Emerging trends driven by need for agility, speed, cost, data volumes ...

Containers + microservices

Public cloud, multi-cloud and hybrid architectures

Heterogeneous app stacks - languages, PaaS, OSS
How does it impact security?

- Significantly **greater surface area** to attack within the network if the perimeter is breached.
- Compromise of shared services enables **replay attacks**.
- Higher risk of indirect unauthorized access using **stolen identities** or by malicious insiders.
Mitigating risk in modern production environments

The zero trust security model for communication security

1. Assume threat already exists within the network
   A peer (service or client) should not be trusted just because it is in the same network even if the client presents valid application level credentials.

2. Ensure every service has its own firewall (micro-perimeter)
   All access - human or programmatic - to production services should be strongly authenticated, authorized and encrypted.

3. Enable central administration and monitoring
   Security teams should be able to understand the overall security posture and manage mandatory security policies across all services.
Google has adopted such a posture for many years...

**BeyondCorp at Google**
- Enterprise security model that builds upon 6 years of building zero trust networks at Google.
- Improves security with regards to how employees and devices access internal applications.

**Application Layer Transport Security at Google**
- Transport security based on strong mutual authentication of peer vs. trusting the network.
- Optimized for Google’s production services.
- Other design principles:
  - transparent from the application
  - long lived connections
But how do you implement a similar posture at scale while retaining the deployment agility and stack heterogeneity enabled by modern production environments?
Istio is an open services platform that incorporates the principles and learnings from securing Google’s production with technologies like ALTS.
What is Istio?

An open services platform to manage service interactions across container- and VM-based workloads.
What does Istio do?

**Observability**
Latency, errors, dependencies, tracing

**Control**
L7 load-balancing, rate limiting, safe rollouts of new versions

**Security**
Encryption, strong authentication, authorization
What can you do with Istio security?

- Enable mTLS for authentication and encryption.
- Authorize access based on service identity or any channel attribute.
- Configure finer grained RPC-level access control for REST and gRPC.
Why do we support mTLS via Istio?

Policy driven encryption in transit with no code changes

... but that’s only the obvious value ...
Peers are authenticated using **non-replayable service identities** bound to the TLS channel.

Similar to ALTS, Istio strongly authenticates the **workload identity** and not the host.

End user or application level identity is propagated as a **bearer token** across service “hops”.
Istio enables **identity and context aware network security policy** enforcement.

Policies based on service identities are **resilient to redeployment of peers**.

REST / gRPC: Finer grained access control and ability to reason about both peer and end user identity.
Istio Component Architecture

Envoy: Network proxy to intercept communication and apply policies.

Pilot: Control plane to configure and push service communication policies to Envoys.

Citadel: Service-to-service authentication using mutual TLS with built-in certificate and key management.

Mixer: Flexible model for policy enforcement and monitoring with a plugin model.
Istio Security: Life of Request

- **JWT + TLS / mTLS**
- **Ingress Proxy**
  - Perimeter security policies
  - mTLS
- **Service A**
  - Routing + Secure Naming
  - Cert issuance
  - HTTP, gRPC, TCP
- **Service B**
  - Policy Enforcement + Reporting
  - mTLS
  - Local AuthZ
- **Egress Proxy**
  - Perimeter security policies
  - mTLS

Security policies can be implemented at different levels of granularity - Service, Namespace, Mesh.
Policy based mTLS enablement
*Enforce strong peer authentication + encryption.*

End-user identity verification
*Assert that client is acting on behalf of an authenticated end user.*

Peer identity based Authorization
*Deny non-whitelisted services even with the right application level credentials (bearer token).*

Monitoring
*Centrally manage and monitor all communication.*
Two-Tier Example

External | Internal

HTTP

frontend

HTTP

backend

ProductPage Pod

Reviews Pod

No Traffic Encryption
No Access Control
No Visibility
Istio without mTLS

External    | Internal
---|---
Ingress Pod | Envoy
| Envoy
| frontend
| Envoy
| backend

HTTP

Reviews Pod

ProductPage Pod
Istio without mTLS: Insider can access with app level credentials
Istio with mTLS: Can only access with valid key/cert
Validate that front end is acting on behalf of authenticated end user.

Backend expects 2 credentials.
Istio ensures that request has valid user credential in addition to an authenticated peer.
Istio Authorization

- External
- Internal

- Ingress Pod
- ProductPage Pod
- Reviews Pod

Envoy

- frontend
- backend
Istio Authorization

External | Internal

- Ingress Pod
- ProductPage Pod
- Reviews Pod

Envoy

- Frontend
- Backend
Istio Authorization

External    Internal

- Ingress Pod
- Frontend Pod
- Reviews Pod

Envoy

[Diagram showing traffic flow and authorization process]
Istio Authorization

External    Internal

Ingress Pod

Envoy

ProductPage Pod

Envoy

Reviews Pod

backend

frontend

Envoy
How to engage with Istio Security

**Users**

Try out Istio on Google Cloud

https://cloud.google.com/istio

Join the Istio user group

groups.google.com/forum/#!forum/istio-users

Participate or ask questions

istio.rocket.chat
How to engage with Istio Security

Developers

● Code contribution on [github.com/istio/](https://github.com/istio/)

● Sign up for Istio security [groups.google.com/forum/#!forum/istio-security](https://groups.google.com/forum/#!forum/istio-security)

● Join the Istio security community meetings ([istio.zoom.us/j/117159906](https://istio.zoom.us/j/117159906)) bi-weekly on Wednesdays from 11am-12pm PST

● Sign up for Istio dev [groups.google.com/forum/#!forum/istio-dev](https://groups.google.com/forum/#!forum/istio-dev)

● Join the wider Istio community meetings ([zoom.us/j/986657835](https://zoom.us/j/986657835)) bi-weekly on Thursdays from 11am-12pm PST
Questions?
Monitoring