About Me

General Info

- Name: Paul Halvorsen
- Contact
  - Email: paul.halvorsen@pm.me
  - Phone: +1-410-236-4665
- Links
  - Personal Blog: https://flow.halvo.me
  - Git Repo: https://git.halvo.me/paul
  - LinkedIn: https://www.linkedin.com/in/paul-halvorsen
- Citizen of the United Stats
- Security Clearance
  - Expired TS/SCI

Summary

I'm a Software Engineer with over 15 years of development and 20 years of professional experience, with expertise in Rust, C, Python, and GoLang; various SQL databases; tokio, Pytest, and Docker frameworks; GitLab CI/CD pipelines; and REST APIs, encryption, JSON, and nginx technologies. Specialized in backend development, systems programming, and security-focused applications.

Keywords

rust, cargo, python, c, docker, containers, TDD, test driven development, pytest, CI/CD, JavaScript, JQuery, PHP, MySQL, rest, API, JSON, XML, git, GitLab, nginx, remote, testing

Experience Levels

- Advanced
  - Rust, Cargo, Python, PyTest, GoLang, MySQL, C
- Intermediate
  - JavaScript, PHP, GoLang, JQuery
- Beginner
  - Java, C++,

- Intermediate
  - Linux, Debian, Ubuntu, RHEL, CentOS
- Beginner
  - Windows, MacOS, OpenSUSE, Android, iOS

- Intermediate
  - Firefox, Chrome
- Beginner
  - IE, Edge, Safari

- Intermediate
  - MySQL, REST API, JSON, Nginx, Encryption, RSA, Docker, CI/CD
- Beginner
  - Tomcat, Apache, DNS, k8s, AWS, Azure, Ghidra, k8s, Kubernetes

Specialities and Target Positions

- Application development
- Backend development
- Security/Cybersecurity
- Systems programming

Target wants in a position

- Remote work environment
- No on-call
- Flexible minimum of $135000

Work Experience

Abnormal AI

Software Engineer: Jan 2026 - Present

- Utilize claude AI, summarize code, aid in coding, planning
- Build and maintain k8s and AWS infrastructure
  - python
  - pacman
  - haml
  - yaml
  - 10 k8s clusters, with auto scale up and down number of instances
- Build and maintain service to aggregate data

  - golang, python
  - pytest, unit testing
- running cron jobs in k8s
- using kubectl, k9s to control k8s
- RBAC
- Team of 5
- Heavy inter-team communication and coordination
- Monorepo with all teams
- Customers in US East, US West, EU West, and government

  - Maintain real time storage and long time storage
  - Generate aggregated data
  - Increase efficiency through auto-scaling, and compression
- 24x7 call

Binary Defense

Sr Software Engineer: April 2022 - Oct 2025

- Gitlab

  - CI/CD pipelines for unit and integration testing, compilation, and deployment
  - docker images for Linux, Windows
  - VMs for MacOS
  - MR/PR contributions, comments and testing
- Rust development

  - cargo, nextest, cmake, WIX, cross compilation, unit tests
  - sqlite encrypted db
  - libraries: tokio, reqwest, anyhow, serde
  - Containment
  - Azure Library
  - Library to watch for windows event logs, file system changes, user changes, and firewall changes

    - White and blacklists for files, file types, file contents, and hashes
    - Sanatize, decorate (add additional data), serialize data for transfer to backend
    - De-duplicate data to reduce network traffic and backend storage costs
    - Event driven
  - Unit tests
  - Public key pinning and certificate transparency
  - Secure key storage

    - Encrypting and decrypting on disk sqlite db
    - dpapi for Windows
    - org.freedesktop.secrets for Linux
- Python development

  - pyenv, pipenv, cython, docker build environment, static compilation, pytest
  - Containment
  - Public key pinning and certificat transparency logs
  - end-to-end integration testing

    - Spin up pre-configured VMs (Windows and Linux)
    - Make specific testing changes to those VMs via ssh
    - Spin up temporary servers
    - Run tests
  - Performance improvements

