Scrutinizing SPIRE to Sensibly Strengthen SPIFFE Security

Evan Gilman, Matt Moyer

@moyerma
@evan2645

Evan Gilman

Engineer at Scytale

@moyerma
@evan2645

Matt Moyer

Engineer at Heptio

@moyerma
@evan2645

What is SPIFFE?

Secure Production Identity Framework for Everyone

@moyerma
@evan2645

SPIFFE is a specification.

SPIFFE ID

spiffe://example.org/foo

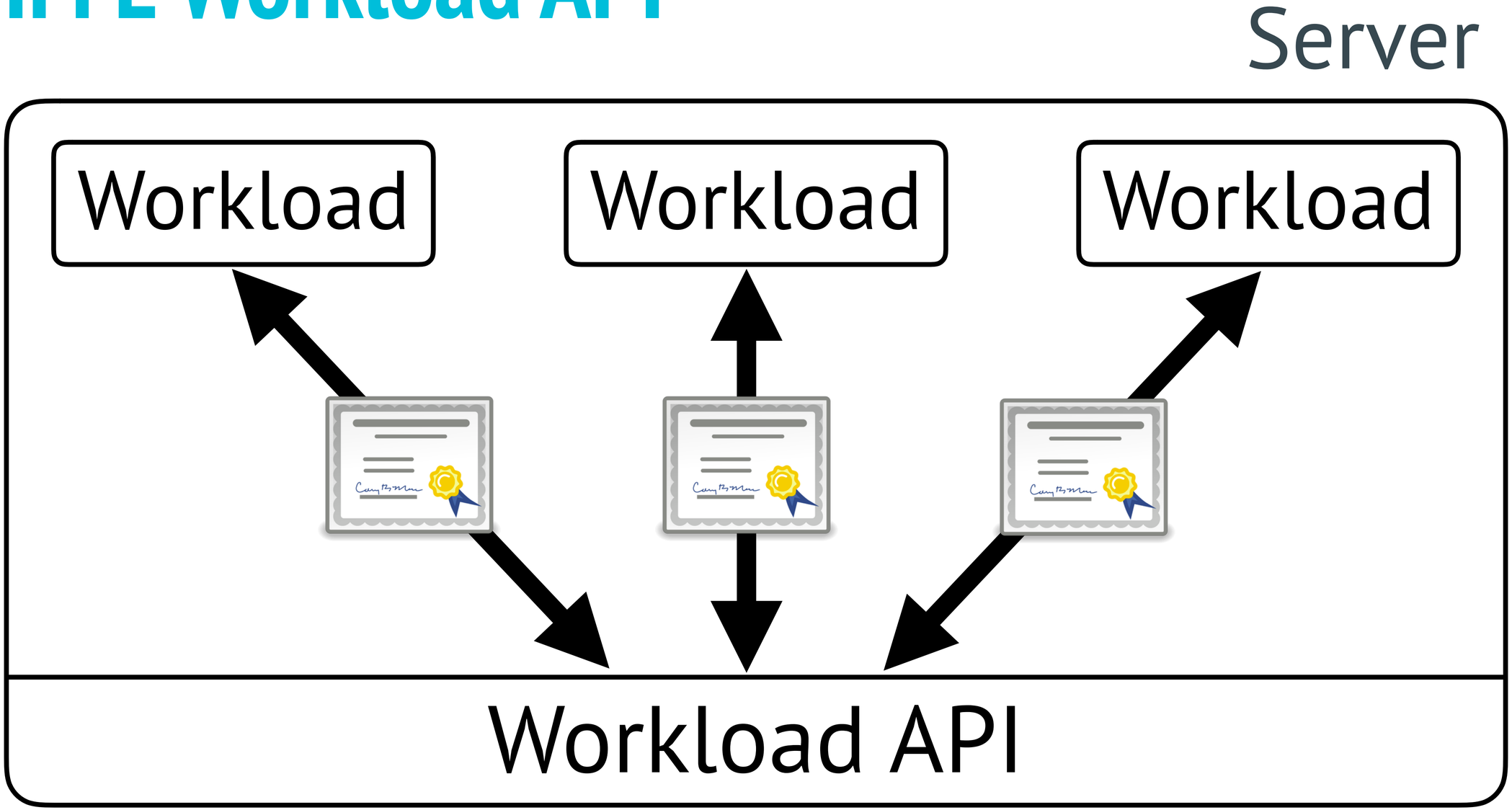
SPIFFE Verifiable Identity Document

spiffe://example.org/foo

@moyerma
@evan2645

SPIRE

SPIFFE Workload API



@moyerma
@evan2645

SPIRE

What is SPIRE?

