

David Dahl

ddahl @ crypto dot im

Summary

- Longtime HTML *superfan*, python *nerd*, node.js *enthusiast*, Bitcoin *maximalist*, engineer & researcher

Experience

- F5 <https://f5.com>

- Jun 2020 to present

Senior Software Engineer, VCS Security Team

- F5 Acquired Volterra (VCS) and the Cloud Services teams were reassigned to Volterra & other business units
- Continued development of CI automation tools, concentrating on security and best practices
- Built a set of daily CI pipelines & associated containers that automate adding various security scanning jobs to all VCS/F5 Gitlab projects
- Integrated with GCP, AWS, Azure and other cloud systems as needed to collect and analyse developer, IAM and project data

Senior Software Engineer, F5 Cloud Services

- Gitlab CI/CD meta-programming: automating security, privacy and compliance into the developer experience at F5
- Developed a suite of tools to automate and nudge developer best practices inside Gitlab CI pipelines

- GROVE COLLABORATIVE <https://grove.co>

- Mar 2019 - Jun 2020

Senior Software Engineer, Team Lead

- Helping scale Grove's database, engineering tools, techniques and team
 - (Python, Postgresql, Django, Docker, Redis, AWS, RDS, Heroku)
- Created automated docker-based developer environment
- Integrated fraud-detection services into Grove's core application

- IBM <https://ibm.com>

- Oct 2016 - Mar 2019

Software Engineering Researcher

- Designed and implemented systems to help IBM with internal tools and web standards
- Worked with IPFS decentralized P2P filesystem & related technology
 - IPFS Social Proof : <https://bit.ly/2Pc7GkB>
- Implemented *GDPR* tracking tool which surfaces compliance status for division applications to management
- Created application based on Lighthouse & browser User Timing API to understand and rectify web page performance issues

Advisory Software Engineer

- Built parts of IBM.com & IBM.com/search using Node, SearchKit, TypeScript and React

- SPIDEROAK <https://spideroak.com>

- Sept 2013 - Mar 2016

Director, Crypton project

- Directed an engineering team that built a privacy framework for mobile devices
- Wrote code for the Crypton framework (Node.js, PostgreSQL) <https://bit.ly/2JdzsGW>
- Created *Kloak* private social network application for iOS and Android
- Coordinated Zooko-led (Least Authority, Inc) security review and remediation of Crypton framework

- MOZILLA CORPORATION <https://mozilla.org>

- Jan 2009 to September 2013

Senior Software Engineer, Privacy

- Contributed to new and existing browser features and WebAPIs to increase user privacy
- Collaborated with the Identity team for FirefoxOS
- Implemented DOMCrypt browser extension, which was used as an initial straw man proposal for the W3C Web Cryptography Working Group
 - <https://bit.ly/2JcS0M> <https://mzl.la/2JhUzb2>
- Implemented window.crypto.getRandomValues
 - <https://mzl.la/2JhP0JO> <https://mzl.la/2HkvQRR>

Firefox Engineer

- Created front-end browser features, developer tools, identity APIs
- Implemented the Web Console developer tool
 - <https://mzl.la/2JrzPBg> <https://mzl.la/1IOQVno>
- Wrote code for bookmarking subsystem, awesomebar
- Worked on Firefox SafeBrowsing client code

- **INDUSTRIAL LIGHT + MAGIC** <https://ilm.com>

- Jun 2007 - Dec 2008

Software Engineer

- Re-factored the in-house special effects teaching CMS, LOIS
- LOIS is built in Python, Django, Postgresql and ffmpeg for training artists, software engineers and other technical staff at ILM / Lucasfilm

Skills

- Linux, Python, JavaScript, CSS, HTML, SQL, automated testing
- Node, Express, npm & yarn, webpack, TypeScript, React, Django
- Postgresql (including replication), MySQL, SQLite, Redis
- PhoneGap / Cordova, CouchDB / Cloudant
- Heroku, AWS, Azure, GCP, Gitlab services & APIs, Docker
- C, C++, make, Android toolchain, iOS toolchain, build process
- Raspberry Pi, hardware sensors, etc.
 - <https://github.com/daviddahl/radar>
- Bitcoin, Litecoin, IPFS and related tools / frameworks
- Litecoin mining (2013/ 2014)
- BTC full node operator
- Browser extensions
 - <https://github.com/daviddahl/nuke-dialog>
- Evaluation and recommendations for technology, teams, business processes

Talks / Writing / Teaching

- Defcon 23: Crypto Village: **Anti-social Networking**
 - Presented on K1oak ; an application I built that resembles Twitter but is **end to end encrypted**
 - <https://bit.ly/2JoSNbu>
- Future Insights Live: **Privacy is a UX Problem**
 - Privacy is not simply a technical issue; more designers are needed to solve privacy application issues
 - <https://bit.ly/2Jr80Jd>
- Hack in the Box Malaysia: **Crypton Workshop**
 - <https://bit.ly/2JaB2JC>
 - Live-coding workshop on **Crypton**
- **Crypton Whitepaper**
 - Crypton paper produced for **Hack In The Box** conference
 - <https://bit.ly/2Jbubjg>
- **K1oak Private Social Networking Application: Slides**
 - Produced for **Investors and Management**
 - <https://bit.ly/2sorG6P>
- **Cato Institute: "NSA Surveillance: What We Know; What to Do About It"**
 - Technology panel
 - <https://bit.ly/2xO8IAS>

Referenced Work

- W3C Web Cryptography API Working Group covered <https://amzn.to/2ZfTWXh>
 - **Engineering Rules** *Global Standard Setting since 1880*
 - Joanne Yates and Craig Murphy, 2019
 - Ch. 8, **Development of the W3C WebCrypto API Standard, 2012-2017**

Awards

- 2018 IBM: **Eminence and Excellence in Engineering Award**