# Paul Halvorsen

Phone: +1-410-236-4665
Email: pmghalvorsen@gmail.com
Citizen of the United States
Holding TS/SCI, Last Re-Up: 2018

## Summary

I'm a Software Engineer with over 11 years development and 15 years professional experience, with exposure to C, Python, PHP, Go, JavaScript, Java, and C++ languages; various SQL databases; JQuery and Pytest frameworks; Docker containerization; and Rest API, JSON, XML, and nginx technologies.

## Work Experience

### Binary Defense

**Sr Software Engineer**: April 2022 - Present

- Python development using pyenv, pipenv, cython, docker build environment, gitlab pipelines, and static compilation
- Develop security alarms for Windows, Linux (Debian and RedHat), and MacOS
- Written RFC and ADR to drive design and decision making on project direction
- Design and build containment for all platforms upon detected compromise
- Design and build secure key exchange and connections

### Kyrus Tech

**Sr Software Engineer**: Nov 2020 - April 2022

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

### Parsons

**Cyber Security Software Engineer**: Apr 2018 - Nov 2020

- Continue development of covert Windows application: C, C++, Python
  - Build modular solution for plugin architecture
  - Design custom API for minimal data transfer to back-end
  - Encrypt storage and comms using AES shared key to maintain confidentiality and integrity
- Build prototype 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
  - Track and maintain multi-level user access
  - 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
  - Deliver covert JavaScript to targets for enumeration and exploitation
  - Design front-end to provide a dynamic UI with real time target data and graphs and charts for in-depth data
  - Design MySQL database to hold and quickly query enumeration and exploitation data
  - Update PHP back-end for security and performance
- 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; 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