    - Reduce CPU usage by filtering out previously observed issues ~ %90
    - Reduce memory usage by using regex and filtering ~ %60
    - Reduce network traffic using regex and filtering ~ %80
    - Reduce disk size by turning multiple strings into regex ~ %20
  - Libraries for watching network traffic on Windows and Linux

    - Event driven
    - White and blacklists in regex
  - Specific Windows events
  - Filesystem changes
  - User changes
  - Event driven
- Supported OSes

  - Windows

    - Server 2009, 2012, 2019
    - xp, 7, 8, 10, 11
  - Linux

    - Debian, Ubuntu
    - Redhat, CentOS
  - MacOS
- Written RFC and ADR to drive design and decision making on project direction
- Containment

  - Design and build containment for all platforms upon detected compromise
  - Containment meaning no network access other than to BD servers
  - Use Linux iptables, windows firewall, and MacOS ip firewall
- Design and build secure key exchange and connections
- Public key pinning and certificate transparency logs

  - For server verification
  - Prevent MITM attacks
- Azure Library

  - Setup library for communication: rust and python
  - Perform API calls for uploading and updating data in database
  - Setup database when it doesn't exist
- Testing performed using VMs built in Proxmox and Virtualbox
- SCRUM
- Customers

  - Small to large (Fortune 500 companies)
  - Thousands of endpoints

Kyrus Tech

Sr Software Engineer: Nov 2020 - April 2022

- Router Fingerprinting
  - C and Python
  - Run on Android phone
  - Compact and rolling logs
  - Aggregated logs
  - Scan for connected routers
  - Perform fingerprinting and vulnerability analysis on device
  - HTTPS, TCP/IP, StreamCypher Encryption, ICMP, DNS
- Covert communications
  - C, Python, Docker
  - HTTPS, Apache Thrift, REST API
  - Multi threaded
  - Routing through multiple middle
  - C front end, and middle, python backend
  - Encrypted transfers
  - RSA key exchange
- Linux kernel backdoor
  - Supress system logging
  - Monitor filesystem changes
  - Supress system monitoring
  - Support for various Linux Kernel versions
  - Ghidra, C
- Test driven development
- C, Python, Pytest, Docker, GitLab CI/CD
- SCRUM

Parsons

Cyber Security Software Engineer: Apr 2018 - Nov 2020

- Covert Windows Application
  - Library injection
  - C, C++, Python
  - Modular solution for dynamic and static plugins
  - Cluster of nodes
  - Custom API and serialization
    - Extremely limited network traffic
    - Reduce size of data transfer
    - Aggregate/Consolodate data from multiple nodes
  - Reverse engineer target's custom data storage to parse and manipulate target data
  - Reverse engineer API calls to proprietary application

    - Manipulate lagitimate traffic
    - Inject traffic
  - Encrypt local storage and comms using shared AES key
- Back-end service for file storage

  - Java, Tomcat, Niagarafiles (NiFi), nginx, hadoop, MySQL, LDAP, RBAC
  - API for uploading files

    - Web interface
    - CLI
  - Remove duplication before storage

    - Allow reads from multiple users uploading the same file
    - Create new file on write
  - Multi-level user access, RBAC and LDAP
  - Produce metadata

    - Provide search functionality

NSA

Security Software Engineer: Nov 2011 - Apr 2018

- RedTeam DevOps
- Browser security

  - enumeration, manipulation, exploitation
  - Languages: PHP, JavaScript, JQuery, CSS, Python, MySQL, Java
  - Platforms: Tomcat, Apache, Nginx
  - OS: Linux, Windows, Android, iOS
  - Browsers: Chrome, Firefox, Safari, IE, Edge
  - Rest JSON API for data transfer to and from target and backend server
  - Recon from browser

    - Browser name, type, version
    - OS name, type, version
    - Possible device make and model
    - Plugins in browser and versions
  - Design dynamic browser UI using JQuery

    - View all data on all connected targets
    - Interact with the targets browsers

      - Change the look
      - Monitor key presses and mouse movements
      - Mimic legitimate sites
      - Redirect the page
    - View stats on currently and past connected targets

      - Query CVEs to view possible exploits
      - Number of versions seen
      - Plugins seen

    - Add more as needed by operator
  - Send exploits to target with backdoor payload
- Build browser exploits using CVE and POC (half day and full day vulnerabilities)
- Obfuscate