SPIFFE Runtime Environment

@moyerma
@evan2645

SPIRE is an (open source) implementation.

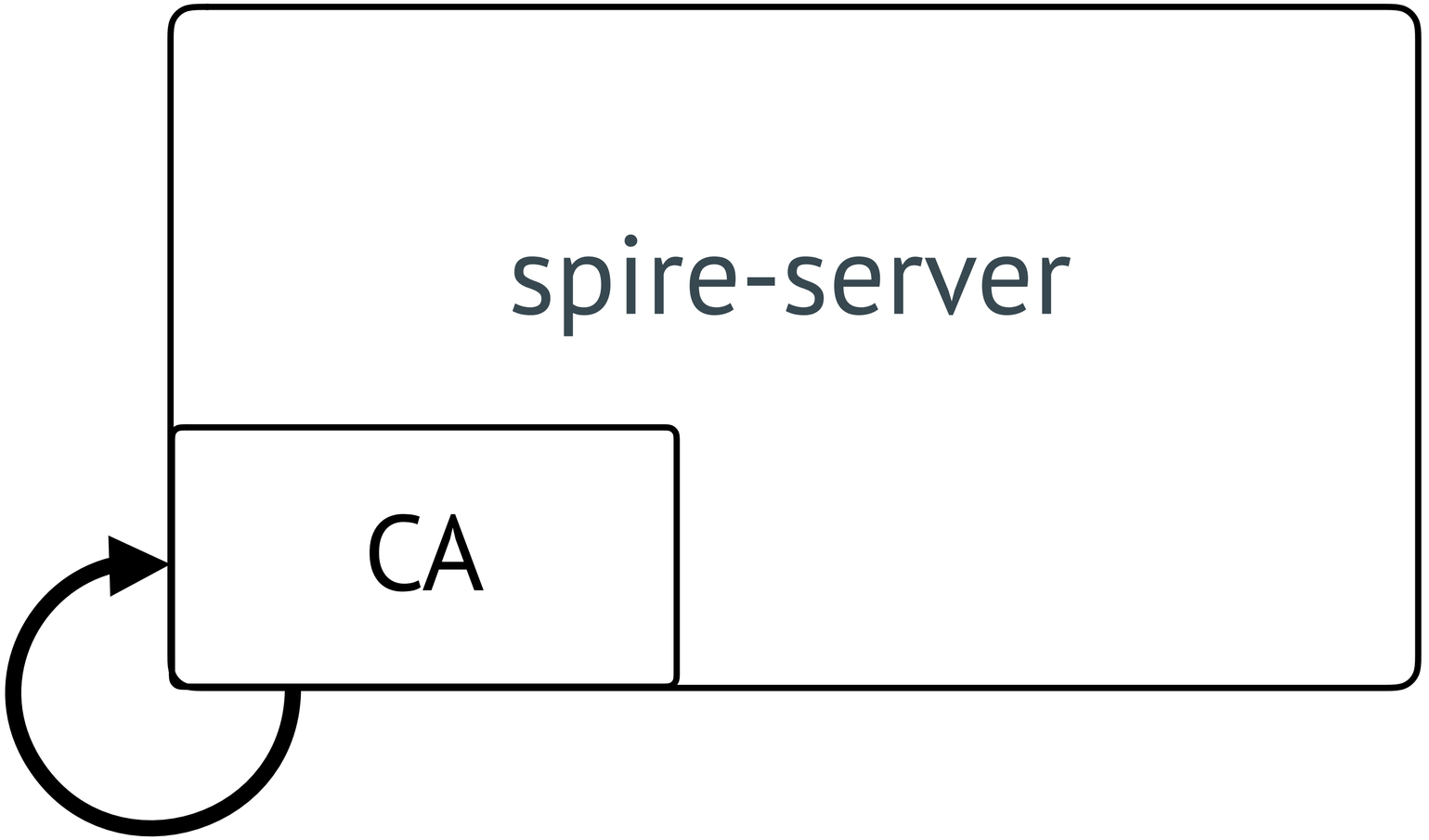
spire-server

- Identity Mapping
- Node Attestation
- SVID Issuance

spire-agent

