Ryan Van Antwerp, Ph.D.

Full Stack Developer · Security SRE

rvanantwerp AT gmail.com | drvan | https://scholar.google.com/citations?user=zRGxukkAAAAJ

Summary

Senior Principal Security Engineer at Comcast with 8+ years experience specializing in full stack software development and security solution engineering. Designed and lead team development on multiple large scale, cost saving, enterprise-wide projects, including infrastructure deployments that support Comcast's entire enterprise security footprint. Defined standards for team code contributions, code reviews, technology stack and programming language choices to continuously produce high quality and robust applications. Considered a subject matter expert in Apache Kafka, API development using Node.js, public key certificates, as well as security log ingestion and analysis. Lead multiple teams and mentored engineers in following software engineering best practices and architecting reliable code and infrastructure. Regularly developed security related patent applications, reviewed and accepted by Comcast's technical committee and invention disclosure team. Interested in leading teams to solve challenging large-scale problems using modern technology and innovative solutions.

Skills

Back end	Node.js, Express, NestJS, REST API Development, Apache Kafka, PostgreSQL, MySQL
Front end	HTML5/CSS/JS, Angular, jQuery, PHP, Bulma, Semantic UI, Pug, Jinja2
Programming	TypeScript, JavaScript, Python, Java, Go, LaTeX
Security	Reverse Engineering (radare2, gdb), Exploitation (pwntools, peda)
Infrastructure	Ansible, AWS, GCP, Docker, Vagrant, Concourse CI, Prometheus, Grafana
Data Science	Tensorflow/Keras, Logstash, Elasticsearch, Apache Spark

Work Experience

Comcast, Comcast Cybersecurity — *Remote*

Senior Principal Security Engineer — *Mar. 2022 - Present*

- Led a team to design and implement a full stack application consisting of a secure API, web front end, and a machine learning model back end to assist in asset owner discovery for auditing and security purposes.
- Reduced Comcast's enterprise attack surface by identifying 35% of previously unknown asset owners to facilitate vulnerability remediation.

Comcast, Comcast Cybersecurity — *Remote*

Principal Security Engineer — *Mar. 2017 - Present*

- Led design, architecture, and implementation of Comcast's enterprise security log aggregation platform, using Apache Kafka. Responsibilities included architecting ingress and egress points, load management, connecting to a variety of technology stacks to both source and sink sensitive security data.
- Defined processes for automated operations, patching, and deployment across our team using Ansible and Docker.
- Designed and developed Comcast's internal certificate management platform using Node.js, Express, TypeScript and Pug. The platform allows Comcast employees to request, revoke, and renew PKI certificates with multiple back end certificate authorities.
- Lead development on Comcast's DDoS protection-as-a-service platform, a large scale revenue-generating project, using NestJS and Angular to develop a full stack application that allows enrollment and management of business customers utilizing the service.

ReturnLogic — *Remote*

Infrastructure Consultant — *Jun. 2020 - Oct. 2021*

- Designed infrastructure automation plan and bootstrapped team with documentation and tools to rebuild and scale critical services.
- Introduced local infrastructure automation testing frameworks for rapid development of repeatable immutable deployments.

University of Delaware, Electrical and Computer Engineering — *Newark, DE*

Adjunct Assistant Professor — *Aug. 2015 - Present*

- Taught each fall semester of CPEG471/671 Pen Testing and Reverse Engineering, both face-to-face and online as part of University of Delaware's Cybersecurity master's degree program.
- Topics have included reverse engineering compiled binaries, exploitation, shellcode, and return-oriented programming.
- Developed a curriculum that uses a combination of Docker, Google Cloud Platform, and Vagrant to setup a lab environment for assignments.

Comcast, Customer Protection — *Philadelphia, PA*

Senior Internet Systems Engineer — *Nov. 2014 - Mar. 2017*

- Architected a solution to centralize threat intelligence data from multiple external sources into a searchable information store for analyzing botnet trends and promoting remediation across Comcast's residential network.
- Developed ingestion software to reliably import critical threat intelligence data for use in customer remediation notifications, reducing network utilization consumed by malicious botnet traffic.
- Automated architecture deployment and monitoring using Puppet and Sensu.
- Organized and distributed work among a small team, introducing and adopting Agile methodologies (Scrum and Kanban).

Comcast, Customer Protection

Philadelphia, PA

Internet Systems Engineer

Jun. 2013 - Nov. 2014

- Contributed to initiatives to better protect Comcast's 20+ million residential subscribers.
- Monitored and managed a combination of more than 100 physical and virtual machines, including automation, security patching, software upgrades, and performance tuning.
- Analyzed botnet and malware trends across residential high speed internet customers and formulated strategies to notify and remediate infected subscribers.

Patents

User Identification System and Method for Fraud Detection

Patent #11200336

Filed Dec. 2018 | Granted Dec. 2021

- Using authorship attribution techniques, identify whether a participant in a text-based chat is imitating a user in order to commit fraud. Users are asked a series of innocuous questions where their answers are analyzed using natural language processing techniques. These attributes are used to train a machine learning model that will identify whether future text-based initiated chats are authored by the user or are being imitated by a third party to commit fraud.

Methods and Systems to Detect Rogue Hotspots

Patent #10911956

Filed Nov. 2017 | Granted Feb. 2021

- Method of identifying a rogue hotspot (a device imitating a legitimate hotspot) through the use of signal strength readings among known good devices. Deployed access points will continually probe nearby networks and report signal strength metrics back to an analysis engine to identify the arrival of new rogue hotspots imitating known good hotspots.

Process For Identifying A Compromised Device

Pending Patent Application #20160226898

Filed Jan. 2015

- Method of identifying an infected device behind a NAT layer using DNS caching on client devices. DNS caches are examined and correlated with external threat intelligence data captured from botnet activity to identify the specific infected device within a network.

Education

University of Delaware

Newark, DE

Ph.D. in Electrical and Computer Engineering

May 2011 - May 2013

- Concentration in penetration testing, exploitation, malware analysis, and reverse engineering.
- Dissertation titled "Using the Presence of Anti-Reverse-Engineering Artifacts to Detect Malware"

University of Delaware

Newark, DE

M.S. in Electrical and Computer Engineering

Aug. 2009 - May 2011

- Concentration in botnet analysis and exfiltration.
- Thesis titled "Exfiltration Techniques: An Examination and Emulation"

The College of New Jersey

Ewing, NJ

B.S. in Computer Engineering

Aug. 2005 - May 2009

- Graduated with the Fred O. Armstrong Award: Highest GPA among TCNJ Computer Engineering graduates for the class of 2009.