  - PHP and JS obfuscation
  - Randomly change the JS and PHP to hide and evade detection
- Design and maintain MySQL database

  - Hold data on each browser, os, and possible exploits
  - Hold and relate data for CVEs and available exploits
  - Reduce redundancy
  - Increase efficiency with pre-compiled queries and indexes
- Maintain backend server
- Additional projects as needed

  - Java Tomcat web backdoor
  - ASP.Net web backdoor
  - ASP.Net document backdoor
  - Run JS inside documents and PDFs
  - Re-work windows backdoor to cross compile on MacOS
- Provide feedback

  - Train and provide SOPs to NSA RT operators for various tools
  - Produce documentation for new developers
  - Train new developers
  - Advise and develop vulnerability mitigation strategies for various military and government customers
- Aid in scoring the NSA Cyber Defense Challenge

  - Build token scoring system
  - Keep track of scores and provide feedback to the teams
  - Report scoring throughout the competition
- Customers

  - Military branches
  - DoD
  - DoJ
  - Other government departments

NSA

Systems Engineer: Sept 2009 - Nov 2011

- Ownership over 30+ systems with 130+ RHEL servers each

  - Stage 10+ systems
  - Deploy 3+ systems, domestic and foreign
  - Soley responsible for 5+ domestic and forign systems
  - Maintain all systems as part of a 24x7 call-in rotation
- Multiple services on each system

  - LDAP, DNS, Apache, NiFi, Hadoop, Puppet, DHCP, PXE boot

- Develop scripts to aid in maintenance
  - Python
  - Auto fix known issues
  - Scan and produce report of all systems in under 30 min
  - Report sent via Web API to Web UI and alerting system
  - Reduced call-ins
- Organize and train team of contractors
  - Trained up and informally supervised team of 5
  - Spun up to work 24x7
  - Provide SOPs for quick fixes
  - Provide SOPs for tier 1 to reduce call-ins for 24x7 team

Salisbury University

Software Developer: Nov 2006 - May 2008

- Funded through the Wallops Flight Facility (NASA)
  - Tasked to provide risk assessments
  - Launch vehicles and UAVs over the DELMARVA peninsula
- Provide simplified UI and scenario builder for the Satellite Tool Kit (STK)
  - Wizard walk through for standard set of launch and safety scenarios
  - Build scenario in both custom simplified UI as well as full STK
- C++, UI built using Visual Studio and Managed C++
- Provide reports on risks of scenarios
  - Realtime graphs and charts
  - Post analysis reporting
- Create graphs designed to display risk throughout the scenario
- Design risk assessment scenarios for launch vehicles and UAVs over the DELMARVA peninsula
- Collaborate with Geographic Information Science (GIS)
  - Provide maps with POI
  - Distances and response times for emergancy vehicles

Salisbury University

Lab Administrator: Sept 2007 - May 2009

- Support Math and CS departments at SU
- Maintain the Linux labs on campus
  - In charge of 2 labs
  - Dual boot OpenSUSE, WindowsXP
  - OpenSUSE server
- Provide SSH access both internal and external
- Perform regular tasking

  - Backups
  - Updates
  - User management (LDAP)
  - Disk quotas
  - Remote access
  - Installation of needed software
- Monitor the labs while in use

Education

- University of Maryland Baltimore Campus
  - Masters in Computer Science
  - Graduated 2013
  - Thesis: “Stateless Detection of Malicious Traffic: Emphasis on User Privacy”
- Salisbury University
  - Bachelors in Computer Science
  - Graduated 2009
  - Magna Cum-Laude
- Security+
  - 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
- Blog: https://flow.halvo.me
- Git: https://git.halvo.me/paul
- Homelab
  - Proxmox
  - Running email
  - Cloud storage, TrueNAS, Nextcloud
  - gitea

  - DNS, pi-hole, adguard
  - Multimedia, Plex, Jellyfin
  - Geneology, Webtrees
  - Static web page services, docs, hugo, blogs, dashboard
  - Home assistant
- Web Admin for PTA

  - Setup and maintain a Wordpress site
  - Setup and maintain weebly site