David Swasey

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

Formal Methods Engineer • Research Engineer • Programmer
Systems Code Verification • Concurrent Separation Logic • Computer Security

EXPERIENCE

Riverside Research — *Senior Research Scientist–Formal Methods*

Pittsburgh - February 2025 - present (under Gordon Stewart)

BlueRock — *Formal Methods Engineer*

Saarbrücken & Pittsburgh - June 2020 - October 2024 (under Gregory Malecha)

- Planned and led effort to specify and verify the NOVA Hypervisor
- 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- Developed a logic for the Firefox security membrane (unpublished)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

CMU (PoP Group) — *Senior Research Programmer*

Pittsburgh - June 1998 - August 2006 (under Robert Harper)

- Improved TILT, a compiler for Standard ML
- Introduced separate compilation to SML

CMU (CSD) — *Research Programmer*

Pittsburgh - July 1996 - May 1998 (under Roger Dannenberg)

- Grew "Just-in-Time Lectures" to licensed software
- Optimized JITL production with a lecture compiler

Visual Symphony — *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

SKILLS

Program Logics

Type Systems

Program Synthesis

Software Architecture

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

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 Mathematical Sciences
August 2006 - University Honors