CNCF Security SIG Deep Dive: 22 May 2019

Justin Cappos, Zhipeng Huang • 22.05.2019

Wednesday, May 22 • 11:05 - 11:40

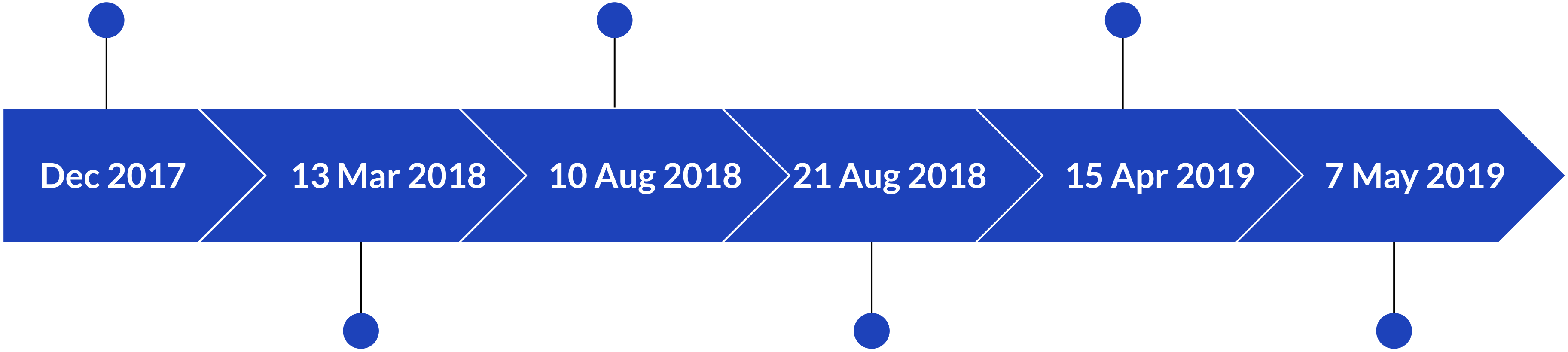
Overview

Focus areas

- Protection of cloud native* systems, while providing needed access
- Common understanding and common tooling to help developers meet security requirements
- Common tooling for audit and reasoning about system properties.

* cloud native *adj.*

heterogeneous, distributed and fast changing systems

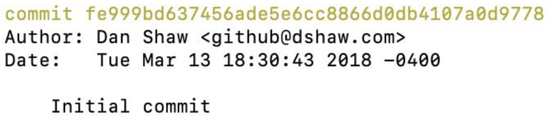


Dec 2017

Started socializing at
Kubecon Austin

13 Mar 2018

Initial Commit for
SAFE repo



```
commit fe999bd637456ade5e6cc8866d0db4107a0d9778
Author: Dan Shaw <github@dshaw.com>
Date:   Tue Mar 13 18:30:43 2018 -0400

    Initial commit
```

