Corsha

Protecting Software Supply Chains with Hyperledger Fabric

22 February 2023
Corsha

Anusha Iyer/ CEO
anusha@corsha.com
The Agenda

01. Today’s Software Supply Chains
02. The Secret about API Secrets
03. The Explosion of CICD Attacks
04. Corsha’s MFA Platform for APIs
05. How we use Hyperledger
06. The Demo
A CICD PIPELINE

CI/CD Pipeline
Dev/Test Environments

Push Artifacts
and Updates

Jfrog Artifactory

Pull Dependencies
Publish Artifacts

Staging/
Prod Environments

Deploy charts,
containers, etc

docker

Google Cloud

STAGING

PROD

Source Code

Third Party
Vendor(s)

Commit
Build
Scan & Test
Publish
Deploy

GitHub

Jenkins

HELM

STAGING

kubernetes

amazon web services

Microsoft Azure
API SECRETS ARE JUST SYSTEM PASSWORDS

- Secrets are often shared, rarely rotated, and often set to never expire
- They get leaked, sprawled, and sprayed across tons of environments
- Their static nature make them ripe targets for adversaries
...AND WEAK PROXIES FOR **MACHINE IDENTITY**

**API KEYS**
Easy to generate but static, long-lived. Dangerous!

**TOKENS**
Standard token formats, can be short-lived but rooted in static secrets

**PKI CERTS**
Facilitates Mutual TLS. Key Management is brutal at scale and with third parties
SECURING MACHINE-TO-MACHINE COMMUNICATION

Automation, cloud, and scale are foundational to connected Critical Infrastructure

REQUIRES
- Security that can keep pace with Automation
- Strong, cryptographic Identity
- Pinned communication between trusted entities
- Self-service credential rotation and hygiene
- Full observability and fine-grained control
THE NEW TARGET: CICD AND AUTOMATION

GitHub: Attacker breached dozens of orgs using stolen OAuth tokens
GitHub revealed today that an attacker is using stolen OAuth user tokens (issued to Heroku and Travis-CI) to download data from private repositories.

Okta source code stolen in GitHub hack
…attackers apparently stealing the company's source code.

CircleCI security alert: Rotate any secrets stored in CircleCI
• Immediately rotate any and all secrets stored in CircleCI. These may be stored in project environment variables or in contexts.
MFA for APIs
API Security Platform
Dynamic Machine Identity + MFA for Machines

- Protect API calls with one-time-use, MFA creds
- Pin access to only trusted machines
- Monitor and control all API traffic
- Use for cloud-native and legacy apps alike
- No Code Change Anywhere

Corsha Flow

1. Each API client periodically extends its dynamic identity in the DLN
2. API clients make API requests with Corsha MFA, one-time-use creds
3. The Corsha Proxy checks the MFA Credit against the DLN per API request.

Diagram:
- Deployed machines (API Clients)
- API Call() + Corsha_MFA_Cred
- Corsha Proxy
- API Service(s)
- Check M3’s Corsha_MFA_Cred
- Deployment System (CI/CD)
- Corsha Distributed Ledger Network (DLN)
- Corsha Console
• DLN is fully Kubernetes-native, Cloud Agnostic

• We have deployments across Azure, AWS, GCP, even air-gapped infrastructure

• Simple Helm Driven deployment in minutes
STREAMING MACHINE IDENTITY

- Authenticator keeps the last few Cryptographic beats in local, persistent fixed storage
- Identity Stream Chained over time
- No code change required on the Authenticator or Proxy side
- Easy to rotate underlying identity
**CORSHA INTEGRATIONS**

**ISTIO/ENVOY**
Envoy Filters to add MFA Credentials and Check Credentials

**VIRTUAL MACHINES**
Deploy Authenticator as binaries or containers within a VM

**API GATEWAYS**
Integrate Corsha’s Proxy directly into API Gateways, such as Nginx, Kong and Apigee

**NATIVE KUBERNETES**
Helm-driven deployments to add Corsha’s Authenticator as a sidecar

**DOCKER CONTAINERS**
Deploy Authenticators as Sidecars, uniquely priming them at the time of deployment

**CODE-LEVEL SDKS**
Integrate Corsha’s Authenticator or Proxy directly into your code
APIS ARE EVERYWHERE

SOFTWARE SUPPLY CHAIN
Artifact publishing, CICD pipelines driven by automation and chained services

ZERO TRUST FRAMEWORKS
Non-person entities = machines. Zero trust starts with strong Identity and Access

THIRD PARTY API ACCESS
Do better and more easily than static keys, tokens, and mutual TLS

CRITICAL INFRASTRUCTURE
Communicating to/from and controlling critical infrastructure

HYBRID CLOUD
Even internal API ecosystems talk across hybrid cloud and on-prem environments

DATA FABRICS AND LAKES
Movement of data into/out of a fabric or data lake
SECURING CICD SYSTEMS

Let’s look at securing Artifact Publishing

1. Trusted Third Party Vendor
   - Deploy a simple Corsha Authenticator to Trusted Machines
   - Push Artifacts and Updates
2. Jenkins
   - Pull Dependencies
   - Publish Artifacts
3. JFrog Artifactory
   - Place a Corsha Proxy in front of Artifactory
4. CI/CD Pipeline
   - Dev/Test Environments
5. Staging/Prod Environments
   - Deploy charts, containers, binaries, etc

Corsha
TAKEAWAYS
IT, OT, and the Supply Chain Seeding Them

Elevate Machine Identity to maturity of Human ICAM

Zero Trust is a layered defense methodology

Software Supply Chain Security is foundational

Corsha’s Cybersecurity Capabilities:
  Zero Trust for NPEs at Scale
  Automated, Dynamic Machine Identity
  MFA for Machines
  Hyper-converged security for OT and IT
  Composable and Self-Servicing