ALEJANDRO MERA

San Francisco, CA | alejoseb@gmail.com | +18572417751 | linkedin.com/in/alejandromera-47ab8b65 | alejandromera.com

PROFESSIONAL SUMMARY

Application Security Engineer with 3+ years securing AWS cloud platforms serving millions of users. Builds security tools and automation to scale AppSec across development teams. Deep expertise in AI/LLM security, threat modeling, secure SDLC integration, and vulnerability management for distributed systems. Published security researcher (USENIX Security, IEEE S&P, NDSS) with PhD in Cybersecurity. Strong communicator who translates complex security risks into actionable guidance for technical and non-technical stakeholders.

PROFESSIONAL EXPERIENCE

Security Engineer II | Amazon Web Services (AWS)

July 2024 – January 2026 | San Francisco, CA

- Security affinity engineer for AWS Console Platform, AWS Console Mobile Application (iOS and Android), customer experience and technical documentation - conducted security reviews, threat modeling, and risk assessments for customer-facing features and third-party integrations
- Assessed and mitigated risks in agentic and generative AI workflows, including unsafe model output handling, authorization boundaries, and runtime security controls
- Built LLM-based automation to improve security documentation quality, reducing senior engineer review time by 75% and enabling machine-consumable guidance
- Drove security architecture changes that eliminated client-side credential exposure by moving sensitive authorization flows to backend-only token handling, with scoped policies, audit logging, rate limiting, and runtime monitoring
- Designed secure authentication patterns for third-party design platform integrations where standard AWS auth mechanisms were unavailable, eliminating long-lived credentials and enabling secure adoption by 8,000+ developers
- Investigated complex, multi-service security reports (e.g., SSRF), tracing downstream data flows to resolve false positives and avoid unnecessary remediation

Security Engineer | Amazon Web Services (AWS)

Oct 2022 - June 2024 | San Francisco, CA

- Conducted threat modeling, code reviews, and security assessments for Amazon SES and Pinpoint messaging platforms processing billions of messages daily
- Led vulnerability management program across 50+ production APIs, tracking security debt, prioritizing remediation efforts, and partnering with service teams on risk-based mitigation strategies
- Performed security review for AWS-Meta WhatsApp integration, ensuring secure authorization controls and data protection for enterprise customers reaching billions of users
- Collaborated with development teams to integrate security controls aligned with AWS standards while balancing scalability and developer experience in high-throughput distributed systems

Research Associate / Assistant | Northeastern University SecLab

Aug 2017 - Jan 2026 | Boston, MA

- Designed and implemented security tools and frameworks for firmware fuzzing, concolic execution, and binary-only analysis
- Built novel security testing methodologies published at top-tier venues (USENIX Security, IEEE S&P, NDSS) - tools used by security researchers worldwide

- Communicated complex technical research to academic and industry audiences through publications and conference presentations

Research Intern | Microsoft

June 2020 - Aug 2020

- Designed and implemented full-system and semantic-aware fuzzing tools to improve Azure Sphere OS security - tools integrated into Microsoft's security testing pipeline

EDUCATION

PhD, Cybersecurity | Northeastern University

RISE 2017 Award (Outstanding Graduate Research) | Published 5 papers at USENIX Security, IEEE S&P, NDSS, IEEE ASE

MS, Information Assurance | Northeastern University

TECHNICAL SKILLS

Application Security: Threat modeling, secure SDLC integration, code review, penetration testing, vulnerability management, OWASP
Security Tools & Development: Built security automation and frameworks; proficient with Burp Suite, OWASP ZAP, Metasploit
AI/LLM Security: Prompt injection defense, unsafe output handling, model authorization, runtime controls, agentic workflow security
Programming & Scripting: Python, C/C++, Java, JavaScript, Bash—strong software development background
Cloud & Infrastructure: AWS services, distributed systems security, API security, authentication/authorization, encryption
Research Tools: QEMU, Ghidra, GDB, AFL, binary analysis and reverse engineering
Certifications: Certified Ethical Hacker (CEH)

SELECTED PUBLICATIONS

• P2IM: Scalable Firmware Testing via Automatic Peripheral Interface Modeling - USENIX Security 2020

• DICE: Automatic Emulation of DMA Input Channels for Dynamic Firmware Analysis - IEEE S&P 2021

• D-Box: DMA-enabled Compartmentalization for Embedded Applications - NDSS 2022