Jeremy Allen

Security Engineering | Offensive Security

LinkedIn · GitHub

jeremyallen@e2nj4y.com · (678) 595-9790

Professional Summary

I am a security engineering professional with 17 years of experience, including co-founding Carve Systems, a cybersecurity consultancy acquired in 2021. I specialize in security engineering and offensive security assessment, with expertise in application assessment, threat modeling, SDL (Secure Development Lifecycle) implementation, code review, reverse engineering, and cloud security. I have extensive experience communicating security issues to diverse audiences in written and presentation-oriented formats. I have previously given talks at BlackHat and other security conferences and released Mallory, an open-source TCP/UDP MITM tool. My previous experience includes software engineering and development. An extended resume with details of my technical and management experience is available upon request.

Experience

VP of Security Engineering Carve Systems, an iVision company *(Aug 2021 - Oct 2023)*

I continued to serve as a post-acquisition technical leader and delivery consultant within the Carve Systems consulting business.

Founder, Principal Carve Systems, LLC *(April 2013 - Aug 2021)*

Founder of a boutique cybersecurity assessment and services firm that worked with Fortune 500 and high-tech businesses. My service delivery focused on security engineering, software security, threat modeling, reverse engineering, and assessment services. The assessment services I delivered included web applications, SaaS, embedded systems, and traditional desktop applications. I have worked with cross-functional teams to communicate, architect, and resolve security issues at the design and implementation level.

As a principal (in the role of a hands-on CTO), I guided the technical and engineering culture of the business. I oversaw the development of service lines and was responsible for recruiting and directly managing consultants.

I gained experience with all aspects of operating a consulting business: recruiting, sales, customer satisfaction, operations, people management, and delivery of services.

Principal Consultant and CTO Intrepidus Group acquired by NCC Group *(March 2010 - April 2013)*

Initially, I was hired as a Principal Consultant and later promoted to Chief Technology Officer of Intrepidus Group, which focused on mobile app and device security. As CTO and a member of the management team, I used my experience to grow service lines and ensure that Intrepidus Group remained competitive in the mobile security space by continually improving the consulting practice, its consultants, and its service lines. I actively delivered technical consulting services throughout my time with Intrepidus Group. After NCC Group acquired Intrepidus Group, I became a post-acquisition Vice President.

Senior Software Security Consultant Foundstone, Inc. (McAfee) *(February 2006 - April 2010)*

I delivered software security and assessment services. I conducted source code reviews in various languages leveraging my development experience. I was responsible for conducting Secure SDLC (Software Development Life Cycle) improvement engagements. I performed application and network penetration testing against a variety of targets.

I conducted threat modeling, code review, and assessment of many critical systems for customers, including smart grid infrastructure, VMware virtualization software (ESX, View, Workstation), payment hubs, and various Dell desktop software applications.

Application Architect elliptIQ Inc, *(June 2000 - February 2006)*

I was responsible for designing software architecture and writing code for a SaaS startup

Skills

- *Programming Languages and Tools*: Python, Go, C, Java, JavaScript, Assembly, Ansible, Git, RDBMS (Postgres, MySQL, SQLite)
- *Security Engineering*: Threat Modeling, Secure Development Lifecycle (SDL), applied cryptography, semgrep, AFL / fuzzing, DevSecOps, static analysis
- *Reversing Tools*: IDA Pro, Ghidra, ImHex, Godbolt, GDB / WinDbg / Debuggers
- *Offensive Security*: Application Assessment, Reverse Engineering, Vulnerability Analysis, Network Penetration Testing, Embedded Security (IoT devices)
- *Web App Assessment Tools*: Burp Suite, mitmproxy, custom-developed tools, and extensions
- *Network Penetration Testing Tools*: Wireshark, Nessus, nmap, zmap, masscan, Kali, Metasploit
- *Network and Data Security*: IDS/HIDS, SIEM tools (Datadog, Splunk), ASM (Attack Surface Management)
- *Cloud Security*: Scout, AWS/Azure configuration review
- *Miscellaneous*: Linux, command line, custom tool development, automation of security engineering workflows, managing small teams (5-20 individuals), technical recruiting, writing and reviewing policy, risk assessment, NIST CSF, BSIMM, compliance (ISO 27001, SOC 2, PCI DSS, HIPAA)

Speaking

SOURCE - Boston, MA *(April 2011)*

Network Stream Debugging with Mallory

Released new features in Mallory, including a significantly revised and enhanced GUI, fuzzing, and other minor enhancements.

BlackHat Las Vegas, NV *(July 2010)*

Network Stream Debugging with Mallory

Mallory was an extensible TCP/UDP man in the middle proxy designed to be run as a gateway. Unlike most other tools of its era, Mallory supported modifying non-standard protocols (especially those that use SSL) on the fly. Dan Kaminsky said Mallory was cool to me in person and I miss having him in our industry.

Publications

Sybex/Wiley *(March 2002)*

Mastering PHP 4.1 - Jeremy Allen and Charlie Hornberger