Dan McArdle

https://github.com/dmcardle

https://nmcardle.com/resume

d@nmcardle.com|315-317-6220

I am a software engineer with over 8 years of experience in security, systems software, and cryptography. I enjoy finding security vulnerabilities in low-level code by writing fuzzers, performing static analysis, and sometimes just by manual inspection. Recently, I developed infrastructure for end-to-end hardware verification of OpenTitan, an open-source silicon root-of-trust chip. I've contributed to IETF specifications and developed prototypes of draft revisions to evaluate their feasibility and correctness. In the defense arena, I hacked on FreeBSD, LLVM's X86 codegen, and I've had exposure to formal verification with the Coq proof assistant.

Experience

Google

Software Engineer | Cambridge, MA | October 2018 - January 2023

OpenTitan

- Developed tooling to splice OTP images into pre-built FPGA bitstreams. This enabled comprehensive end-to-end tests and saved >1 hour per test.
- Created infrastructure for JTAG-based tests defined with GDB and OpenOCD.
- Wrote end-to-end tests for the chip, e.g. PR #16169, PR #16139, PR #15798.
- Optimized memory functions and achieved a 1.5-5x speedup. PR #14243.
- Enabled *semantic* codesearch features for C/C++ sources, e.g. dif_otbn.c.
- Designed and added a tool for rapid bisecting. PR #16701.

Chrome

- Developed prototypes of *TLS Encrypted Client Hello* (ECH) in BoringSSL. ECH enables clients to encrypt sensitive fields such as the desired server name, which are sent in cleartext by default.
  - Added GREASE support for drafts 08 and 09 [CL 40204, CL 44784]. GREASE staves off ecosystem ossification by enabling clients to send fake ECH data to servers that do not support it; passive middleboxes cannot tell the difference.
  - Implemented backend server for draft 09 [CL 43924].
  - Completed C and Go server prototypes for draft 09 [CL 45285].
  - More CLs of prototypes?
- Developed prototypes of RFC 9180: Hybrid Public Key Encryption (HPKE) in BoringSSL.
  - Implemented draft-irtf-cfrg-hpke-04 in C [CL 41304].
  - Implemented draft-irtf-cfrg-hpke-05 in Go [CL 42124].
  - Updated C implementation to draft-irtf-cfrg-hpke-05 [CL 42444].
  - Added PSK variants of HPKE [CL 42664].
  - Updated C and Go implementations to draft-irtf-cfrg-hpke-07 [CL 44904].
- Contributed to specification for SVCB/HTTPS, a new DNS resource record required for practical deployment of TLS ECH.
  - While HTTPS record specification was in flux, designed and ran a Chrome experiment to study the impact of new resource records on the DNS ecosystem [design doc].
  - Add crbug?
  - **Find GitHub PRs**
- Developed many fuzzers for Chrome.
  - Discovered and fixed tons of security bugs.
  - Link to a few specific bugs.

- Hosted an intern who implemented RFC 8914: Extended DNS Errors in Chrome's net stack.

Draper Laboratory

Software Engineer / Member of Technical Staff | Cambridge, MA | March 2018 - October 2018

- 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

Software Engineer | Ithaca, NY | August 2015 - February 2018

- Cybersecurity R&D for DoD customers and technical proposal writing.
- Wrote winning Phase II SBIR proposal and managed two-year development effort.
- Proposal work lead to nine patents.
- 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

Adjunct Professor | Buffalo, NY | June 2015 - August 2015

- Taught 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

Graduate Teaching Assistant | Syracuse, NY | August 2013 - May 2014

- CIS 252: Introduction to Computer Science (Spring 2014).
  - Graded papers, held 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

Intern & Software Engineer | Syracuse, NY | May 2011 - August 2014

- 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

State University of New York at Buffalo | Buffalo, NY | 2015

- Contributed to published research on adding real-time capabilities to Standard ML, a functional programming language.

Bachelor of Arts | Computer Science

State University of New York at Geneseo | Geneseo, NY | 2013

- Multiple semesters of 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).

Skills

- Languages: C, C++, Rust, Python, Go, Bash. Some experience with RISC-V and X86 assembly. Approximate knowledge of many other languages.
- Version control: Git. Some experience with Mercurial and Perforce.
- Build systems: Bazel, GN, Make. Some experience with CMake.
- Debuggers: GDB and RR.
- Technical writing: DoD proposals and software documentation. Contributed to some IETF specifications.

Patents & Publications

- Daniel McArdle, Judson Powers, Robert A. Joyce (2022-12-06). *Self-healing architecture for resilient computing services* (US-11522904-B2). https://patents.google.com/patent/US11522904B2/en
- Paul Nicotera, Robert Joyce, Judson Powers, Daniel McArdle (2022-03-15). *Systems and methods for used learned representations to determine terrain type* (US-11275940-B1). https://patents.google.com/patent/US11275940B1/en
- Judson Powers, Daniel McArdle, Robert A. Joyce (2018-09-18). *Late-stage software feature reduction tool for security and performance* (US-10078510-B1). https://patents.google.com/patent/US10078510B1/en
- Judson Powers, Robert A. Joyce, Daniel McArdle (2019-05-07). *Application randomization mechanism* (US-10284592-B1). https://patents.google.com/patent/US10284592B1/en
- Judson Powers, Robert A. Joyce, Daniel McArdle (2019-09-10). *Mechanism for concealing application and operation system identity* (US-10412116-B1). https://patents.google.com/patent/US10412116B1/en
- Daniel McArdle, Judson Powers (2021-05-18). *Systems and methods for runtime enforcement of data flow integrity* (US-11010495-B1). https://patents.google.com/patent/US11010495B1/en
- Judson Powers, Robert A. Joyce, Daniel McArdle (2019-02-05). *Evaluating results of multiple virtual machines that use application randomization mechanism* (US-10200401-B1). https://patents.google.com/patent/US10200401B1/en
- Judson Powers, Robert A. Joyce, Daniel McArdle (2019-02-05). *Configuration of application randomization mechanism* (US-10200406-B1). https://patents.google.com/patent/US10200406B1/en
- Judson Powers, Robert A. Joyce, Daniel McArdle (2019-09-10). *Application randomization mechanism* (US-10412114-B1). https://patents.google.com/patent/US10412114B1/en
- Li, Muyuan, Daniel E. McArdle, Jeffrey C. Murphy, Bhargav Shivkumar, and Lukasz Ziarek. "Adding real-time capabilities to a SML compiler." ACM SIGBED Review 13, no. 2 (2016): 8-13.