Mark E. Haase
1455 Spring Vale Ave
McLean, VA 22101

1-202-815-0201
mehaase@gmail.com
https://markhaa.se/

# SOFTWARE & CYBERSECURITY ENGINEER

**Software Engineer • Cloud Engineer • Penetration Tester**

*Goal: Full-time work in cybersecurity research & engineering.*

A detail-oriented problem solver with a passion for security and engineering that goes beyond just a career. Adept at communicating technical subjects to non-technical audiences. Motivated by work that has positive social impact.

## EXPERIENCE

**MITRE, McLean, VA** **2021 – Current**

Lead Offensive Security Engineer

- Software engineer and offensive cybersecurity research for US government sponsors.

**Microsoft, Reston, VA** **2020 – 2021**

Site Reliability Engineer 2

- Lead engineer for redeveloping legacy log scrubbing system, to include cloud-first design and deploying in multiple cloud environments.
- Lead engineer for deploying and debugging internal cybersecurity monitoring tools to USGOV clouds.
- On-call engineer for USGOV clouds, supporting directory services, service auth, security monitoring, and customer escalations.

**Hyperion Gray LLC (Contractor), Concord, NC** **2015 – 2020**
*A small business that works on DARPA R&D contracts and penetration testing.*

Sr. Software Engineer (Full-time Remote)

- Lead engineer on Tor hidden service crawling & scraping application built in Dart, Angular, and Python. Wireframed in 8 weeks and delivered prototype in 24 weeks. Deployed pilots to Dept. of Justice, Homeland Security Investigations, and other law enforcement organizations. Production-ready in less than a year.
- Lead engineer on headless browsing system prototyped in 8 weeks for DARPA with a *de novo* Python implementation of Chrome DevTools Protocol (CDP). Production-ready within 6 months.
- Published Dark Web Map, an interactive visualization of the dark web that received 100k hits and was featured on forbes.com, vice.com, and cnbc.com.
- Developed CAPTCHA solving library that uses OpenCV and Keras to build convolutional neural networks (CNNs) that can solve CAPTCHA tests for some popular software such as WordPress and phpBB. Deployed using TensorFlow Lite models inside AWS Lambda with API Gateway.

Penetration Tester (Full-time Remote)

- Senior penetration tester on multinational law firm engagement and several tech startups for web application and network pen tests.
- Discovered 0-day local privilege escalation (LPE) in Liquidware Labs ProfileUnity and wrote a working proof-of-concept.
- Published proof-of-concept exploits for several vulnerabilities such as CVE-2019-6111/CVE-2019-6110 and CVE-2018-11235.

**Lunarline Inc., Arlington, VA** **2012 – 2014**

*A cybersecurity consulting, training, and products company.*

Director of Product Development

- Launched a new product for Lunarline in the first 3 months of employment.
- Overhauled the software development process, including tools, documentation, mandatory code review, and continuous integration.
- Oversaw project management, engineering, and quality control for 5 proprietary products as well as the corporate website.
- Participated in several penetration tests, including a medical records company and a UAV company. Discovered an exploitable shell injection vulnerability in the UAV software.
- Participated in secure code review for a client, including multiple static analyzers (FindBugs, RATS, and Klocwork) and manual code review.
- Used Peach fuzzer to analyze proprietary routing protocol for a client.

**Hidden Layer LLC, Washington, DC** **2012 – 2012**

*A small business formed to perform advanced research in the field of software verification.*

Co-founder

- Principal author and editor of a DARPA research proposal.
- Wrote a prototype static analyzer using a Naïve Bayes bag-of-words classifier and various n-grams and smoothing techniques, achieving recall rates over 80%.
- Administrative POC, project manager, and technical writer for the 4-month research project, meeting all milestones in the statement of work and receiving positive reviews from our DARPA sponsor.

**Endeavor Systems Inc., McLean, VA** **2008 – 2012**

*A boutique consulting firm specializing in federal government cybersecurity and compliance.*

Software Team Lead

- Grew revenues from $50k to $500k on flagship product over 3 years.
- Overhauled the software development process, including tools, documentation, mandatory code review, and continuous integration.
- Created a comprehensive hiring process for screening and interviewing software engineers.