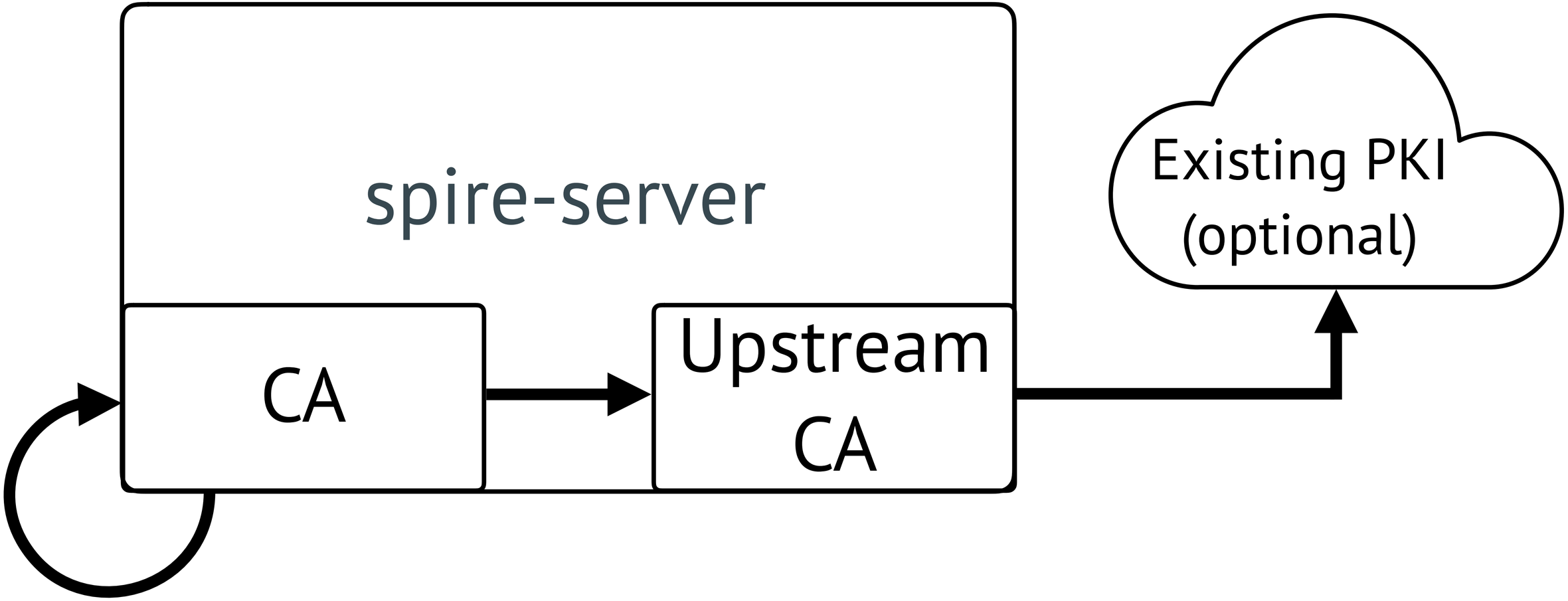
- Workload Attestation
- Workload API

SPIRE Walkthrough



@moyerma
@evan2645

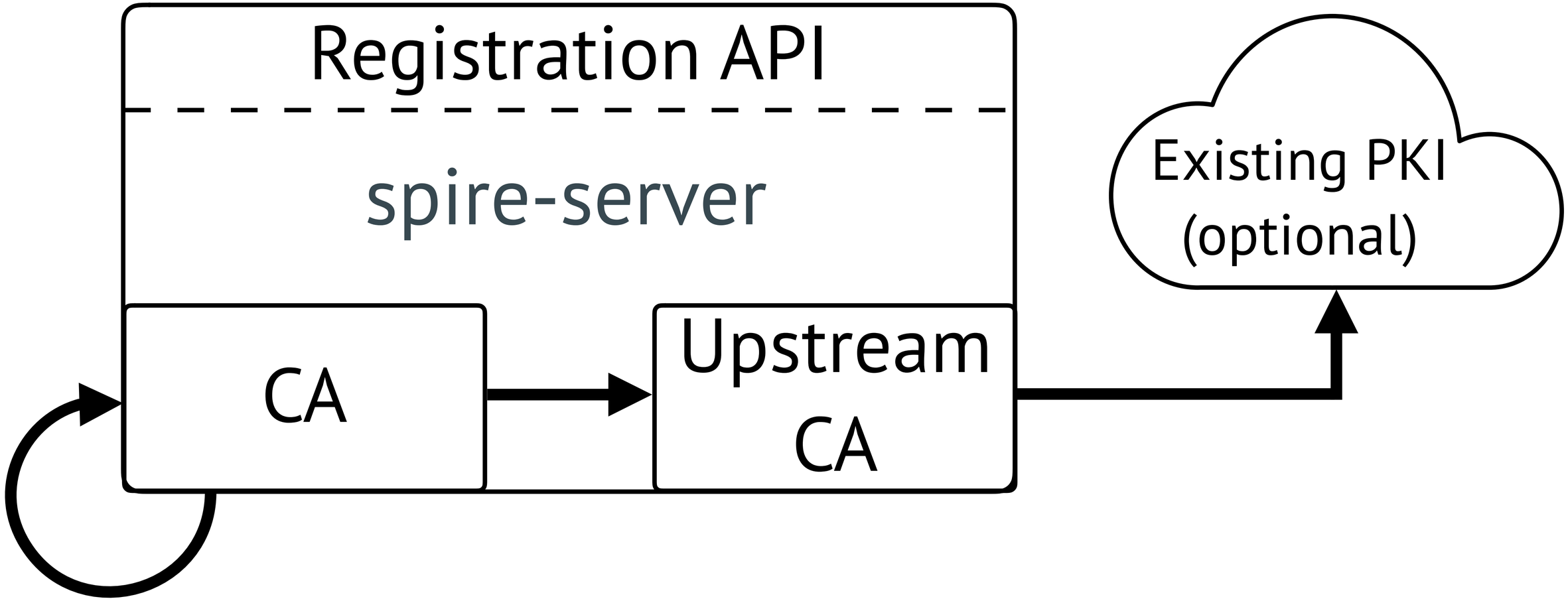
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

