# David Swasey

Pittsburgh, PA 15218
david.swasey at gmail
swasey.github.io

## SUMMARY

Formal Methods Engineer • Research Engineer • Programmer
Program Logics • Type Systems • Program Synthesis • Software Architecture
Systems Code Verification • Concurrent Separation Logic • Computer Security

## EDUCATION

**Max Planck Institute for Software Systems**
*Ph.D. Candidate*
July 2012 – May 2020

**Carnegie Mellon University**
*B.S. in Computer Science with a minor in Mathematical Sciences*
August 2006 with University Honors

## AWARDS

**2023 Alonzo Church Award** for Outstanding Contributions to Logic and Computation, for the design and implementation of Iris, a higher-order concurrent separation logic framework.

**PhD Scholarship,** Microsoft Research, January 2014 – December 2016.

## EXPERIENCE

**Riverside Research** — *Senior Research Scientist–Formal Methods*
Pittsburgh ⋄ February 2025 – present (under Gordon Stewart)

**BlueRock Security, Inc.** — *Formal Methods Engineer*
Saarbrücken & Pittsburgh ⋄ June 2020 – October 2024 (under Gregory Malecha)

- Planned and led effort to specify and verify the NOVA Microhypervisor
- Added (with Malecha) a semantics and logic for C++ templates
- Improved axiomatic semantics for C++
- Expanded and improved specification synthesis
- Contributed to proof automation

**MPI-SWS** — *Ph.D. Candidate*
Saarbrücken ⋄ July 2012 – May 2020 (co-advised by Derek Dreyer and Deepak Garg)

- Introduced (with others) the Iris separation logic framework
- Introduced the security property *robust safety* to separation logic
- Developed a logic for the Firefox security membrane (unpublished)

**CMU (CyLab)** — *Principal Research Analyst*
Pittsburgh ⋄ September 2006 – June 2012 (under Lujo Bauer)

- Improved Grey, a proof-carrying authorization system deployed in CyLab and the University of North Carolina
- Introduced (with others) delegation across authorization logics
- Improved all Grey software

**CMU (PoP Group)** — *Senior Research Programmer, Research Programmer*
Pittsburgh ⋄ June 1998 – August 2006 (under Robert Harper)

- Improved TILT, a compiler for Standard ML
- Introduced separate compilation to SML
- Improved the FoxNet and other software in the ConCert and Fox projects

**CMU (CSD)** — *Research Programmer, Research Assistant*
Pittsburgh ⋄ August 1994 – May 1998 (under Roger Dannenberg)

- Grew "Just-in-Time Lectures" to licensed software
- Optimized JITL production with a lecture compiler
- Added encryption to QuickTime
- Added curriculum analysis and a user-interface to the IDEAS system for intelligent tutors

**Visual Symphony, Inc.** — *Programmer*
Pittsburgh ⋄ February 1993 – July 1994 (under Peter Capell)

- Led (with Capell) development of the award-winning Federal Railroad Administration FRALSS training software for CSX
- Added digitial video support to Authorware
- Prototyped user interfaces

## PUBLICATIONS

### *Conference and Workshop Publications*

1. David Swasey, Deepak Garg, and Derek Dreyer. Robust and compositional verification of object capability patterns. In *OOPSLA 2017: Proceedings of the ACM on Programming Languages, Vol. 1, No. OOPSLA*, pages 89:1–89:26, Vancouver, Canada, October 2017. Recipient of an **OOPSLA Distinguished Paper Award**.

2. Ralf Jung, David Swasey, Filip Sieczkowski, Kasper Svendsen, Aaron Turon, Lars Birkedal, and Derek Dreyer. Iris: Monoids and invariants as an orthogonal basis for concurrent reasoning. In *POPL 2015: 42nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 637–650, Mumbai, India, January 2015.

3. Elli Fragkaki, Lujo Bauer, Limin Jia, and David Swasey. Modeling and enhancing Android's permission system. In *Computer Security — ESORICS 2012 — 17th European Symposium on Research in Computer Security*, pages 1–18, Pisa, Italy, September 2012. Springer LNCS 7459.

4. Lujo Bauer, Limin Jia, Michael K. Reiter, and David Swasey. xDomain: Cross-border proofs of access. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, pages 43–52, Stresa, Italy, June 2009.

5. David Swasey, Tom Murphy VII, Karl Crary, and Robert Harper. A separate compilation extension to Standard ML. In *Proceedings of the 2006 ACM SIGPLAN Workshop on ML*, pages 32–42, Portland, Oregon, September 2006.

### *Technical Reports*

6. Elli Fragkaki, Lujo Bauer, Limin Jia, and David Swasey. Modeling and enhancing Android's permission system. Technical Report CMU-CyLab-11-020, CyLab, Carnegie Mellon University, April 2012. Extended version of [3].

7. Lujo Bauer, Limin Jia, Michael K. Reiter, and David Swasey. xDomain: Cross-border proofs of access. Technical Report CMU-CyLab-09-005, CyLab, Carnegie Mellon University, March 2009. Extended version of [4].

8. David Swasey, Tom Murphy VII, Karl Crary, and Robert Harper. A separate compilation extension to Standard ML (revised and expanded). Technical Report CMU-CS-06-104R, School of Computer Science, Carnegie Mellon University, September 2006. Extended version of [5].

9. David Swasey, Tom Murphy VII, Karl Crary, and Robert Harper. A separate compilation extension to Standard ML (working draft). Technical Report CMU-CS-06-104, School of Computer Science, Carnegie Mellon University, January 2006. Superseded by [8].

## PROFESSIONAL ACTIVITIES AND SERVICE

External reviewer, POPL 2017, CSF 2015, ESOP 2015, SBMF 2015, ICFP 2014, AsiaCCS 2013, Oakland 2013, TDSC 2012, PPDP 2000.

Artifact Evaluation Committee, POPL 2019.

Technical support, ICFP 2002 and PPDP 2002, Pittsburgh, PA, October 3–8, 2002.

Local organizer, CADE-17, Pittsburgh, PA, June 17–20, 2000.

Technical support, ICFP 1999, Paris, France, September 27–29, 1999.

Attendee, TYPES Summer School, *Theory and Practice of Formal Proofs,* Giens, France, August 30–September 10, 1999.

### *Teaching*

TA, core graduate course *Semantics* (taught by Derek Dreyer and Gert Smolka), MPI-SWS & Saarland University, Winter Semester 2017–2018.

TA, advanced graduate course *Parametricity and Modular Reasoning* (taught by Derek Dreyer), MPI-SWS & Saarland University, Winter Semester 2012-2013.

JITL presentation, United States Army, Combined Arms Support Command, Fort Lee, VA, March 24–27, 1997.

Guest lecturer, graduate course 15–820B *Advanced Topics in HCI: User Interface Software,* Carnegie Mellon University, 1996.

### *Lectures on JITL Production*

Singapore, February 16–19, 1998.

Schaumburg, IL, November 10–14, 1997.

Schaumburg, April 22–24, 1997.

Schaumburg, December 1–6, 1996.

Scottsdale, AZ, 1996.

## PROFESSIONAL MEMBERSHIPS

ACM & ACM SIGPLAN, January 1999 – December 2013.

ACM SIGACT, January 1999 – December 2000.

Society for Applied Learning Technology (SALT), August 1997 – August 1998.

Last updated: February 15, 2025
https://swasey.gitlab.io/Swasey-David-CV-2025.pdf