Paul Halvorsen

Sr Software Developer
Email: paul.halvorsen@pm.me
Phone: +1-410-236-4665
Last Updated: March 6, 2026

Personal Blog: https://flow.halvo.me
LinkedIn: www.linkedin.com/in/paul-halvorsen
Git Repo: https://git.halvo.me/paul
Citizen of the United States

Summary

I'm a Software Engineer with over 14 years development and 18 years professional experience, with exposure to Rust, C, Python, PHP, Go, JavaScript, Java, and C++ languages; various SQL DBs; tokio, JQuery, and Pytest frameworks; Docker and GitLab CI/CD; and Rest API, NATS, JSON, XML, and nginx technologies.

Work Experience

Binary Defense

Sr Software Engineer: April 2022 - Oct 2025

- Rust development including: tokio (test), reqwest, anyhow, serde, windows, cargo, cmake, and WIX
- Python development using pyenv, pipenv, cython, docker, GitLab pipelines, and static compilation
- Develop security alarms for Windows, Linux (Debian and RedHat), and MacOS: Event driven by Windows Events, file and directory updates, and network connections
- Written RFC and ADR to drive design and decision making on project direction
- Design and build encrypted SQLite DB (configuration and cache), network containment, and secure key exchange and authentication
- Design and build HTTP and NATS Rest API for receiving configuration (JSON) and sending data to backend servers and Microsoft Azure
- Aid in distributed deployment to dozens of customers with hundreds of endpoints

Kyrus Tech

Sr Software Engineer: Nov 2020 - April 2022

- Perform test driven development: C, Python/Pytest, Docker, GitLab CI/CD, Ghidra
- Build covert communications and file transfers proxy: HTTPS, Apache Thrift, Rest API
- Design compact router fingerprinting and vulnerability analysis: Android, TCP/IP, StreamCypher
- Modify C code to suppress system logging in various Linux Kernel versions

Parsons

Cyber Security Software Engineer: Apr 2018 - Nov 2020

- Develop covert Windows application: C, C++, Python
  - Build modular solution for plugin architecture and distributed deployment
  - Design custom API for minimal communications on limited bandwidth
  - Encrypt storage and comms using AES shared key to maintain confidentiality and integrity
- Build back-end service for file storage and search: Java, Tomcat, NiagaraFiles (NiFi), nginx, Hadoop, MySQL, LDAP, RBAC
  - Create API for uploading files via web interface or CLI
  - Generate metadata for searching

NSA

Security Software Engineer: Nov 2011 - Apr 2018

- RedTeam DevOps development of browser enumeration, manipulation, and exploitation: PHP, JavaScript, JQuery, CSS, Python, MySQL, Java, Apache, Tomcat, Linux, Windows, Chrome, Firefox, Safari, IE, Edge
  - Design Rest and JSON API to transfer data between targets, server, and UI
  - Distribute covert JavaScript to targets across US government networks for enumeration and exploitation
  - Design front-end to provide a dynamic UI with real time target data, graphs, and charts
  - Design MySQL database to hold and quickly query enumeration and exploitation data
- Advise and develop vulnerability mitigation strategies for various military and government customers
- Train and provide SOPs to NSA RedTeam operators for various tools

Systems Engineer: Sept 2009 - Nov 2011

- Deploy, maintain, and monitor 30+ systems with 130+ Red Hat Enterprise Linux (RHEL) servers: LDAP, DNS, Apache, NiFi, Hadoop, Apache, Puppet, DHCP, PXE
- Develop and deploy monitoring, reporting, and issue correcting scripts: Python
- Organize, train, and participate in team performing 24x7 call-in rotation
- Responsible for 5+ domestic and foreign system deployments

Salisbury University

Software Developer: Nov 2006 - May 2008

- Funded through the Wallops Flight Facility (NASA)
- Provide simplified UI and scenario builder for the Satellite Tool Kit (STK): Managed C++
- Design risk assessment scenarios for launch vehicles and UAVs over the DELMARVA peninsula
- Collaborate with Geographic Information Science (GIS) for mapping

Lab Administrator: Sept 2007 - May 2009

- Support Math and CS departments at SU
- Maintain the Linux labs on campus: dual boot OpenSUSE, WindowsXP, and OpenSUSE server
- Perform backups, updates, user management (LDAP), disk quotas, and remote access

Education

- **University of Maryland Baltimore Campus**: Masters in Computer Science; 2013. Thesis: "Stateless Detection of Malicious Traffic: Emphasis on User Privacy"
- **Salisbury University**: Bachelors in Computer Science, Minor in Math; 2009. Magna Cum-Laude
- **Security+** (Expired): ID: COMP001021281239; Exp Date: 04/04/2024
- **Royal Military College (RMC Canada)**: Training in OpenBSD development and administration

Miscellaneous

- **RedBlue Conference**: Presented combination web enumeration/exploitation tool
- **National Conference for Undergrad Research (NCUR)**: Presented development of STK scenario building and manipulation
- **SANS Courses**: Staying up-to-date on security research
- **Homelab**: Proxmox running test VMs, email, cloud storage, gitea, DNS, multimedia, genealogy, and static web pages
- **Web Admin for PTA**: Setup and maintain WordPress pages, calendar, and blog