
- Panelist, 2014 Google Bay Area PhD Summit.
- **Program Committees:** ACM PLDI (ERC) 2014, ETAPS POST 2014, ACM PLAS 2013, HOTSPOT 2013.
- **External Reviewer:** Journal of Computer Security, ACM POPL 2012 & 2013, IEEE S&P 2011 & 2010, ACM CCS 2011, ACM PLDI 2010, ACM OOPSLA 2011, ACM PLAS 2011, ESORICS 2009.

Selected Awards and Honors

- **Outstanding paper award** for Publication [4], 21st European Symposium on Research in Computer Security, Sep. 2016
- **3rd prize** for Publication [2], **AT&T Best Applied Security Paper Award** competition, Nov. 2011.
- **Google PhD Fellowship in Language Security (2010-2012)**, Jun. 2010.
- Selected for **best papers from VMCAI 2009**, 10th Int'l conference on Verification, Model checking and Abstract Interpretation, for Publication [10], Dec. 2009.
- **Stanford Computer Forum Fellowship**, Sep. 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.

Research Interests

Machine Learning, Applied Cryptography, Computer Security, Programming Languages, and Mathematical Logic.

Research Experience

- **Understanding Deep Neural Networks** May. 2016 — present
with colleagues at Google Inc.
Working on techniques for debugging and understanding the behavior of deep neural networks (DNN), in order to better comprehend their inner workings, and reason about their correctness and robustness. (**refer Publication [3]**)
- **Identity and Authorization** Aug. 2012—present
with colleagues at Google Inc.
The goal of this research is to develop cutting-edge Identity, Authentication and Authorization frameworks for highly distributed services and applications. My key contributions so far have been: (1) Vanadium security model — fully decentralized identities, mutual authentication and authorization, fine-grained delegation, and end-to-end encryption, and (2) *Macaroons* — a flexible authorization credential for decentralized and controlled delegation of authority among principals in the Web, Cloud and other distributed system settings. (**refer Publications [1, 4, 5, 6], Patents [1–4]**)
- **Language Security and Web Security** Nov. 2007—present
with Sergio Maffeis (Imperial College London), John Mitchell (Stanford University), Ulfar Erlingsson (Google), Mark Miller (Google), and Jasvir Nagra (Google)
The goal of this research is to develop mechanisms for securing software comprising of untrusted code by restricting the language in which untrusted code is written. In the past few years, I have worked on developing a mathematical foundation for reasoning about JavaScript, designing provably-correct language-based mechanisms for sandboxing untrusted JavaScript code on a trusted Web page, and developing provably-sound

static analysis techniques for JavaScript programs. I also analyzed several real-world sandboxing mechanisms such as Yahoo! ADSafe, Facebook FBJS and Google Caja and identified (and reported) several security vulnerabilities in them. (refer Publications [8, 10, 12, 13, 14, 16])

- **Verification and Synthesis** Jun. 2008—Dec. 2011
with Ashish Tiwari (SRI International), Patrice Godefroid (Microsoft Research, Redmond)
The goal of this research is to develop techniques for verifying and synthesizing provably-correct hardware, software, and hybrid systems using techniques from constraint-solving, and mathematical logic. My work in this area has focussed on automatically verifying safety, stability, and reachability properties of hybrid systems, synthesizing safe switching logics for hybrid systems, and synthesizing symbolic instruction encodings for the x86 instruction set. (refer Publications [1, 7, 9, 11, 15, 17, 18])

Publications

Journals and Book Chapters:

1. Ankur Taly, Asim Shankar—“Distributed Authorization in Vanadium”, in proc. of *Lecture Notes on Foundations of Security, Analysis and Design* (FOSAD), Springer, Sep. 2016.
2. Ankur Taly, Sumit Gulwani, Ashish Tiwari—“Synthesizing Switching Logic using Constraint Solving”, in proc. of *Int’l Journal on Software Tools for Technology Transfer* (STTT), Springer, Jan. 2011.

Conferences/Workshops:

3. Mukund Sundararajan, Ankur Taly, Qiqi Yan—“Axiomatic Attribution for Deep Networks”, in proc. of *34th International Conference on Machine Learning* (ICML), Aug. 2017.
4. David Wu, Ankur Taly, Asim Shankar, Dan Boneh—“Privacy, Discovery and Authentication for Internet of Things”, in proc. of *21st European Symposium on Research in Computer Security* (ESORICS), Sep. 2016 (**award paper**).
5. Martin Abadi, Mike Burrows, Himabindu Pucha, Adam Sadovskiy, Asim Shankar, Ankur Taly—“Distributed Authorization With Distributed Grammars”, in proc. of *Programming Languages with Applications to Biology and Security* (PLABS), Jun. 2015.
6. Arnar Birgisson, Joe Politz, Ulfar Erlingsson, Ankur Taly, Michael Vrable, Mark Lentczner—“Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud”, in proc. of *21st Int’l Conf. on Network and Distributed System Security Symposium* (NDSS), Feb. 2014.
7. Patrice Godefroid, Ankur Taly—“Automated Synthesis of Symbolic Instruction Encodings from I/O Samples”, in proc. of *34th ACM Int’l Conf. on Programming Language Design and Implementation* (PLDI), Jun. 2012.
8. Ankur Taly, Ulfar Erlingsson, John C. Mitchell, Mark S. Miller, Jasvir Nagra—“Automated Analysis of Security-Critical JavaScript APIs”, in proc. of *32nd IEEE Int’l Symposium on Security and Privacy* (S&P), May 2011 (**award paper**).
9. Ankur Taly, Ashish Tiwari—“Switching Logic Synthesis for Reachability”, in proc. of *10th ACM Int’l Conf. on Embedded Software* (EMSOFT), Oct. 2010.
10. Sergio Maffei, John C. Mitchell, Ankur Taly—“Object Capabilities and Isolation of Untrusted Web Applications”, in proc. of *31st IEEE Int’l Symposium on Security and Privacy* (S&P), May 2010.
11. Ankur Taly, Ashish Tiwari—“Deductive Verification of Continuous Dynamical Systems”, in proc. of *29th Int’l Conf. on Foundations of Software Technology and Theoretical Computer Science* (FST&TCS), Dec. 2009.
12. Sergio Maffei, John C. Mitchell, Ankur Taly—“Isolating JavaScript with Filters, Rewriting, and Wrappers”, in proc. of *14th European Symposium on Research in Computer Security* (ESORICS), Sep. 2009.
13. Sergio Maffei, Ankur Taly—“Language-Based Isolation of Untrusted JavaScript”, in proc. of *22nd IEEE Int’l Symposium on Computer Security Foundations* (CSF), Jul. 2009.

