tetrate

# TOP TEN ISTIO SECURITY RISKS AND MITIGATION STRATEGIES

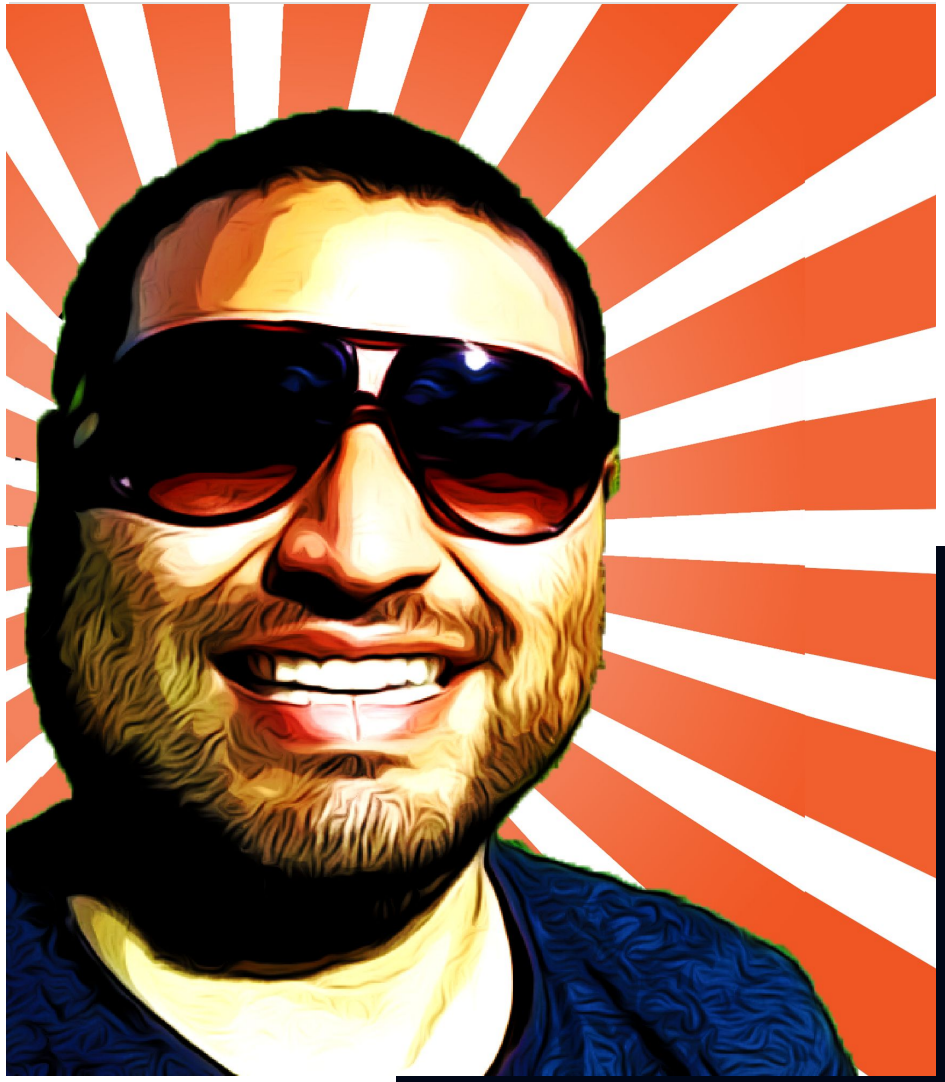
KubeCon | CloudNativeCon

Europe 2023

# José Carlos Chávez

SOFTWARE ENGINEER @ TETRATE

- Open source enthusiast
- OWASP Coraza Co-leader
- Zipkin core member
- Loving father



KubeCon | CloudNativeCon
Europe 2023

@jcchavezs

# SECURITY RISKS AND MITIGATION STRATEGIES

**SECURITY RISKS:** Likelihood + Impact

- **how easy** is it for attackers to carry out an attack? Does it take a **skilled** adversary? **how cheap** it is to launch attacks?
- **how sensitive** are the systems likely to be affected, **how valuable and sensitive** is the target data? is it **hard to recover** the data?

**MITIGATION STRATEGIES:** Dealing with risks

1. **assume** and accept risk
2. **avoidance** of risk
3. **controlling** risk
4. **transference** of risk
5. **watch and monitor** risk

“

# Isn’t Istio secure by default?

# Security layers

Security is a combination of multiple protection mechanism on multiple levels

Underlying infrastructure

Kubernetes platform

Istio service mesh

Applications

# THREAT ACTORS

### INTERNAL ATTACKER

An entity with some level of privilege that would seek to exceed one or more trust boundaries.

