Dan McArdle

Experience

Google | October 2018 - January 2023

Software Engineer | Cambridge, MA

- **OpenTitan**
  - Bitstream splicing. Saves hours of CPU time.
  - JTAG-based test infrastructure. Define tests in GDB script.
  - Developed a handful of e2e tests for the chip.
  - Achieved a 1.5-5x speed in memory functions with PR #14243.
  - Created a pipeline that enables semantic code search for C/C++ sources. For example, see dif_otbn.c.
  - Developed bitstream bisect tool, that enables rapid git-bisecting by avoiding multi-hour builds.
- **Chrome**
  - Developed prototypes of *TLS Encrypted Client Hello* (ECH) in the BoringSSL library.
    - Server prototype in CL 45285
  - Developed prototypes of Hybrid Public Key Encryption (HPKE) in BoringSSL.
    - draft-irtf-cfrg-hpke-04 in CL 41304
    - draft-irtf-cfrg-hpke-07 in CL 44904
  - Contributed to specification of a new DNS resource record.
    - https://datatracker.ietf.org/doc/draft-ietf-dnsop-svcb-https/
  - Developed many fuzzers for Chrome.
    - Discovered and fixed tons of security bugs.
  - Hosted an intern developing Extended DNS Errors.

Draper Laboratory | March 2018 - October 2018

Member of Technical Staff | Cambridge, MA

- Technical work on DoD projects with a focus on formal methods and cybersecurity.
- Specific topics include formally-verified software, static taint analysis, and fuzzing
- Audited Adam Chlipala's Spring 2018 *Formal Reasoning about Programs* at MIT

Architecture Technology Corporation | August 2015 - February 2018

Software Engineer | Ithaca, NY

- Cybersecurity R&D for DoD customers and technical proposal writing
- Wrote winning Phase II SBIR proposal and managed two-year development effort
- Supervised interns developing interactive security coursework
- Technical work included Linux/FreeBSD kernel hacking and modifying the LLVM compiler

State University of New York at Buffalo | June 2015 - August 2015

Adjunct Professor for CSE 305: Introduction to Programming Languages

- Developed lectures and coursework teaching a variety of programming paradigms
- Focused on Haskell programming language and the Lambda calculus

Syracuse University | August 2013 - May 2014

Graduate Teaching Assistant | Syracuse, NY

- CIS 252: Introduction to Computer Science (Spring 2014) Graded papers, held weekly office hours, and led two lab sessions per week in Haskell language.
- CIS 275: Discrete Math (Fall 2013) Graded papers, held office hours, and led a weekly recitation.

Metis Consulting Group | May 2011 - August 2014

Intern & Software Engineer | Syracuse, NY

- Responsible for web application development projects, specializing in travel
- Tech stack included ColdFusion, PHP, Microsoft SQL Server, and JavaScript

Education

Master of Science | Computer Science and Engineering | 2015

State University of New York at Buffalo, Buffalo, NY

- Published research on adding real-time capabilities to a functional programming language

Bachelor of Arts | Computer Science | 2013

State University of New York at Geneseo, Geneseo, NY

- Directed Studies focused on Document Image Analysis
- Presented *Stompbox* framework for real-time simulation of analog audio effects at GREAT Day (Geneseo Recognizing Excellence, Achievement, and Talent)