14. Sergio Maffei, John C. Mitchell, Ankur Taly—“Run-Time Enforcement of Secure JavaScript Subsets”, *3rd Web 2.0 Security and Privacy (W2SP) workshop*, May 2009.
15. Ankur Taly, Sumit Gulwani, Ashish Tiwari—“Synthesizing Switching Logic using Constraint Solving”, in proc. of *10th Int’l Conf. on Verification, Model Checking and Abstract Interpretation (VMCAI)*, Jan. 2009 (selected as one of the best papers).
16. Sergio Maffei, John C. Mitchell, Ankur Taly—“An Operational Semantics for JavaScript”, in proc. of *6th Asian Programming Languages Symposium (APLAS)*, Dec. 2008.
17. Stephane Gaubert, Eric Goubault, Ankur Taly, Sarah Zennou—“Static Analysis by Policy Iteration on Relational domains”, in proc. of *16th European Symposium on Programming (ESOP)*, Mar. 2007.
18. Sudeep Juvekar, Ankur Taly, Varun Kanade, Supratik Chakraborty—“Efficient Symbolic Reachability of Networks of Transition Systems”, in proc. of *1st General Motors Workshop on Next Generation Design and Verification Methodologies for Distributed Embedded Control Systems*, Jan. 2007.

Manuscripts:

19. Ankur Taly - “Separation Logic and Mashup Isolation”, Technical report, Stanford University, Apr. 2010.

Theses:

20. Ankur Taly—“Sandboxing Untrusted JavaScript”, Doctoral thesis, Stanford University, May 2013.
21. Ankur Taly—“Efficient Guided Symbolic Reachability Analysis”, Bachelor’s thesis, IIT Bombay, May 2003.
22. Ankur Taly—“Automata on Infinite Inputs”, Junior thesis, IIT Bombay, Dec. 2006.

Patents

1. Raja Daoud, Ankur Taly, Himabindu Pucha, Michael Burrows, Jatin Lodhia—“Signatures Of Updates Exchanged In A Binary Data Synchronization Protocol”, Sep. 2016.
2. Martin Abadi, Mike Burrows, Himabindu Pucha, Adam Sadovsky, Asim Shankar, Ankur Taly—“Authorization in a Distributed System Using Access Control Lists and Groups ”, May. 2015.
3. Ankur Taly, Asim Shankar, Gautham Thambidorai, David Presotto—“Security Model For Identification And Authentication In Encrypted Communications Using Delegate Certificate Chain Bound To Third Party Key”, Apr. 2015.
4. Ulfar Erlingsson, Ankur Taly, Michael Vrabie, Mark Lentczner—“Macaroons: Methods and Systems of Generating and Using Authentication Credentials for Decentralized Authorization in the Cloud”, Aug. 2013.

Selected Invited Talks

- Bhabha Atomic Research Center, Mumbai, India Nov. 2015
- Keybase.io, San Francisco, USA Aug. 2015
- Vail Computer Elements Workshop (VCEW), Vail, USA Jun. 2015
- EasyAuth seminar series, Google Inc., Mountain View, USA Aug. 2013
- Computer Systems Laboratory, SRI International, Menlo Park, USA Apr. 2012
- CS Colloquium, Microsoft Research Silicon Valley, Mountain View, USA Mar. 2012
- Tech Talk, Google Inc., Mountain View, USA Feb. 2012
- Programming Languages group, Adobe Systems, San Jose, USA Feb. 2012

- Dagstuhl Workshop on Foundations of Scripting Languages, Schloss Dagstuhl, Germany Jan. 2012
- Computer Security Awareness Week (CSAW), NYU-Polytechnique, Brooklyn, USA Nov. 2011
- Logic and Semantics group, Queen Mary College, London, UK Feb. 2011
- Software Validation group, Fujitsu Labs America, Sunnyvale, USA Feb. 2010
- Rigorous Software Engineering group, Microsoft Research Bangalore, Bangalore, India Dec. 2009
- Stanford Computer Security Workshop, Stanford, USA Apr. 2009

Programming Skills

- **Programming Languages:** Go, Python, JavaScript, ML, C/C++.
- **Tools:** ProVerif (theorem prover), Z3 (SMT solver), bddbddb (Datalog engine).

Activities

- Attended Dagstuhl workshop on Foundation of Scripting Languages, at Schloss Dagstuhl, Germany, 2012.
- Finalist at the 2011 CSAW Applied Security Quiz competition.
- Course Assistant at Stanford University for the courses: CS155: “Computer and Network Security” (Mar.—May 2011), CS242: “Programming Languages” (Sep. — Nov. 2008)
- Coordinated the Stanford security seminar from Sep. 2008 to Jun. 2012.

Last updated: June 8, 2017