### CONTRIBUTORS TO ISTIO

Contributors could harm Istio by attempting to intentionally introduce vulnerable code and subsequently exploit it.

### CONTRIBUTORS TO 3RD-PARTY DEPS

Istio's dependencies may be used by malicious attackers to exceed their trust boundaries in Istio.

### UNTRUSTED USERS

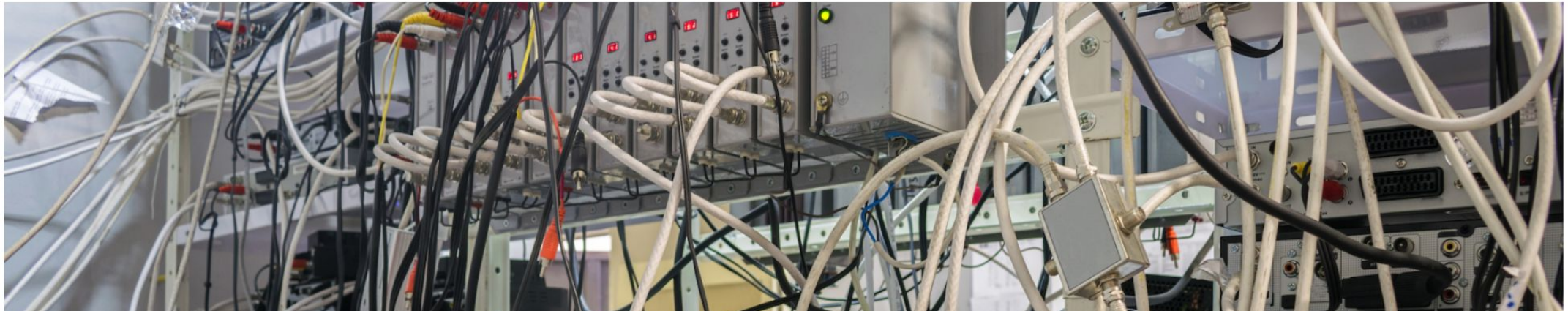
Users with the lowest level of privilege of Istio's threat actors and may seek to cause harm by exceeding their trust boundaries.

RESEARCH

# Misconfiguration leaves thousands of servers vulnerable to attack, researchers find

Simple mistakes and configuration errors is still a major cybersecurity issue, according to security firm Censys.

BY CHRISTIAN VASQUEZ • APRIL 19, 2023



# I01: INSECURE COMMUNICATION

Insecure communication can pose a significant security threat: on-path attacks, spoofing, credential stuffing, brute force, phishing, malicious API requests, etc.

- The Istio `permissive` security setting is useful but insecure as it accepts plaintext and encrypted traffic.
- A `strict` security setting would force all communication to be secure

**Mitigation:**

- Enable `mTLS` through a `PeerAuthentication` policy on namespace or wide mesh (`istio-system` namespace).
- If `permissive` mode is required, use `AuthorizationPolicy` to restrict traffic on plaintext.

# I02: UNSAFE AUTHORIZATION PATTERNS

Istio allows fine-grained authn policies to connections between workloads using the `AuthorizationPolicy`

```
...
spec:
  action: ALLOW
  rules:
  - to:
  - operation:
  notPaths:  ["/private"]
```

**Mitigation**

- Use `default-deny patterns`: your system denies all requests by default
- Use `ALLOW-with-positive-matching` and `DENY-with-negative-match` patterns



@jcchavezs

# I03: WEAK SERVICE ACCOUNT AUTHN

One of the most important principles of computer security is the **least privilege principle**: A user should have no more access privileges than what is necessary for their task.

- `init_container` has permissions to create network policies
- Bypass `outboundTrafficPolicy` by impersonating the `istio-proxy` user (UID 1337)
- Usage of `first-party-jwt`.

**Mitigation**

- Use Istio `CNI` plugin to avoid requiring privileges like `NET_ADMIN` capability.
- Require containers inside pods to run as non root using `MustRunAsNonRoot`
- Use `third-party-jwt` to restrict its usage to sidecar

# I04: BROKEN OBJECT LEVEL AUTHZ (BOLA)

Istio provides `AuthorizationPolicy` to perform checks on HTTP headers and the path, Kubernetes metadata (origin and destination services) as well as validating JWTs.