SPIRE Walkthrough



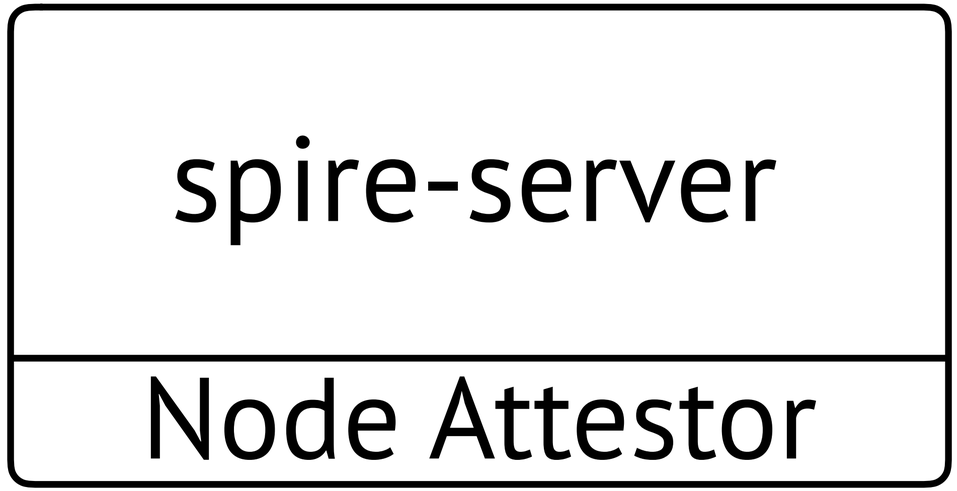
@moyerma
@evan2645

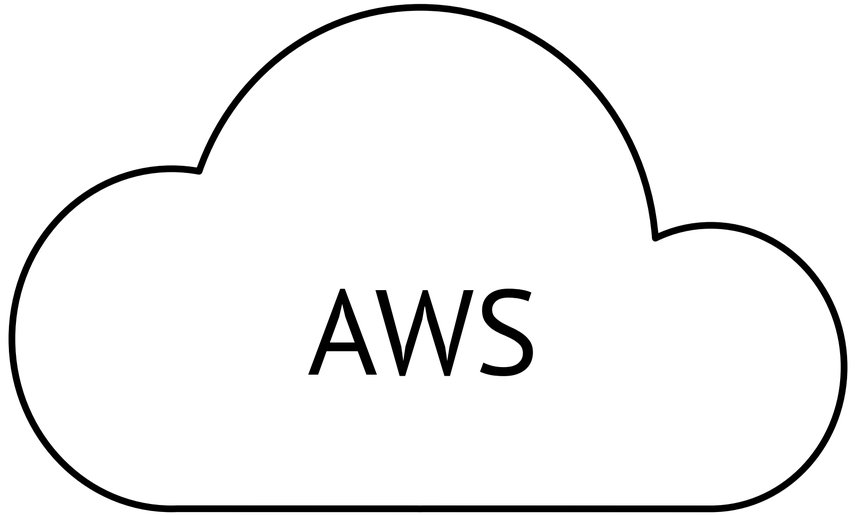
SPIRE

SPIRE Walkthrough

Parent ID:	spiffe://example.org/k8s/cluster/foo
Selector:	k8s:ns:operations
Selector:	k8s:sa:mediawiki
Selector:	docker:image-id:746b819f315e
SPIFFE ID:	spiffe://example.org/ops/wiki

