Ryan Lester

hacker@linux.com
+1(337) 935 0016

P.O. Box 3402
McLean, VA 22103

Employment History

Cyph *CEO / Chief Architect / Lead Developer* 2014 – Present

Quantum-resistant encrypted messenger, with dramatically better UX than alternatives (cyph.com)

WebSign
Patented web application code signing technology, architected in collaboration with Cure53

Potassium
Quantum-resistant Sodium-like high-level crypto API

Castle
End-to-end encrypted messaging protocol with automatic always-on public key authentication via air gapped certificates

Account Database Service
High-level client-side real-time database API with automatic signing of public data and encryption of private data

SpaceX *Software Design Engineer in Test* 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 it fast with Selenium Grid, and increased utility with user-facing "macros" app

Talks

Black Hat
Abusing Bleeding Edge Web Standards for AppSec Glory
Covered WebSign and other new techniques to improve user security
Demoed HPKP supercookie and RansomPKP ransomware concept

DEF CON
Second delivery of Abusing Bleeding Edge Web Standards for AppSec Glory

TechCrunch Disrupt
Off-the-record Privacy & Security panel

Georgetown University
Guest lecture on applied cryptography to Professor Hans Engler's class

Education

Carnegie Mellon University *Dropped Out*

CVEs

CVE-2016-1636 *Severity: High*
Subresource Integrity bypass in Chrome

CVE-2016-1694 *Severity: Low*
HTTP Public Key Pinning eviction in Chrome

Open Source Projects

Quantum-resistant cryptography libs *Author*
WebAssembly/asm.js packages of McEliece, NTRU, RLWE, SIDH, and SPHINCS

Napster.fm *Author*
Social music streaming service that was featured on TechCrunch and ultimately shut down after an unexpected lawsuit

libsodium.js *Co-Author*
Official WebAssembly/asm.js package of the Sodium crypto library

emscripten *Contributor*
Developed the `SINGLE_FILE` flag, which has made WebAssembly significantly more practical to adopt for many use cases

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 a deniable encrypted communications via password

Online Presence

AngelList	angel.co/ryanl
Cyph	cyph.me/ryan
Facebook	facebook.com/ryan.h.lester
GitHub	github.com/buu700
HN	news.ycombinator.com/user?id=buu700
LinkedIn	linkedin.com/in/theryanlester
Reddit	reddit.com/u/buu700
Twitter	twitter.com/theryanlester