

Alex Chebaturkin

Security Infrastructure — Identity, Authorization & Privileged Access at Cloud Scale

Seattle, WA · alex@chebaturkin.dev · chebaturkin.dev · linkedin.com/in/alex-chebaturkin

Staff-level engineer (Consulting Member of Technical Staff, IC5) building the security infrastructure that governs privileged access across Oracle Cloud Infrastructure. Architected and shipped the SSH certificate authority, the RBAC/ABAC authorization control plane, the just-in-time access system, and the authN/Z proxy that together mediate access for tens of thousands of operators to hundreds of thousands of hosts across 150+ regions. 12+ years in backend and distributed systems; deep in Go.

EXPERIENCE

Oracle Cloud Infrastructure — Consulting Member of Technical Staff (IC5)

Seattle, WA · 2017 – Present

Security infrastructure for privileged access: identity, authorization and session control across every OCI region.

- **SSH certificate authority (SSH-CA / OSSH).** Architected and shipped the CA issuing short-lived SSH certificates for operator and service accounts, plus the client tooling that mints them on demand, scoped to a specific set of hosts. Serves tens of thousands of operators daily, issuing ~5,000 certificates per day per region across 150+ regions. Replaced Yubikey distribution and eliminated standing keys fleet-wide.
- **Authorization control plane.** Designed and built the service evaluating RBAC/ABAC policy for operator accounts and permissions, with policy data replicated to 150+ regions. A gating control for OCI's FedRAMP High authorization.
- **AuthN/Z sidecar proxy.** Led the rewrite from Python to Go and the migration of 40 service teams in 6 weeks with 2 engineers, against a 6-month baseline — the difference was a configuration translation tool I scoped and built to remove per-team migration work. Supports SAML, OAuth2 / OpenID Connect, OCI IAM, Holder-of-Key, JWT/JWE and mTLS. Benchmarked at 1.5K req/s per host with 3 ms p99.9 for authentication; with authorization in the path, ~500 req/s per host at 30–100 ms, bound by the downstream IAM dataplane hop rather than the proxy.
- **Just-in-time privileged access.** Built time-boxed role activation with region-scoped grants, replacing standing global access for operators. Currently designing in-band token issuance to bring activation latency from minutes to sub-second, after measuring the approval-based version's cost to on-call workflows.
- **Session containment and host enforcement.** Built a constrained shell in Go bounding what an authenticated operator can execute on a host, and the agent governing access to hundreds of thousands of Linux hosts across all OCI regions. Identified and drove remediation of privilege-escape paths through permitted binaries.
- **Shared platform and mentorship.** Built go-service-toolkit — metrics, logging, secrets, health checks, TLS termination with auto-refresh — adopted by 15+ internal services. Shipped 10+ microservices; mentored new hires and senior engineers.

Microsoft, Bing — Software Development Engineer II

Bellevue, WA · 2012 – 2016

- Rebuilt the schema compiler for the workflow engine serving every Bing query: incremental compilation, intelligent partitioning of a 17K+ schema graph, parallel code generation. Cut compile time from 1h20m to 2m at p95, and 1h40m to 10m at p99.
- Designed and shipped a workflow language as a C# extension with full IDE tooling — syntax highlighting, completion, find-usages, refactoring.
- Redesigning the serialization stack, cutting footprint 40%. Built a code-index service over 90K+ workflows, used by 800+ Bing partners.

JetBrains, YouTrack — Software Developer

St. Petersburg, Russia · 2009 – 2011

- Designed the DSL and execution engine for custom issue-management workflows — YouTrack's primary customer extension point. Implemented an LL(1) query parser. Shipped the first release of YouTrack InCloud on AWS EC2.

SKILLS

Security	PKI and certificate authorities · SSH-CA and short-lived credentials · OAuth2 / OpenID Connect · SAML · JWT/JWE · mTLS and Holder-of-Key · RBAC / ABAC authorization · privileged access management · threat modeling · FedRAMP High
Languages	Go · Python · C# · Java · TypeScript · SQL
Systems	Distributed systems · multi-region deployment · Docker · Terraform · Grafana · Linux · OpenSSH internals

WRITING, OPEN SOURCE & EDUCATION

Writing — [SSH Certificate Authority at Scale](#): design and failure modes of short-lived SSH credentials across a global fleet.

B.S. and M.S., Mathematics & Computer Science
ITMO University, St. Petersburg · 2006 – 2012

Microsoft Bond — contributor. Framework for schematized data, comparable to Protocol Buffers.

The Mono Project — designed the post-build static analysis tool for .NET binaries checking code contracts — non-null, interval and array-bounds analysis.