**Hewlett-Packard Company, Washington, DC** **2006 – 2008**

Business Intelligence Consultant

- Designed and implemented extract-transform-load (ETL) applications for interfacing modern platforms to legacy systems at Fannie Mae using Ab Initio and Oracle PL/SQL.

## OPEN SOURCE

**Agnostic Database Migrations (★45):** A tool for managing database migrations. Supports Postgres, MySQL, and SQLite.

**Chrome DevTools Protocol (★33) / Trio Chrome DevTools Protocol (★30):** A stack designed for driving headless Chrome using the Chrome DevTools Protocol (CDP). The first layer (PyCDP) uses code generation to produce native Python wrappers from the machine-readable CDP specification. The second layer (Trio CDP) adds I/O using the Trio asynchronous framework and adds support for multiplexing and other high-level functionality.

**Encoding Tools (★7):** A tool for generic byte string manipulations, similar to Burp Suite Encoder or GCHQ CyberChef. Online version available at https://encoding.tools.

**Page Compare (★68):** A simple heuristic for comparing the structural similarity of two HTML documents. This algorithm was also used for the clustering step in the construction of the Dark Web Map.

**Starbelly (★33):** A GUI-driven web crawler written on top of the Trio asynchronous framework. The crawler uses a novel "crawl policy" system to simplify the configuration of directed crawlers.

**Trio WebSocket (★51):** An implementation of the WebSocket protocol on top of the Trio asynchronous framework. This library is used in Starbelly, Trio CDP, and internal Hyperion Gray projects.

## PUBLIC SPEAKING

### Dark Web Investigations (2017-2018)

*NW Regional ICAC Conference, and National LE Training on Child Exploitation.*

- A 90-minute dark web primer for law enforcement professionals who specialize in counter-child-exploitation.
- Discussion of dark web technologies Freenet, I2P, and Tor, and the ramifications for traditional digital crime investigative techniques.
- Hands-on labs for officers to gain first-hand experience with dark web tools and OSINT methods.

### Securing Web Applications (2014-2015)

*Peterson AFB, Scott AFB, Dept. of Transportation*

- Developed and presented this class in both 1-day and 4-day formats covering web application vulnerabilities and exploitation, including lecture, slides, hands-on labs, and assessment.

### Web Technologies & Security (1 Day)

*NASA Goddard Space Flight Center*

- Developed and presented this 1-day course covering basic web technologies, the OWASP Top 10, and how to mitigate security vulnerabilities through the software development lifecycle.

**NYU-Poly THREADS (2013)**
*A Machine Learning Approach to Software Vulnerability Detection.*

- Presented details of DARPA research, including background and overview of natural language processing (NLP) and machine learning (ML) classifiers used.
- Presented quantitative results of our research including explanation of the metric used including *precision*, *recall,* and *F-score*.

**AppSec USA (2012)**
*Reverse Engineering "Secure" SSL APIs*

- Conducted an educational overview of SSL/TLS and how it should be used when building a web API.
- Constructed proof-of-concept iOS game and "secure" high score server to demonstrate weaknesses and possible mitigations.

## EDUCATION

**University of Pennsylvania (2005)**

- B.A. with Distinction in Philosophy, Politics & Economics.
- Minor in Computer Science & Engineering (30 hours in computer science, math, and statistics).
- Honors Thesis titled *A Survey In Network Economics*

## CERTIFICATIONS & OTHER INFO

- **OSCP (current):** Offensive Security Certified Professional. 2016. Put in 200 hours of lab work and exploited 46 lab machines. The final exam is a hands-on penetration test.
- **CEH (lapsed):** Certified Ethical Hacker. 2013.
- **CISSP (lapsed):** Certified Information Systems Security Professional. 2012.
- 23k reputation on Stack Overflow.
- Discovered CVE-2019-2413, a reflected XSS in Oracle Reports.
- Contributed 10 reverse engineering challenge problems for PicoCTF 2019.
- Drafted Python enhancement proposal PEP-505 to include null-coalescing operators in the language.
- Gathered all 50 stars on the 2018 Advent of Code.
- Published cybersecurity and dark web articles on my personal blog: https://markhaa.se