# Nik Ogura

### Principal Engineer

*Platform - Tools - Infrastructure - Security*

*I make things - things that work- and by ‘work’ I mean work superlatively.*

### San Diego County, USA

#### *Aut viam inveniam, aut faciam.*

*(I will find a way, or I will make one)*

# Interesting Accomplishments

#### Orion’s On-Premises Kubernetes System

Picture a stand-alone, self-bootstrapping, one click Kubernetes based system that works in on-prem, cloud-prem, and even air-gapped installations. In addition to Orion’s PTT stack, the system sports it’s own auto-unsealing certificate authority powered by Hashicorp Vault.

The real power of the system is it’s UX. You enter a command, and it creates itself *ex nihilo*. Huge power, amazing complexity, yet it *just works*.

*Components:* **Kubernetes**, **Go**, **ElasticSearch**, **Logstash**, **Kibana**, **Fluent-Bit**, **Hashicorp Vault**, **Prometheus**, **Grafana**, **AlertManager**.

#### Scribd’s SIEM System

Scribd’s world-wide footprint creates interesting challenges from a monitoring and abuse standpoint. Merely being able to see what’s going on is a challenge. There’s so much data coming in that ‘spinner disks’ can’t keep up with it and start smoking the moment you turn the system on. I had to write code that could receive, process, correlate, and consume information for processing. With it we discovered all sorts of interesting things- better insights into how our legitimate users were using the product, and also the bad actors and their botnets.

It’s all available in a self service fashion that allows anyone in the company to answer for themselves the question “What’s going on?”.

*Components:* **Go**, **ElasticSearch**, **Logstash**, **Kibana**, **ElasticBeats**

#### Scribd Managed Secrets System

Define your secrets- what they look like, and how to generate them. The system takes care of the rest. A developer can define a secret, and who should access it, but not be able to know the prod value. Any user gets the proper value for their environment.

Authenticate via LDAP, TLS Certificate, Kubernetes, IAM - it doesn’t matter. One binary tool magically does the right thing and ‘your secrets’ magically appear at your fingertips.

*Components:* **Hashicorp Vault**, **Go**

#### Stitch Fix Algorithms Access and Identity System

It was the means by which the entire department of data scientists and engineers connected to every system, instance, and container in the tech stack. Virtual machines, containers, in the cloud, locally. One single, unified, independent access system.

*Components:* **OpenLDAP**, **OpenVPN**, **OpenSSH**, **SSSD**, **PAM**, **Python**, **Go**

#### Self-Updating Signed Binary Tool Distribution and Execution Framework

It’s used for distributing and running signed binaries on user laptops, in cloud instances and docker containers. It’s always up to date, works on and offline, and best of all it *just works*.

*Components:* **Go**, **Artifactory**, **OpenPGP**

#### Apple Pay’s Test-Driven Cloud-Based CI/CD Pipeline

*Components:* **Chef**, **Java**, **Spring**, **Maven**, **OpenStack**, **Python**, **Ruby**, **GitHub**, **TeamCity**

#### Application Stack Prototyping and Orchestration Suite

Basically I wrote ‘docker-compose’, before what we now know of as ‘docker-compose’ was totally stable.

*Components:* **Java**, **Python**, **OpenStack**, **Docker**, **Netscaler**, **HPNA**

#### Static Code Analysis Tools for Puppet Modules

There were no tools to do SCA of Puppet modules for GRC (Governance, Risk- Management, and Compliance). So I made some.

*Components:* **Java**, **Spring**, **Tomcat**, **Spring Security**, **Antlr**, **Ruby**, **GitHub**, **jQuery**, **Puppet**

#### US Bank’s Encryption Key Management and Delivery System

A PKI was purchased, and it didn’t do what we needed. The parts didn’t talk to each other. It couldn’t deliver the keys. Manual key management was not working.

*Components:* **Java**, **Spring MVC**, **Spring Security**, **jQuery**, **jQueryUI**, **BouncyCastle**, **Jackson**, **Apache Commons**, **StringTemplate**, **SQLite**, **ProtectApp**

#### Credit Card PAN Encryption and Tokenization System

It encrypted/decrypted and masked credit card numbers for a Merchant Acquiring systems (Credit Card Authorization and Settlement).

