JONATHAN DEFREEUW

(757) 619 - 5687 ⋄ defreeuw@vt.edu
https://jonathandefreeuw.com
Active DoD TS/SCI Security Clearance

EDUCATION

Virginia Tech August 2016 - December 2018
M.S., Computer Engineering **Overall GPA**: 3.61/4.0
Thesis: *Embedding Network Information for Machine Learning-based Intrusion Detection*

Virginia Tech August 2013 - May 2017
B.S., Computer Engineering - Magna Cum Laude **Overall GPA**: 3.60/4.0
Minors in Cybersecurity, Computer Science, and Mathematics

WORK EXPERIENCE

U.S. Naval Research Laboratory June 2017 - Present
Computer Engineer *Washington, D.C.*

- Develop and administer automated malware analysis platform to support Navy network operations, including frontend, backend, database management, and DevSecOps pipeline
- Explore machine learning techniques for analyzing malware and related artifacts to provide orthogonal methods of detecting malicious behavior in suspicious files
- Investigate threat model of 5G network interfaces and service-based architecture by analyzing 3GPP specifications and testing interface implementations in open-source 5G cores
- Principal investigator of R&D projects totaling >$1M of funding, utilizing agile workflows to lead two projects of three to five developers and researchers

Information Technology and Security Lab May 2016 - August 2016
Undergraduate Researcher *Virginia Tech, Blacksburg, VA*

- Automated mobile network traffic generation using Android devices and a RESTful application backend
- Supported lab research through deployment of Guacamole remote access gateway
- Configured and managed lab infrastructure, including network and hardware

TECHNICAL STRENGTHS

Languages & Frameworks	Python, Javascript, CSS, Django, Flask, Celery, jQuery, Bootstrap
Data Management Systems	Cassandra, PostgreSQL, Redis, MinIO, Elasticsearch
DevOps Technologies	Docker, Kubernetes, GitLab CI/CD, Jenkins, Ansible
5G Systems	Free5GC, Open5GS, UERANSIM, SCTP, NGAP/NAS
Other Tools	Cuckoo Sandbox, Zeek, OpenFlow, OpenVSwitch

PROJECT EXPERIENCE

Securing 5G Service-Based Architecture Using Cilium *in progress*

- Extract producer-consumer relationships between network functions in a 3GPP-compliant core using OpenAPI files and rich-text documents
- Generate a set of CiliumNetworkPolicy objects to enforce API specifications in Kubernetes
- Automate pipeline to generate security profiles for new network functions or update existing profiles as specifications are updated

Cloud Resume Challenge *in progress*

- Develop a static website using Hugo to deploy in AWS using S3, CloudFront, and Route53, with a visitor counter using DynamoDB and Lambda
- Automate updates to the website using Terraform and GitHub Actions to push new files, create new AWS resources, and invalidate caching
- Progress can be viewed at *https://jonathandefreeuw.com*

Home Raspberry Pi Cluster

- Operating a 6-node Raspberry Pi cluster as a testbed for practicing container technologies at home
- Deployed 3-master, 3-worker Kubernetes cluster using K3s
- Enabled PXE Boot on Raspberry Pis using pfSense and TrueNAS SCALE for reliable storage and backups
- Run containers for at-home services such as Pihole, Omada Controller, and BookStack

Brute Force Defense Using OpenFlow on Raspberry Pi

- Prototyped a software-defined network on a cluster of Raspberry Pis and designed a threshold-based IPS
- Used a POX controller and OpenVSwitch to perform rate-limiting to protect Internet-connected camera
- Performed brute force login attempt using Hydra as a proof-of-concept attack

VOLUNTEER EFFORTS

Transit Church September 2020 - Present
Media Director

- Lead and train a team of volunteers in audio mixing and video presentation for weekly services
- Integrate new technologies to simplify and improve processes at the church
- Operate church website and social media for livestreams, podcasts, and announcements