10 Aug 2018

Policy WG merged
with SAFE

21 Aug 2018

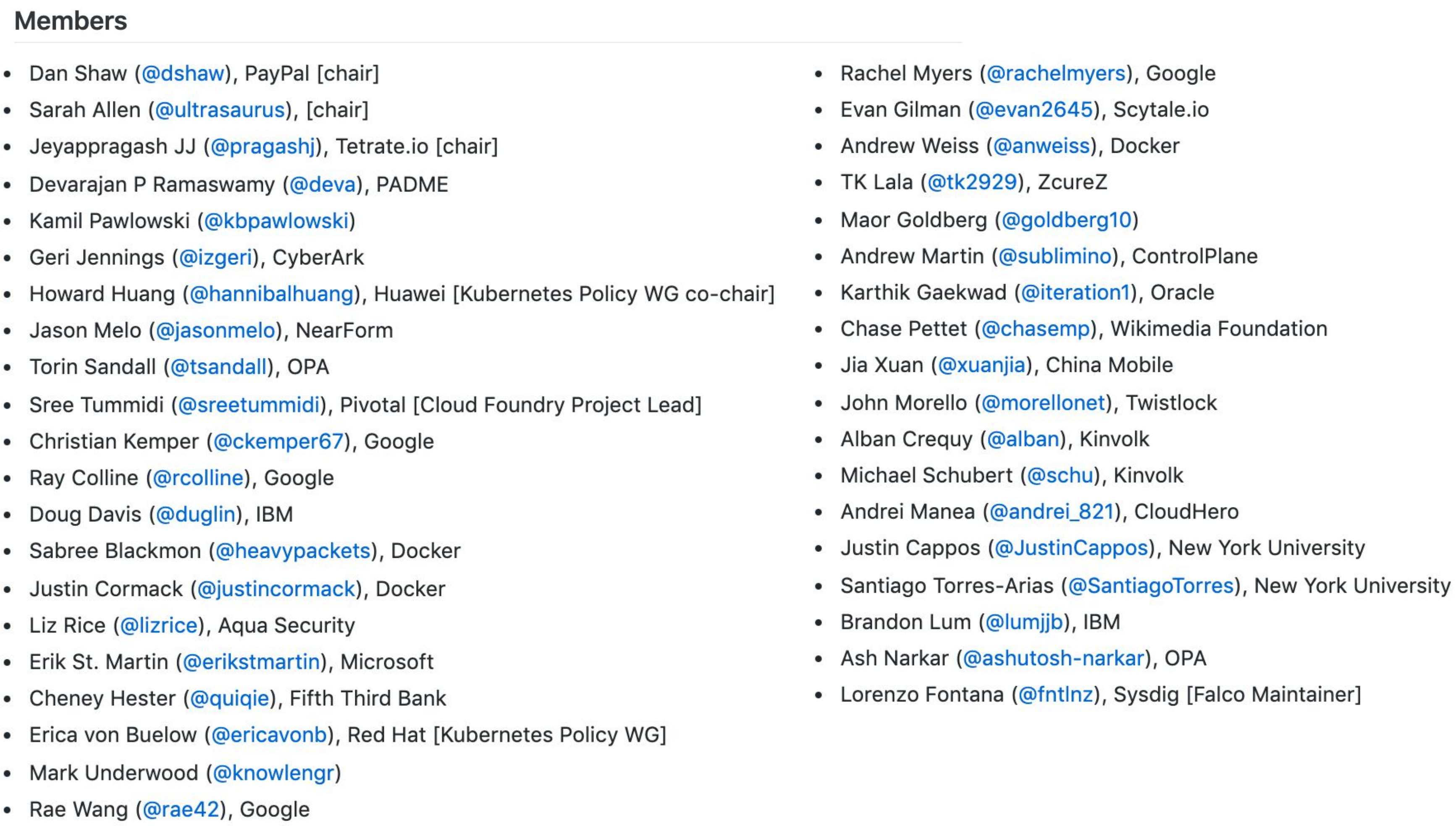
PR created for
CNCF consideration

15 Apr 2019

Rename to
CNCF SIG-Security

7 May 2019

Updated Charter and
Governance



Members

- Dan Shaw (@dshaw), PayPal [chair]
- Sarah Allen (@ultrasaurus), [chair]
- Jeyappragash JJ (@pragashj), Tetrate.io [chair]
- Devarajan P Ramaswamy (@deva), PADME
- Kamil Pawlowski (@kbpawlowski)
- Geri Jennings (@izgeri), CyberArk
- Howard Huang (@hannibalhuang), Huawei [Kubernetes Policy WG co-chair]
- Jason Melo (@jasonmelo), NearForm
- Torin Sandall (@tsandall), OPA
- Sree Tummidi (@sreetummidi), Pivotal [Cloud Foundry Project Lead]
- Christian Kemper (@ckemper67), Google
- Ray Colline (@rcolline), Google
- Doug Davis (@duglin), IBM
- Sabree Blackmon (@heavypackets), Docker
- Justin Cormack (@justincormack), Docker
- Liz Rice (@lizrice), Aqua Security
- Erik St. Martin (@erikstmartin), Microsoft
- Cheney Hester (@quiqie), Fifth Third Bank
- Erica von Buelow (@ericavonb), Red Hat [Kubernetes Policy WG]
- Mark Underwood (@knowlengr)
- Rae Wang (@rae42), Google
- Rachel Myers (@rachelmyers), Google
- Evan Gilman (@evan2645), Scytale.io
- Andrew Weiss (@anweiss), Docker
- TK Lala (@tk2929), ZcureZ
- Maor Goldberg (@goldberg10)
- Andrew Martin (@sublimino), ControlPlane
- Karthik Gaekwad (@iteration1), Oracle
- Chase Pettet (@chasemp), Wikimedia Foundation
- Jia Xuan (@xuanjia), China Mobile
- John Morello (@morellonet), Twistlock
- Alban Crequy (@alban), Kinvolk
- Michael Schubert (@schu), Kinvolk
- Andrei Manea (@andrei_821), CloudHero
- Justin Cappos (@JustinCappos), New York University
- Santiago Torres-Arias (@SantiagoTorres), New York University
- Brandon Lum (@lumjjb), IBM
- Ash Narkar (@ashutosh-narkar), OPA
- Lorenzo Fontana (@fntlnz), Sysdig [Falco Maintainer]

Security Assessments

Goals

High level security review

- Do goals / limitations make sense?
- Does the project use reasonable development practices?
- Are there concerns about how the project may be used?

Template PR#125

Provide guidance to project, TOC, and potential users

An independent, detailed security (code) audit will follow later

Security Assessments (#167)

Priority order