*Components:* **Perl**, **C**, **Java**

#### Hardened LAMP stacks for PCI Compliant Credit Card Processing Applications

*Components:* **Apache**, **Tomcat**, **Java**, **Perl**, **OpenSSL**, **libxml2**, **libxslt**, **MySQL**, **Git**, **Subversion**, **ModSecurity**, **ModAuthVAS**, **Kerberos**, **ModJk**

#### US Bank’s Web Application Firewalls

I’ve designed, implemented, and maintained Web Application Firewalls for cross platform applications, some directly handling credit card PAN data.

*Components:* **Apache**, **ModSecurity**, **OWASP ModSecurity Core Ruleset**

#### Brought a Whole Business Line’s Tech Stack into PCI Compliance

I participated in creating and executing a plan to bring a multi- million dollar business line centered around credit card processing systems from zero to PCI 2.0 compliant in < 12 months. Can do it again too.

# Profiles

*Home Page* <http://nikogura.com>

*Code Repos* <https://github.com/nikogura>

*LinkedIn* [https://www.linkedin.com/in/nikogura/](https://www.linkedin.com/in/nikogura)

# Technical Background

*Programming Languages:* **Java**, **Ruby**, **Python**, **Groovy**, **JavaScript**, **C**, **C++**, **Perl**, **Go**, **Bash**

*Communication:* Educator for Best Practices, Test Driven Development, Application Security, Network Security, Penetration Testing. Instructor for Leadership, Public Speaking.

*Configuration Management:* **Chef**, **Puppet**, **Ansible**

*Operating Systems:* **RPM Linux Systems (RHEL, SLES, CentOS, Oracle Linux)**, **Debian Linux Systems (Debian, Ubuntu)**, **Arch Linux**, **Android**, **MacOS**

*System Administration:* **Physical Machines**, **Virtual Machines**, **Containers**, **Clouds**, **Workstations**, **TCP/IP Networks**, **Routers**, **Switches**, **Firewalls**, **Kubernetes**

*Logging and Monitoring* **LogStash**, **ElasticSearch**, **Kibana**, **ElasticBeats**, **Syslog**

*Web Servers & Application Containers:* **Apache HTTPD**, **Tomcat**, **ModPerl**, **Nginx**, **HaProxy**, **Gunicorn**

*Testing:* **jUnit**, **TestNG**, **Selenium**, **Test::More**, **Rspec**, **ServerSpec**, **Inspec**, **unittest**, **go test**

*CI Systems:* **Jenkins**, **TeamCity**, **CircleCI**, **Strider**

*Security:* **SSL**, **SSH**, **IPSec**, **PCI DSS**, **Spring Security**, **ModSecurity**, **Kerberos**, **Vault**

*Networks:* **IPTables**, **PF**, **BIND**, **DHCP**, **Dnsmasq**, **Sendmail**, **Postfix**, **CUPS**, **OpenLDAP**

*Version Control:* **Git**, **GitHub**, **GitLab**, **Subversion**, **Mercurial**

*Databases:* **MySQL**, **Oracle**, **SQLite**, **HSQL**, **MongoDB**, **Cassandra**, **Postgres**

*Build Tools:* **Make**, **Ant**, **Maven**, **Gradle**, **Archiva**, **Artifactory**, **Rake**

*Virtualization:* **VirtualBox**, **VMWare**, **Vagrant**, **Packer**, **Qemu**, **ESXi**, **vSphere**, **OpenStack**, **Docker**, **KVM**, **libvirt**

