Apoorv Dayal

apoorvdayal@outlook.com | (650) 495 9943 | Seattle, WA
linkedin.com/in/apoorvdayal | Github.com/Apoorv13

Professional Experience

Microsoft — Redmond, WA
Security Software Engineer II — Apr'21 - Current

- Conducted extensive security reviews for over 20+ Azure offerings discovering over 100+ security vulnerabilities engaging multiple service teams.
- Developed partnerships with over 5+ service teams, both internal and external (Azure Data, Databricks), including multiple rounds of architecture and design reviews along with Threat modelling reviews.
- Developed pentest tools from ideation to product delivery stage, currently in use by over 150+ customers, handling 4M+ requests, creating infrastructure and features.
- Performed research on containers and container orchestration platform security creating guidelines and automated tools to detect misconfigurations directly impacting over 10 Azure core services and over millions of customers.
- Actively supported incident response efforts by performing variant hunt on reported cloud critical bugs across multiple Azure products, suggesting and validating potential fixes to service teams.

Ernst & Young India LLP — Mumbai, India
Senior Cybersecurity Analyst — June '17 - July '19

- Slashed the average turn-around time required for static analysis security testing (SAST) of mobile applications based on OWASP Mobile Top 10 by 40% at various fortune 500 clients.
- Secured 500+ web and mobile applications, complex payment systems, delivery networks and warehouse controls including IOT devices for retail operations through penetration testing exercises.
- Developed tools & internal frameworks for web/mobile applications security based on OWASP top 10.
- Conducted workshops and seminars on awareness and coding best practices at multiple venues.

Internships & Academic Experience

Mandiant (FireEye) — Remote / Reston, VA
Technical Threat Intelligence Analyst Intern — May '20 – Aug '20

- Triaged nation-state malware as a part of the Cyber Espionage team in intelligence services using static and dynamic malware analysis techniques with tools such as IDA, Ghidra, Ollydbg and Wireshark.
- Modeled threat intelligence based on attacker attribution and malware analysis while working with the most senior technical reverse engineers on analysis / reverse engineering tasks, collaborating with other technical and threat analysts on joint intelligence reporting.
- Created automation framework for Malware Analysis leveraging OSINT resources and FE's internal sources for ease of analysis for Analyst's as a part of company wide intern project.

Johns Hopkins University — Baltimore, MD
Graduate Research Assistant — Sept '19 – Dec '20

- Devised content and codebase for Cisco sponsored research based on Applied Cryptography.
- Mentored 30+ students towards their Course Capstone for Object Oriented Programming course as TA.
- Built code review analysis tool based on CFGs, data-flow diagrams and ASTs for node.js apps in Python.

Academic Projects and Research

- Secure, real-time drug delivery monitoring for neurologic pathology (2020): Designed threat models, security policies and CI/CD pipeline for development activities in an effort to enforce secure SDLC and DevSecOps practices, developing a lightweight protocol on top of Bluetooth stack for FDA clearances.
- My robot is Flawless, right? (Autonomous Vehicle Security / Machine Learning) (2019): Developed Q Learning based red teaming tool, for automating penetration testing and vulnerability testing on Autonomous Vehicles, utilizing turtlebot3 as test subject after researching & conducting various exploitation techniques.
- Decentralized Firewall for Malware Detection (Blockchain / Machine Learning) (2019): Constructed a prototype as an alternative more durable solution to traditional firewalls (more predictable) and intrusion detection systems using blockchain technology along with autoencoder based Deep learning techniques.

Education

Johns Hopkins University Baltimore, MD
MS in Security Informatics (Cybersecurity) Aug ’19 – Dec ‘20

- Graduate coursework: Software Vulnerability Analysis, Security & Privacy in Computing, Cloud Computing Security, Network Security, Ethical Hacking, Critical Infrastructure Protection, Cryptography, Global Trends.

University of Mumbai Mumbai, MH, India
BTech in Information Technology May ’13 – Jun ‘17

- Undergraduate coursework: Data Structures & Algorithms, Database Management Systems, Systems & Web Security, Big Data Analytics, Computer Organization Architecture, Object Oriented Programming.

Skills

- Programming Languages: C#, Python
- Frameworks: .NET, OWASP Top 10 Web / Kubernetes / LLMs / Containers
- Techniques: Secure code reviews, Architecture and Design reviews, Threat model reviews, Penetration testing, Network traffic analysis, Container security, Kubernetes, Red Teaming
- Platforms: Azure, Infrastructure deployment and review