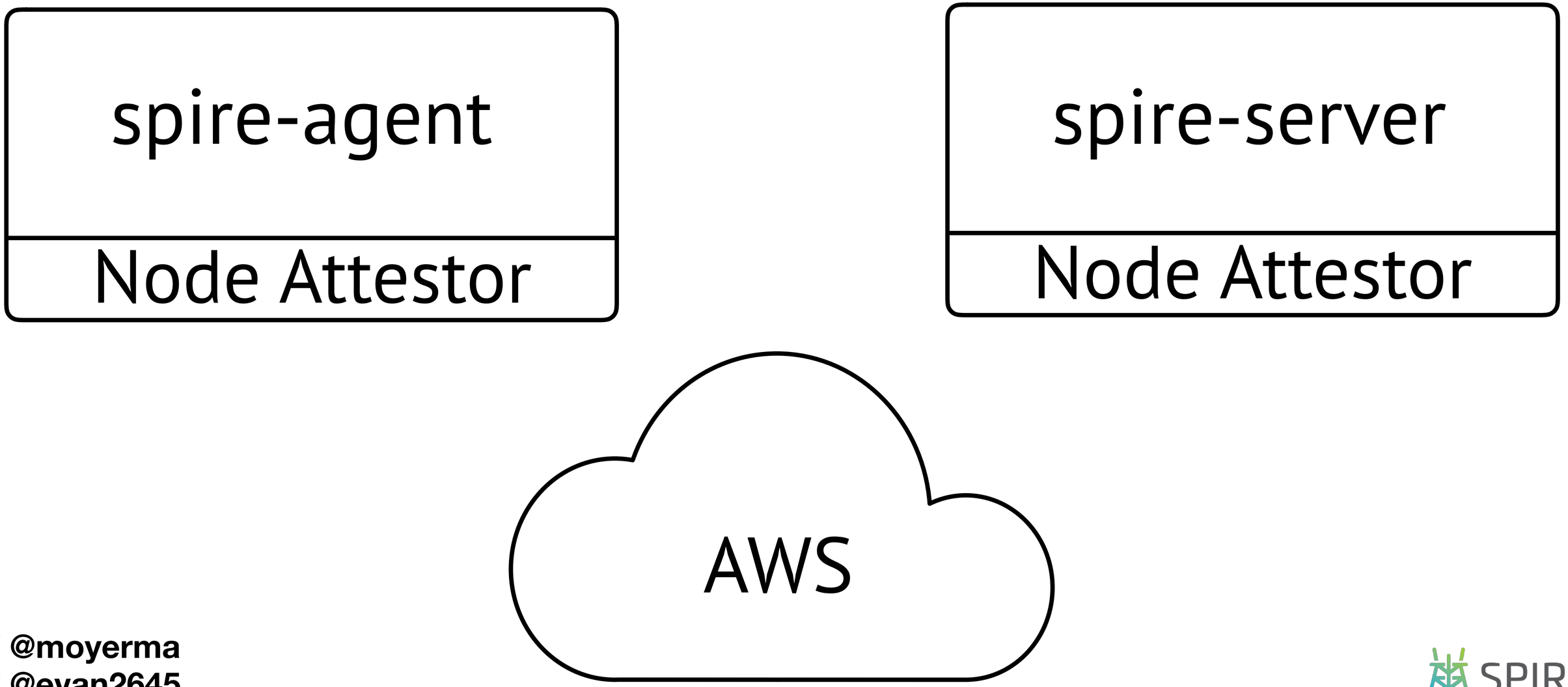
SPIRE Walkthrough





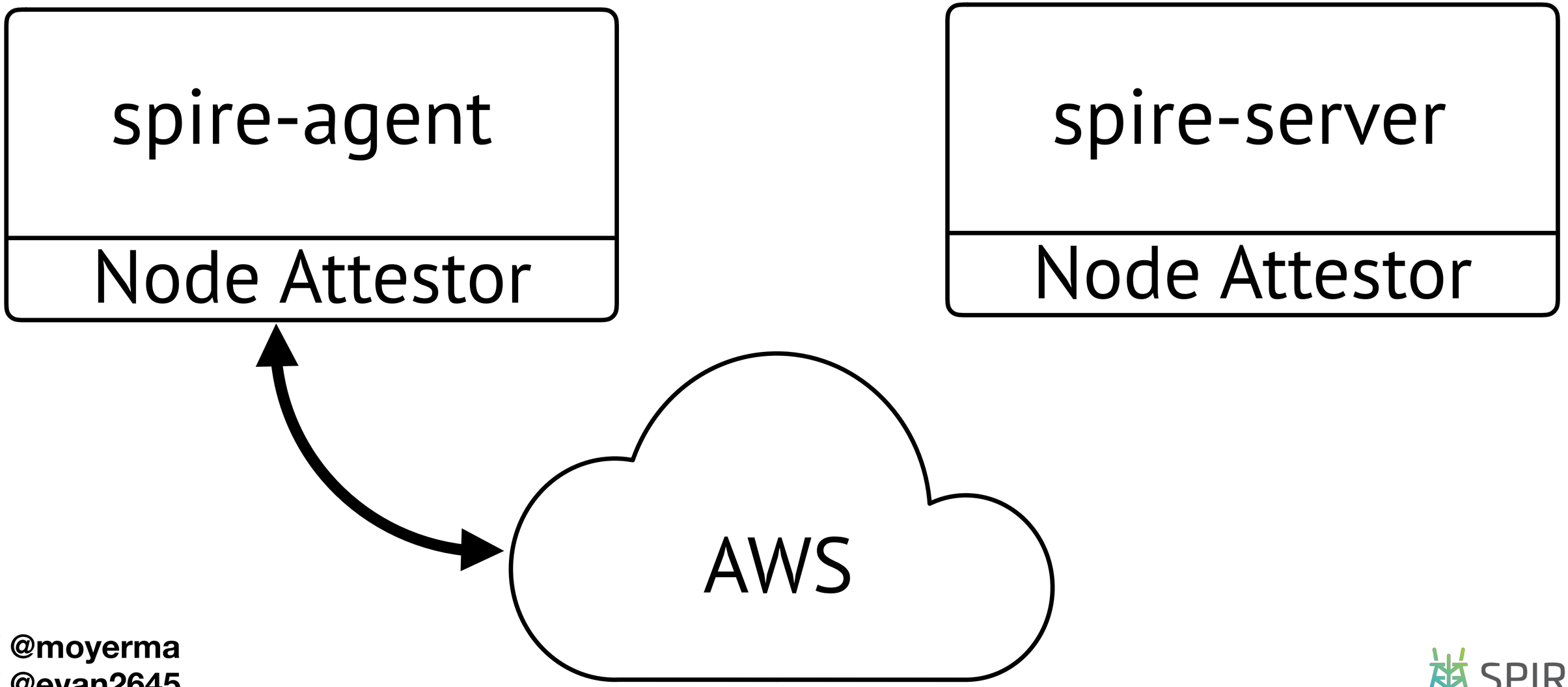