*SCA/ Language Tools:* **Antlr**, **RATS**

# Open Source Projects:

* [dbt](https://github.com/nikogura/dbt) “Dynamic Binary Toolkit” A framework for authoring and using self-updating signed binaries. Listed in [awesome-go](https://github.com/avelino/awesome-go)
* [gomason](https://github.com/nikogura/gomason) A tool for doing clean-room CI testing locally. Listed in [awesome-go](https://github.com/avelino/awesome-go)
* [go-postgres-testdb](https://github.com/stitchfix/go-postgres-testdb) A library for managing ephemeral test databases.
* [python-ldap-test](https://github.com/zoldar/python-ldap-test) A testing tool Python implementing an ephemeral in-memory LDAP server
* [CGI::Lazy](http://search.cpan.org/~vayde/CGI-Lazy-1.10/lib/CGI/Lazy.pm) A Perl Web Development Framework.
* [Selenium4j](https://github.com/nextinterfaces/selenium4j) A Java Library for translating HTML format Selenium tests into JUnit4 at runtime.

# Professional History

## AWS Global Financial Services

2022 - Present *Senior DevOps Consultant*

Serving as ‘Jack of All Trades’ (and master of some) to the Financial Services and Banking sector. Teaching DevOps Principles and driving Cloud Adoption.

Bringing the Financial Sector into the 21st century - kicking and screaming if necessary.

Pro Tip: There usually is a bit of kicking and screaming involved. Modern tools and principles are as much about HOW you use them as WHAT tools you use. People love shiny new tools, but are slow to change their thinking and their procedures.

You can’t drive a Ferrari as if it was a Model T - not and get all the benefits of driving a Ferrari. The cost, sadly, is the same regardless.

## Orion Labs - San Francisco, CA

2020 - 2022 *Principal Staff Engineer*

I took a legacy EC2 autoscaling application stack and re-architected it as a stand-alone, self-bootstrapping, one click Kubernetes based system that works in on-prem, cloud-prem, and even air-gapped installations. In addition to Orion’s PTT stack, the system sports its own auto-unsealing certificate authority powered by Hashicorp Vault.

Feedback from one secretive governmental customer whose name I am not cleared to know was one word: “flawless”. Another very large well known company described it as “The smoothest, easiest, highest quality installation they have ever seen”.

While doing that, I replaced an expensive Splunk based monitoring/metrics system with a totally modern, best in class, and most importantly free stack based on Prometheus, Grafana, and Alertmanager. What’s more, since it’s based on open source technology, our monitoring/metrics stack was able to be bundled into our on-premises product as a value add for our customers.

For an encore, I created the Golang development standards for the company. Once the new standard was created, I refactored the legacy microservices to this new standard, wrote a few new ones, and created the Orion Voice Bot framework in golang, complete with its own Kubernetes Operator for easy deployment and management.

I was also responsible for all technical training within the company. I designed curriculum and taught internal classes on topics such as golang, elasticsearch, kubernetes, dns, IP networks, TLS/SSL, and both symmetric and asymmetric encryption. If it happened on a computer, I was responsible for teaching people how to do it.

#### Scribd - San Francisco, CA - Sec/DevOps Engineering Lead - 2018 - Present

I created one-click self-service deployment tooling to bare-metal hosts and Kubernetes clusters. Heck, I even created a series of Kubernetes clusters myself, ex nilhio, and lead the effort to use them in anger.

The company’s entire onboarding and access system, both to our network and our K8S clusters came out of my fertile mind and busy fingers, as did our internal PKI- with a little help from Hashicorp Vault and a ton of golang magic.

I designed and build a system of ‘Managed Secrets’ so that we could generate, rotate, and well, ‘manage’ secrets across the enterprise - in AWS and in a bare metal datacenter. An app getting the right secret is important, but you also need to know who has access to what, when to rotate, et al.

I tamed the ELK stack, and wrote event correlation tools to take incoming request data from Fastly’s WAF and make it available to detect and counter bad actors all over the world. This system ingests hundreds of Gb of information daily that flows in so quickly that it melts old-fashioned spinner disks.

I revel in a porous boundary between Sec / Dev / Ops that allows me to secure, advise, and build amazing solutions that not only work, but are object lessons in *doing it right*.