#1: security software

#2: influence security patterns

#3: other projects

“Completed” (unofficially)

TUF, Notary, SPIFFE, SPIRE

In Progress

*in-toto assessment #1

OPA assessment #2

Upcoming

Falco

*Keycloak

+non-security project(?)

Security Knowledge Sharing

Helping project selection

When should you use a project?

What are the security limitations?

What are deployment best practices?

What “in-the-wild” analyzes have been done on a project’s security?

What gaps exist?

How do we improve cloud native security?

Where do we need to add security projects?

How do we improve existing projects?

Audited projects

Solutions to problems	One line tag
Securing software installation/update: TUF/Notary	One time setup, invisible
Secure introduction/identity: SPIFFE/SPIRE	Cross-platform, simple
General policy management: OPA	Collate / manage policy
Software supply chain security: in-toto	General, verifiable provenance

Wed, May 22
14:00 - 14:35
Inside CNCF Project Security Reviews

sched.co/MPdf

Landscape

What got done

CNCF Landscape review

Categories were proposed

Approach to mapping to categories specified

567 open source projects
40 security-related

Things to do

- Validate landscape

(lots of debate / discussion)

Other Security SIG efforts

Expertise

Specialized, security sensitive issues

Crypto, TOCTTOU, etc.

Tooling

Collect, document, and recommend security testing tools / techniques

Security Awareness

Whitepaper (#138), policy doc

Accessible communication

Outreach

Join: **#sig-security**

Solicit community feedback

learn more...

github.com/cncf/sig-security

Wed, May 22

14:00 - 14:35

Inside CNCF Project Security Reviews

Justin Cormack, Docker

sched.co/MPdf

Cloud Native Policy

What is Cloud Native Policy

- Goes beyond auditing/compliance
- Automates Security
- Different from config (not really declarative only with config)
- End-to-end abstraction
- Bring liveness to a cloud that human could talk to

Policy != Config

History

CNCF SAFE Working Group Proposal

Secure Access for Everyone (SAFE) Working Group will explore secure access, policy control and safety for operators, administrators, developers, and end-users across the cloud native ecosystem.