- Can't access to al JWT's fields
- Policies get out of sync with architecture

**Mitigation**

- All access decisions have to be based on least-privilege principles, per-request, context-based, and on identities.
- Use rich model policies like NGAC or OPA for declarative, domain-compatible policies.

# I05: SUPPLY CHAIN VULNERABILITIES

Istio itself uses several open-source components and third-party code (e.g. Envoy and Prometheus) but a typical istio deployment include several images from different sources. Some of the risk are:

- Image Integrity
- Image Composition
- Known Software Vulnerabilities

**Mitigation**

- Image scanning
- Image Composition & Software Bill of Materials (SBOM)
- Image Signing
- Curated registry
- Web Application Firewall



@jcchavezs

# I06: INGRESS TRAFFIC CAPTURE LIMITATIONS

Istio sidecar is supposed to hook inbound and outbound traffic in the pod, however:

- It does not support UDP traffic, so traffic will be passed to services inside the Pod.
- Inbound capture is disabled on ports used by the sidecar (including port 22)

**Mitigation**

- For control of UDP traffic, use Kubernetes `NetworkPolicy` at ingress.

# I07: EGRESS TRAFFIC CAPTURE LIMITATIONS

Istio cannot securely enforce that all egress traffic actually flows through the egress gateways, meaning that it can not enforce calls to be done to known destinations.

**Mitigation**

- Kubernetes `NetworkPolicy` for egress
- Istio's egress restrictions (e.g. `outboundTrafficPolicy: REGISTRY_ONLY`),
- Runtime checks on linux system calls (e.g. falco)

# I08: SECURITY OBSERVABILITY AND MONITORING FAILURES

Security observability and monitoring are critical components,  however, incorrect collection, processing or reporting of such data can pose significant risks to the security.

- Log level paradox
- Insufficient or inadequate audit logs
- Lack of context

**Mitigation**

- Ensure access logs and error logs are emitted.
- Implement a org-wide log format
- Log data should be encoded/redacted correctly
- Ensure high-value transactions have an audit trail
- Establish an incident response and recovery plan



@jcchavezs

# I09: VULNERABLE ISTIO VERSIONS

Using an outdated Istio version can pose significant security risks, as older versions may contain known vulnerabilities that have been addressed in later versions. Some of the disclosed attacks are:

- (DoS) attacks
- CVEs
- Bypass of Istio policies
- Cryptographic

**Mitigation**

- Use compliant Istio distributions e.g. Tetrate Istio Distro
- Track CVE databases and Istio Security Bulletins
- Web Application Firewall

# I10: WHAT IS YOUR SECURITY RISK?

Come by and participate

https://forms.gle/6vmLq5LkjKYXcQVz8

KubeCon | CloudNativeCon

Europe 2023

@jcchavezs

# CONCLUSIONS

- Most of the security risks are related to configuration mistakes.
- Prefer being explicit over relying on default, sometimes “auto” capabilities.
- No single component or function will be sufficient to achieve a good level of security alone, but collectively they need to enforce security patterns across all layers in the infrastructure.
- Policies have to be defined based on the assumption that the attacker is already inside the network.

tetrate

# Thank you everyone.
# Gracias, mamá.

jcchavezs | jcchavezs | www.tetrate.io

For any further queries, feel free to contact me at jc@tetrate.io

# References


Sysdig 2023 Cloud-Native Security and Usage Report — https://sysdig.com/blog/2023-cloud-native-security-usage-report/

Istio Security Audit - Ada Logics 2022 — https://istio.io/latest/blog/2023/ada-logics-security-assessment/

NIST SP 800-207A: A Zero Trust Architecture (ZTA) Model for Access Control in Cloud Native Applications in Multi-Location Environments

State of Service Mesh Market 2022 - Tetrate — https://tetrate.io/tetrate-service-mesh-survey-2022/


@jcchavezs

# References


| | |
|---|---|
| 2022 Service Mesh Adoption Survey | https://www.solo.io/resources/report/2022-service-mesh-adoption-survey/ |
| State of Kubernetes security report - Redhat, 2022 | https://www.redhat.com/en/resources/state-kubernetes-security-report |

tetrate

# TOP TEN ISTIO SECURITY RISKS AND MITIGATION STRATEGIES

KubeCon | CloudNativeCon

Europe 2023