#### Stitch Fix Inc. - San Francisco, CA - Data Platform Engineer - 2017

* Created the Access and Identity systems whereby the Algorithms & Analytics department connects to every resource, instance and container in the stack.
* Enabled AWS IAM Role based development that works transparently on a laptop as if the computer were actually an EC2 node. Whether you’re local or in the cloud your code works exactly the same.
* Built a self- building, self-updating, extensible userspace binary tooling system that creates and distributes signed binaries for doing work on laptops with no external depenencies.

#### Apple iOS Systems - Cupertino, CA - Senior DevOps Engineer - 2015 ~ 2017

* Designed and built a dynamic test driven CI/CD pipeline for Apple Pay, Apple Sim, and every Apple device in the world.
* Implemented a private OpenStack cloud for testing and verification of applications.
* Designed a system whereby the entire deployment footprint of a group of applications can be described and manipulated in code.
* Transitioned the organization from Subversion to Git.

#### Data Recognition Corporation - Maple Grove, MN - Principal DevOps Engineer - 2014 ~ 2015

* Designed an auto scaling Continuous Delivery environment for educational testing.
* Shepherded multiple applications from proprietary systems to fully Open Source platforms.
* Designed and taught internal training curriculum for the technology, disciplines, and cultural concepts that come under the heading of DevOps.

#### Wells Fargo - Minneapolis, MN - Sr. Software Engineer - 2014

* DevOps Consultant for Development, Testing, Building and Delivery of Applications and Middleware.
* Module Developer for Continuous Integration/ Continuous Delivery of multiple applications across multiple technologies and multiple operating systems.
* Designed and built SCA tools to parse the Puppet DSL for GRC.

#### U.S. Bank - Minneapolis, MN - Application Systems Administrator Sr. 2007 ~ 2014

* Specialty Application Development- Projects too sensitive or specialized for a general development team, or things that were deemed ‘impossible’.
* Designed, built and implemented encryption key fullfillment system used by mulitple users in multiple countries.
* Designed, build, and maintained encryption and tokenization system for PAN data in Merchant Acquiring systems.
* Security Consultant for an Application Architecture team.
* Designed and Maintained full SDLC for High Availability PCI Compliant Apache Servers and LAMP Applications in multiple network tiers.
* Third level support of Web Applications, RHEL and SLES Servers, Oracle Databases, and IP Networks.
* Worked with Application Architecture teams and Development teams to preemptively address emerging threats while maintaining PCI DSS compliance across mixed technologies and multiple operating systems.
* Designed Monitoring and Alerting modules for High Availability Apache Servers (Custom Apache Modules).
* Full Stack Web Development on a variety of platforms.
* Presented internal courses/talks to business and technology teams on web communication and its dangers.
* Trained Development and QA personnel in methods and tools for Unit/ Integration testing.
* Designed IPSec and IPTables security profiles for protection of PAN data in PCI Enclaves.
* Designed and implemented processes for Code Signing, Continuous Integration, and Application Building.
* Consultant for Penetration Testing, Exploit Confirmation, and Proof of Remediation.
* Consultant/SME for SSL, SSH, Encryption, Public Key Infrastructure.
* Consultant/SME for Software Packaging, Build, Deployment.

#### Plain Black - Madison, WI - Developer - 2006~ 2007

* Provided online troubleshooting for supported customers.
* Core development on the WebGUI CMS

#### Universal Talkware - Minneapolis, MN - NOC Administer - 2000

* I handled internal tools development, built the NOC, and even supported the physical plant.

#### Hessian & McKasy - Minneapolis, MN - IT Administrator - 1999 ~ 2000

* I started out as the help desk, and ended up as the head of IT for a 40 seat Law Firm.

#### United Martial Arts - Plymouth MN - CEO and Head Instructor - 1998 ~ 2007

* Responsible for day to day operations of the martial arts studio, including management, financial planning, and personnel.
* Taught classes in Exercise, Wellness, Leadership, and the Martial Arts in the studio as well as for corporations and in the community.
* Designed, built and maintained a custom studio management desktop application that handled enrollment, financials, lesson plans, scheduling, video and print library management, and curriculum.
* Authored training curriculum for leadership programs as well as physical curriculum.