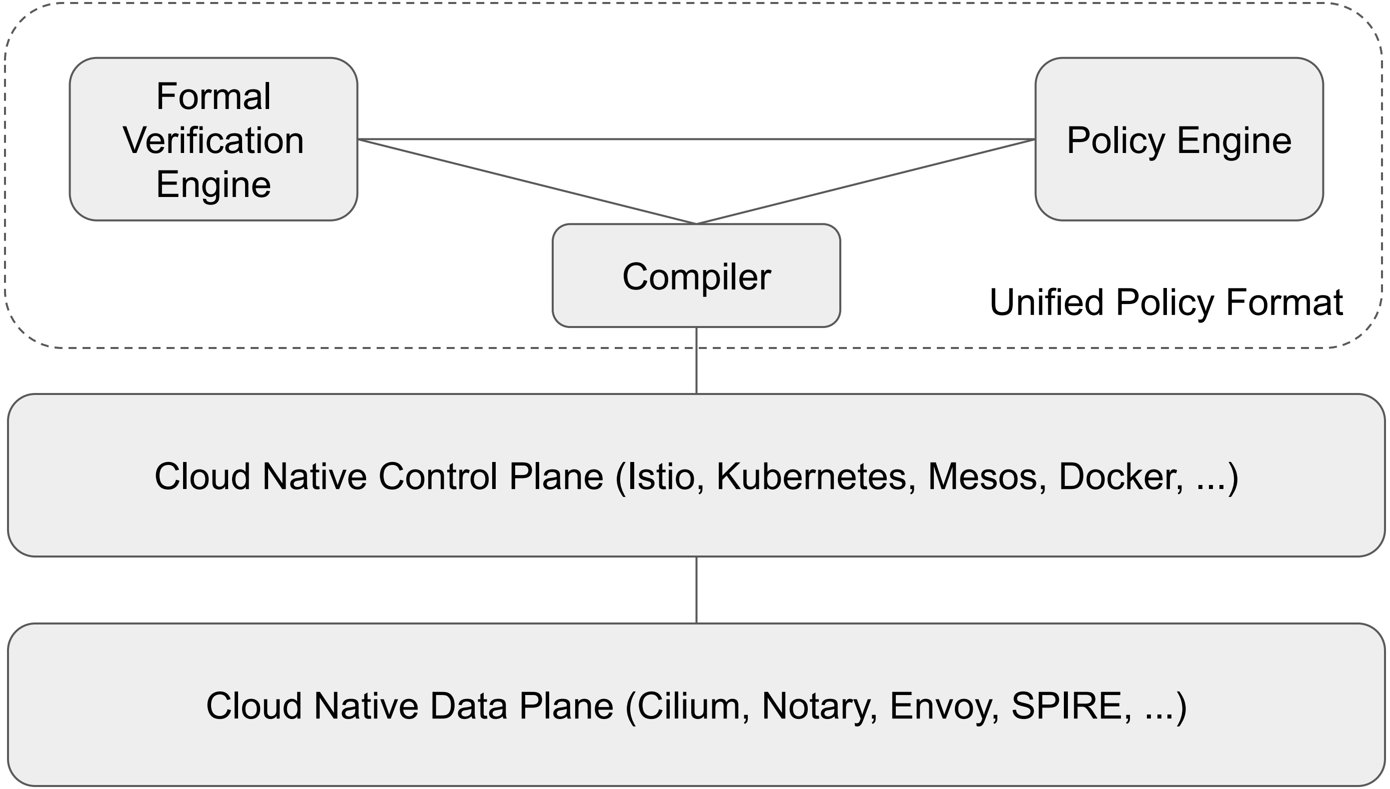
- SAFE WG + *Proposed* CNCF Policy WG = CNCF SAFE WG
- Members from:

synchrony
Google
HUAWEI
Microsoft
Styra
Fifth Third Bank
SCYTALE
Tetrate
redhat
IBM
Pivotal
Cloud Foundry
nearForm
docker
CYBERARK
aqua
NYU

