

Employment History

| | | |
|---|---|----------------|
| WebSign | <i>Cofounder & CTO</i> | 2022 – Present |
| WebSign is a static website host with end-to-end client-side security (code signing) — websign.app | | |
| PullRequest | <i>Code Reviewer</i> | 2022 – Present |
| I review code in various languages/frameworks, including web/mobile apps, smart contracts, and shell scripts | | |
| PlusMinus | <i>Full-Stack Developer</i> | 2019 |
| Developed applications with an Angular/.NET stack for a Fortune 100 client | | |
| Cyph | <i>Cofounder & CEO / Lead Developer</i> | 2014 – Present |
| Cyph is a user-friendly quantum-resistant end-to-end encrypted messenger — cyph.com | | |
| SpaceX | <i>Software Design Engineer in Test</i> | 2012 – 2013 |
| Built out web UI testing stack for the internal ERP software Warp Drive; rapidly scaled up test coverage with page object code generation and recorder UI, made CI fast with Selenium Grid, and increased utility with a user-facing "macros" app | | |
| Robin Hood Camp | <i>Counselor & Reports Director</i> | 2008 – 2010 |
| Taught chess and Rubik's Cube (my record was 26 seconds); developed simple administrative software in FileMaker Pro | | |

Talks

| | | |
|---|--|------|
| HackerOne Security@ | <i>"Lessons Learned in the Race to Secure Open Source"</i> | 2022 |
| Discussed open source software security topics, the role of organizations, and potential future ecosystem developments | | |
| W3BX | <i>"Building a Secure Bridge from Web2 to Web3 is a Fundamental Infrastructure Investment for the Ecosystem"</i> | 2022 |
| Walked through WebSign and the critical need for it in the crypto/web3 space to enable user-friendly self-custody solutions | | |
| TechCrunch Disrupt | <i>Off-the-record Privacy & Security panel</i> | 2017 |
| Spoke on various privacy and security topics, including predictions on future industry and regulatory developments | | |
| Black Hat & DEF CON | <i>"Abusing Bleeding Edge Web Standards for AppSec Glory"</i> | 2016 |
| Demoed novel web security techniques and the "RansomPKP" attack concept, which ultimately led to the deprecation of HPKP | | |

Projects

| | | |
|--|---|----------------|
| libsodium.js | <i>Co-Author</i> | 2017 – Present |
| Official WebAssembly version of the widely used libsodium cryptographic library | | |
| pqcrypto.js | <i>Author</i> | 2015 – Present |
| Collection of quantum-resistant cryptographic libraries for WebAssembly (primarily NIST PQC selections) | | |
| Napster.fm | <i>Author</i> | 2013 – 2014 |
| Social music streaming application that was featured on TechCrunch and ultimately shut down after an unexpected lawsuit | | |
| Stripe: Capture the Flag | <i>Winner (one of 250, out of 12k participants)</i> | 2012 |
| CTF competition to root a Linux server; vulnerabilities I exploited include buffer overflows, validation failures, and a timing attack | | |

Patents

| | |
|-------------------|---|
| 9,794,070 | Method of ephemeral encrypted communications |
| 9,906,369 | System and method of cryptographically signing web applications |
| 9,948,625 | Encrypted group communication method |
| 9,954,837 | Method of multi-factor authentication during encrypted communications |
| 9,961,056 | Method of deniable encrypted communications |
| 10,003,465 | System and method of encrypting authentication information |
| 10,020,946 | Multi-key encryption method |
| 10,103,891 | Method of generating deniable encrypted communications via password |
| 10,419,223 | Method of using symmetric cryptography for sign-on authentication |
| 10,491,399 | Cryptographic method for secure communications |

Education

| | |
|---|-----------------------|
| MACH37 Cyber Accelerator | 2014 |
| Three-month MBA-style curriculum | |
| Carnegie Mellon University | 2010 – 2012 |
| Planned CS major; dropped out | |
| Certifications | 2009 |
| Microsoft Certified Systems Administrator, et al. | |
| CVEs | |
| CVE-2016-1636 | <i>Severity: High</i> |
| Subresource Integrity bypass in Chrome | |
| CVE-2016-1694 | <i>Severity: Low</i> |
| HTTP Public Key Pinning eviction in Chrome | |