David E. Mandelberg

david@mandelberg.org
Somerville, MA, United States

Overview

Technical Experience

- Wide range of programming experience in over a dozen languages:
  - Currently proficient with: C++, C, and Python.
  - Formerly proficient with: Java, POSIX make, POSIX shell, SQL, Perl, PHP, Bro Scripting Language, TI BASIC, and WML.
  - Currently familiar with: JavaScript, AWK, m4, LaTeX, and Prolog.
  - Formerly familiar with: Scheme, R, TCL, XSLT, and MATLAB.
- Between reviewing protocol specifications, designing network systems, and writing code, I've gained experience with a range of network protocols, including: Ethernet, IPv4, IPv6, MPLS, GRE, VXLAN, ICMP, ICMPv6, TCP, UDP, BGP, TLS, DNS, SMTP, and HTTP.
- I understand how to deploy and use software engineering tools and best practices:
  - Currently proficient with: Git, Valgrind, and GDB.
  - Formerly proficient with: Buildbot, Autotools, Subversion, SVK, and JUnit.
- I've set up and maintained a variety of servers and other network nodes, from custom network security analysis consoles, to intrusion detection systems, to my own personal email and XMPP/Jabber servers.
  - Operating systems: Linux (Debian, Fedora, and Ubuntu), NetBSD, and Android.
  - Server software: Apache httpd, MySQL, Postfix, Dovecot, ejabberd, Nextcloud, and OpenConnect.
  - Detection and analysis software: Snort, Suricata, Bro Network Security Monitor, Nessus, Netflow, and Samhain/Yule.
  - Other software: iptables, Xen, and Docker.
- Low-level ASN.1 manipulation, OpenSSL's documentation, and NetBSD's kernel code have all failed to faze me.

Security Expertise I can analyze a complex system and figure out how an adversary could compromise the security of the system, then suggest ways to fix or mitigate the problem. In multiple cases, my reviews have led to improvements in protocol specifications before widespread deployment, hopefully leading to an overall more secure Internet when the protocols are deployed. I have been an active member of the Internet Engineering Task Force's (IETF's) security directorate review team since July, 2015.

Mathematics Background My comfort with statistics has helped on numerous occasions, including designing and fine-tuning intrusion detection system components, and presenting data in order to convey a point. Understanding how to apply the fundamentals of abstract algebra and real analysis has come in handy when designing a variety of algorithms. I have a firm grasp of many cryptographic primitives, and enough sense to ask somebody with more experience before attempting to use one in a way I'm not positive it was designed to be used.

Experience

Google Cambridge, MA, United States
Software Engineer August, 2018 – *present*

Self-Employed Somerville, MA, United States
Cyber security consultant, software developer, and more July, 2017 – August, 2018

I decided to try freelancing as something of an experiment. On the more experimental side, I produced two ambient movies and three music albums. The ambient movies were both generated with C++ implementations of mathematical functions. On the more traditional side, I provided software development and technical support services to a livestock farm, and continued to review network protocol specifications for security issues. I also pursued a couple of startup business ideas.

Google Cambridge, MA, United States
Software Engineer June, 2016 – July, 2017

As an early member of the Google Cloud Private Interconnect and Partner Interconnect team, I worked on the design, implementation, and deployment of an enterprise-grade cloud networking feature. Private Interconnect enables cloud customers to privately peer their on-premise networks with their cloud networks at Google's edge. Partner Interconnect enables similar private peering, but with a carrier's network between the customer's edge and Google's edge. I had primary responsibility for the component that coordinates interactions between Google's core cloud systems and network, and the edge network.

BBN Technologies Cambridge, MA, United States
Staff Scientist May, 2010 – April, 2016

At BBN, I worked on a variety of projects for multiple customers. I was the software lead on a project to improve the security of global Internet routing, using the RPKI and BGPsec. As a public face for the project's open source RPKI relying party software, I talked with users and addressed their concerns. I helped write multi-threaded server software, and a comprehensive test suite that found bugs in all public implementations of RPKI relying party software and a couple of bugs in the published RPKI specifications. I attended Internet Engineering Task Force standards meetings, provided valuable reviews on drafts, wrote and co-authored a few drafts, and helped move drafts through the standards process.

On other projects, I developed algorithms to detect anomalies in network traffic, wrote specially-crafted Android apps to help research and development teams write anti-malware software, and set up and debugged custom hardware.

Brandeis University, Library and Technology Services Waltham, MA, United States
Student Information Security Administrator October, 2007 – May, 2010

In Brandeis's information security group, I detected insecure and compromised computers on the network, monitored network usage and investigated anomalies, responded to data breaches, assisted law enforcement, detected exposed confidential personal information, and answered security questions.

Brandeis University, Computer Science Department — Waltham, MA, United States
Teaching Assistant — August, 2008 – December, 2008

At a professor's request, I graded programming assignments and held office hours for Programming in C and Java.

Yankee Flyer — Bloomfield, CT, United States
Computer Administrator — June, 2004 – August, 2004

During a summer in high school, I set up web and email servers, created a backup system, fixed problems on workstations and servers, and tightened security.

Education

Brandeis University — Waltham, MA, United States
Bachelor of Science — August, 2007 – May, 2011

Majors Computer Science and Mathematics
GPA 3.75
Honors and Awards Justice Louis D. Brandeis Full-Tuition Scholarship and Dean's List
Leadership Positions Brandeis Computer Operators Group (president) and Brandeis Contra Dancers (president and founder)

Other

Open Source Contributions

- RPSTIR (professional project): Resource Public Key Infrastructure (RPKI) relying party. I was the software lead for part of my time at BBN Technologies.
- CoHydra (personal project): Python library for managing multi-headed collections of files. I created it to help me manage my music collection across multiple devices.
- Polyball Bounce (personal project): Four player game similar to Pong, but with more players and moving obstacles.
- MusicBrainz Picard plugin for automatic sequence vinyl (personal project): Audio file tagging plugin to make rips of automatic sequence vinyls play in the correct order on a computer.

Music Metadata I've been a member of MusicBrainz, "a community-maintained open source encyclopedia of music information," since 2005. In 2006, I was nominated and elected as an auto-editor, a type of editor with additional privileges.

Uncommon and/or Irrelevant Skills Dog sled packing, constructive solid geometry, sheep hoof clipping, animal videography, jumping in near-freezing water, and typing in multiple Unicode scripts at once.