Motivation

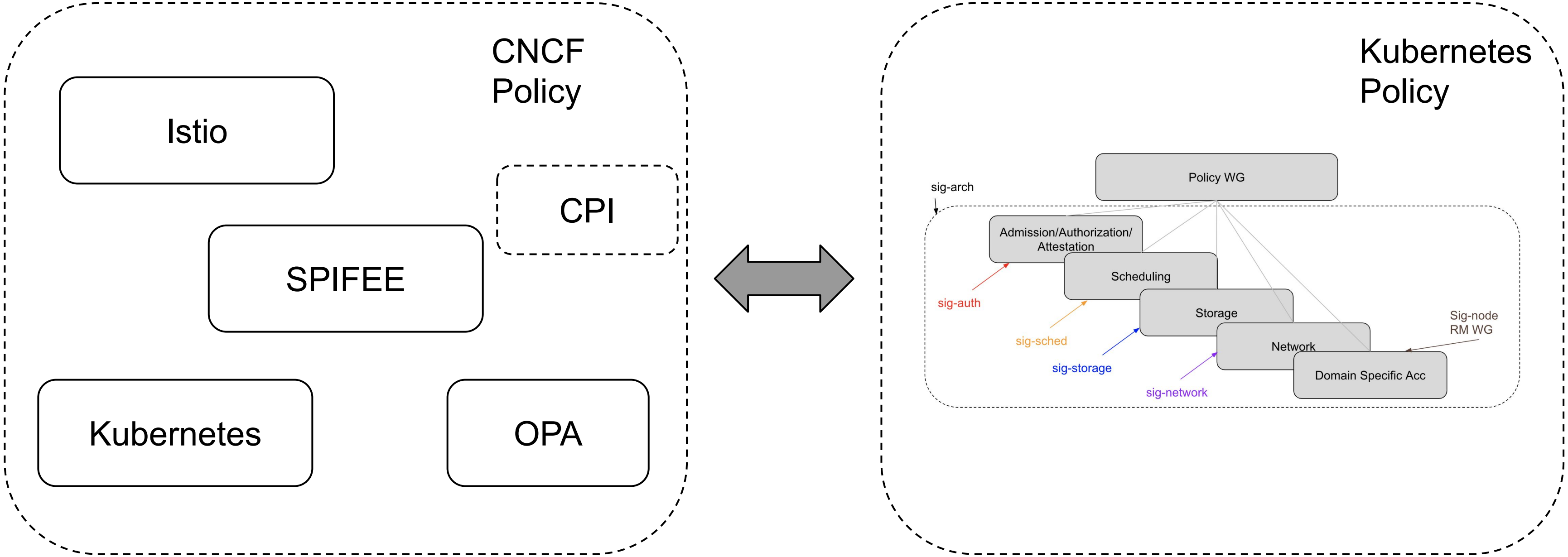
- Policy are needed and designed all over the place
- Policy description are domain specific in nature:
  - Not only in the sense Brian G meant (Kubernetes' domain), but also in a larger context of usage (audit, security, storage, network, AI...), vertical adoption (finance, telco, pharma,...), languages, ...
  - Usually out of scope for SIG Work
- Policy semantic and control mechanism is universal
  - Policy semantic: the actual policy content
  - Policy control mechanism: lifecycle of policy itself, and lifecycle of elements defined in policy

Overview


Formal Verification Engine
Policy Engine
Compiler
Unified Policy Format
Cloud Native Control Plane (Istio, Kubernetes, Mesos, Docker, ...)
Cloud Native Data Plane (Cilium, Notary, Envoy, SPIRE, ...)

