Yuliia Borodavka

Software Engineer with 4+ years of experience designing, building, and operating high-availability systems at Amazon. Focused on authentication and authorization for AI agents, distributed systems, and service security.

CONTACT

hi@yuliia.dev
yuliia.dev
Vancouver, BC, Canada
linkedin.com/in/yuliia-borodavka

SKILLS

Java · Python · TypeScript · JavaScript · Kotlin · AWS · AWS CDK · OAuth 2.0 · OIDC · Git

LANGUAGES

Ukrainian, English, Russian

INTERESTS

3D Design, Snowboarding, Painting, Muay Thai

EDUCATION

UC San Diego
Sep 2018 – Mar 2022
B.S. Cognitive Science, Specialization in ML & Neural Computations
Minor: Interdisciplinary Computing Arts

EXPERIENCE

Software Development Engineer, Identity & Authentication

Amazon Development Centre Canada, ULC
December 2025 – Present · Vancouver, BC

- Designed and implemented OAuth 2.0 assertion-based authentication (RFC 7523) for AWS's AI agent identity service, letting AI agents call OAuth-protected APIs without static credentials across 35,000+ internal services
- Built and tested end to end the reference integration and onboarding guide for AI agents acting on behalf of users (OAuth 2.0 authorization code flow), plus a live demo of user-delegated, service-to-service, and delegated token-exchange flows
- Built automatic credential propagation for multi-step AI agent workflows in a Python auth SDK; fixed a token-exchange bug that let agents overwrite the original caller's identity and extend token lifetime, shipping the fix to production in under a day
- Removed public internet access from the standard network template for AI agents, routing all dependencies over private connections with multi-AZ egress filtering
- Built an on-host CPU profiler with encrypted storage and analysis tooling that identified the root cause of a production CPU spike unexplained for 5 months
- Automated service onboarding, reducing engineering effort by 50% while maintaining security standards

Software Development Engineer

Amazon.com Services LLC
August 2022 – May 2025 · New York, NY

- Led the integration of a company-wide authentication service with distributed rate limiting across 9 regions: client integration, infrastructure-as-code rules scaled to fleet size, a shadow-mode rollout alongside the existing local rate limiter, and monitoring
- Led a security remediation campaign that triaged 500+ risks and cut them by 50% in one week, and automated outreach for a company-wide security initiative reaching 33,000+ applications
- Led capacity planning for Prime Day and holiday peak across 20 services on an internal container platform, including a business-critical service at ~19,000 TPS: sized fleets from load tests and live traffic, with 100% availability through peak
- Built observability for a new Java runtime: monitoring, separated logging, and container-level heap and thread dumps for debugging, with documentation that enabled team adoption
- Mentored interns, providing technical guidance through onboarding and project delivery