Semantic + Control = Architecture

Overview



Approach: Top down discussion

Approach: Bottom up discussion

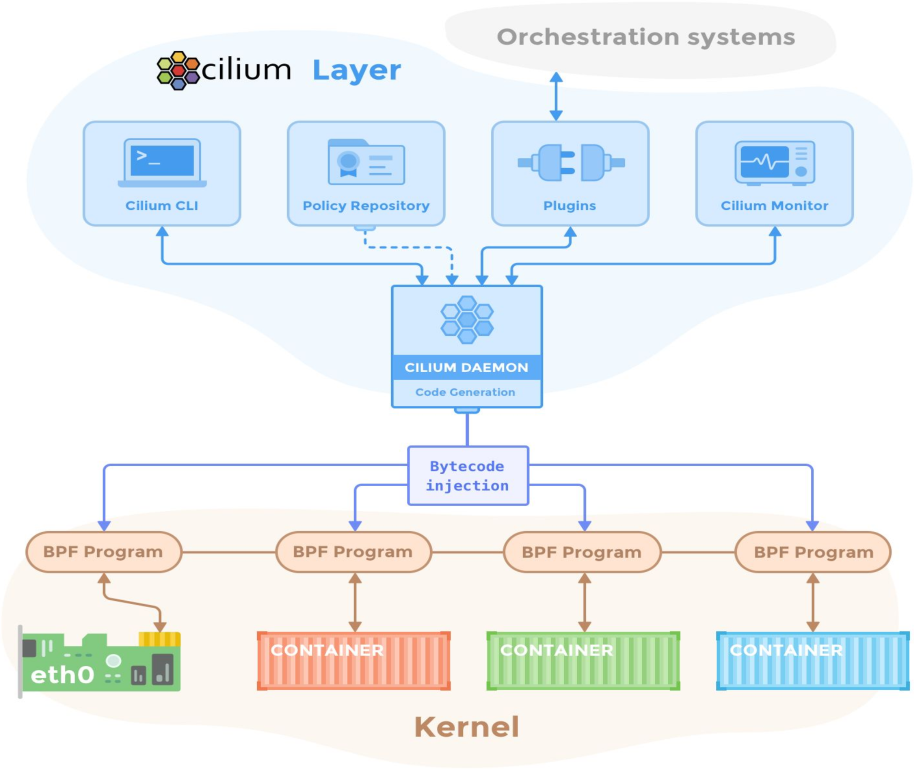
Overview

- Deliverable - Cloud Native Policy Whitepaper
    - Define the overall cloud native policy architecture
    - Case study to identify requirements and gaps
    - Specific long term research topics
    - Reference implementations

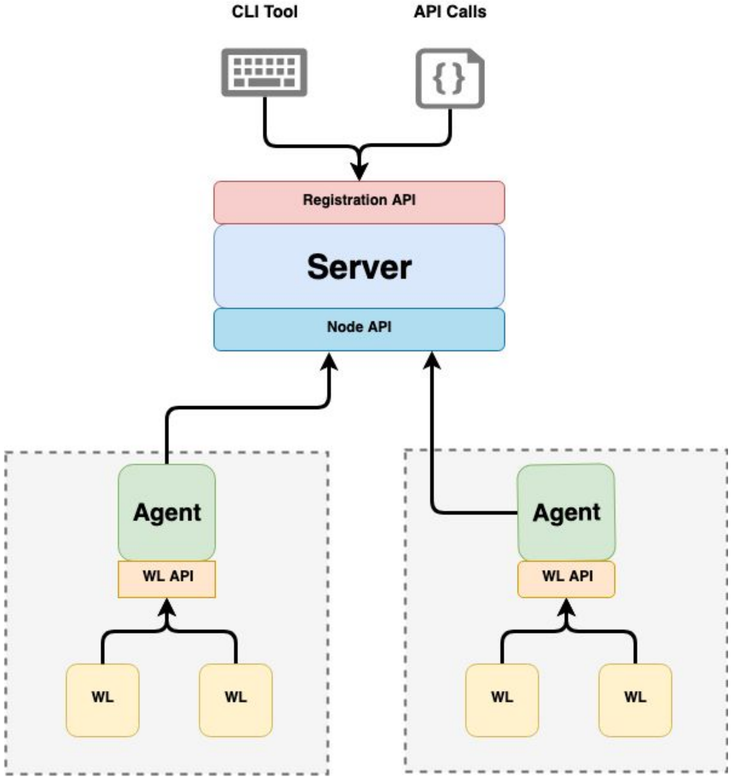
Policy Case Studies

- Case Study So Far:
  - Kubernetes (Storage, Multi-tenancy, Network)
  - OPA Gatekeeper
  - Istio Security Policy
  - Cilium
  - SPIFEE/SPIRE
  - TUF/Notary/In-Toto/Uptane
- https://docs.google.com/document/d/1StDYW1zHVSF1Qswk0ScsyKw766AbAHOikyCNtqCsMMY/edit#heading=h.40fpl0da5vi4

Policy Case Studies - Cilium



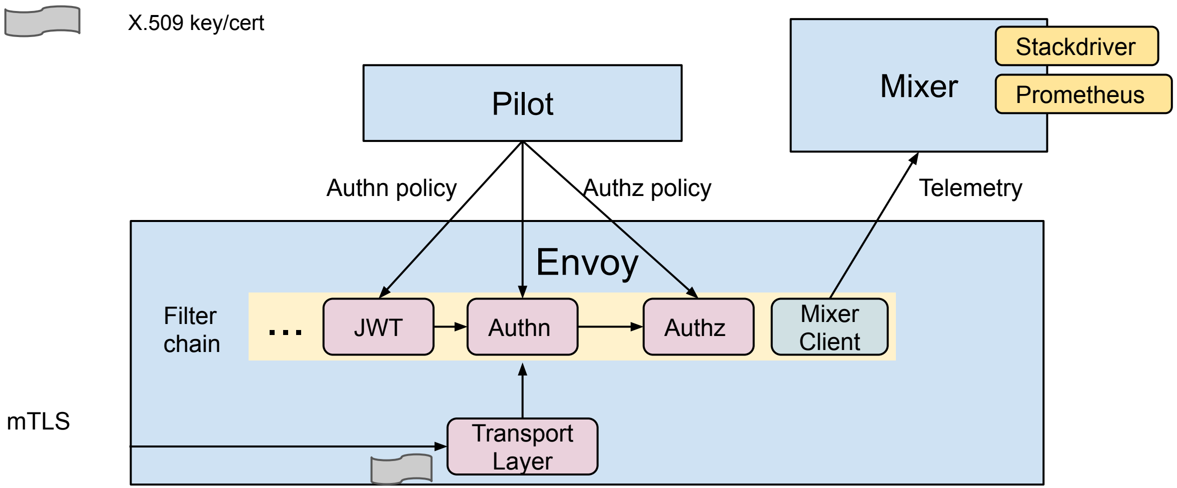
Policy Case Studies - SPIFFE/SPIRE



Policy Case Studies - TUF/Notary and In-toto

- The Update Framework provides a specification of metadata system which could help secure the packaging of software. Notary is the golang implementation of TUF. In-toto is the supply chain security framework,
- During the case study we found that the main policy related aspect of TUF and its derivatives mostly involves “actions” and “roles”. For example there will be possible policy enforcement point needed for the revocation action in TUF/Notary/In-toto, or to have policy action semantic defined for In-toto concept of “Artifact Rules” such as MATCH and CREATE , or policy defined for In-toto layout (especially for multiple layouts).

Policy Case Studies - Istio



Policy Case Studies - Summary

- There is a trend for having standalone defined policy objects such as AuthorizationPolicy, AuthenticationPolicy, SchedulingPolicy, instead of having fragments of policy in some other configuration
- The policy objects should have various verbs which reflects the desired action (CREATE, RECLAIM, ALLOW, DENY, MATCH...), the reason for having a specific verb instead of using ALLOW/DENY for every conceivable condition is mostly about the scalability.
- The policy objects could also have various adverbs which reflects the desired priority (STRONG, PREFERRED, WEAK, MEDIUM,...)
- Together with verbs+adverbs, the policy objects could then effectively provide a typesafe system for cloud native platforms. Policy Engines like OPA will be the entity that checks the type system

Additional Interesting Areas Planned For 2019

- Formal Verification (working with AWS, Styra, ...)
- Policy Type System
- Container Policy Interface

Join the convo

- Feel free to join the weekly meeting or leave a note on the meeting minute doc (https://goo.gl/auTfy2) if you have more interesting items to add !
- Find us at #sig-security on cncf slack channel or #wg-policy on kubernetes slack channel

learn more...

github.com/cncf/sig-security

Thur, May 23

11:05 - 12:30

Kubernetes Policy WG Deep Dive

Zhipeng Huang, Erica Von Buelow

Hall 8.0 E9