@moyerma
@evan2645

SPIRE Walkthrough



@moyerma
@evan2645

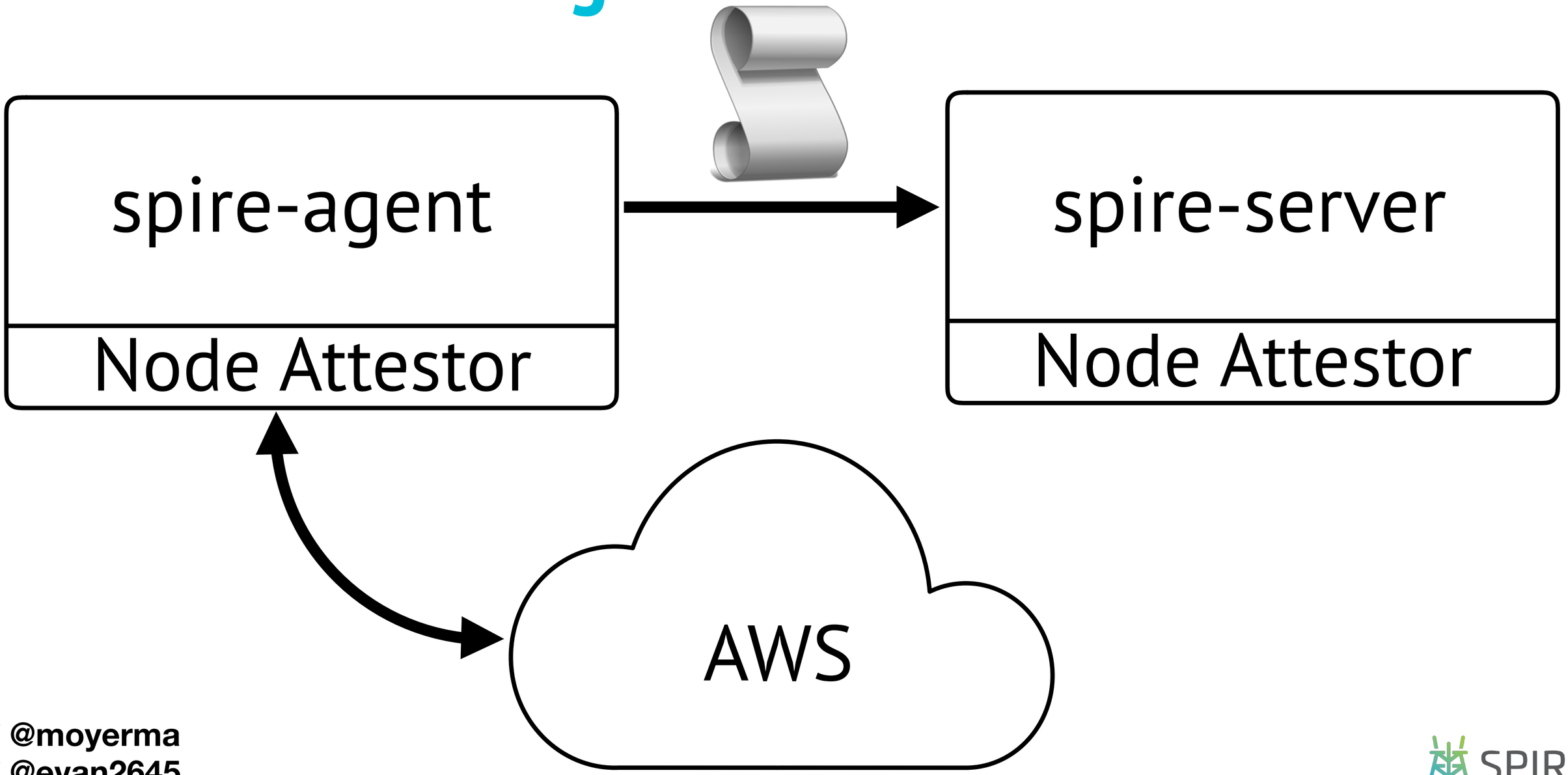
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

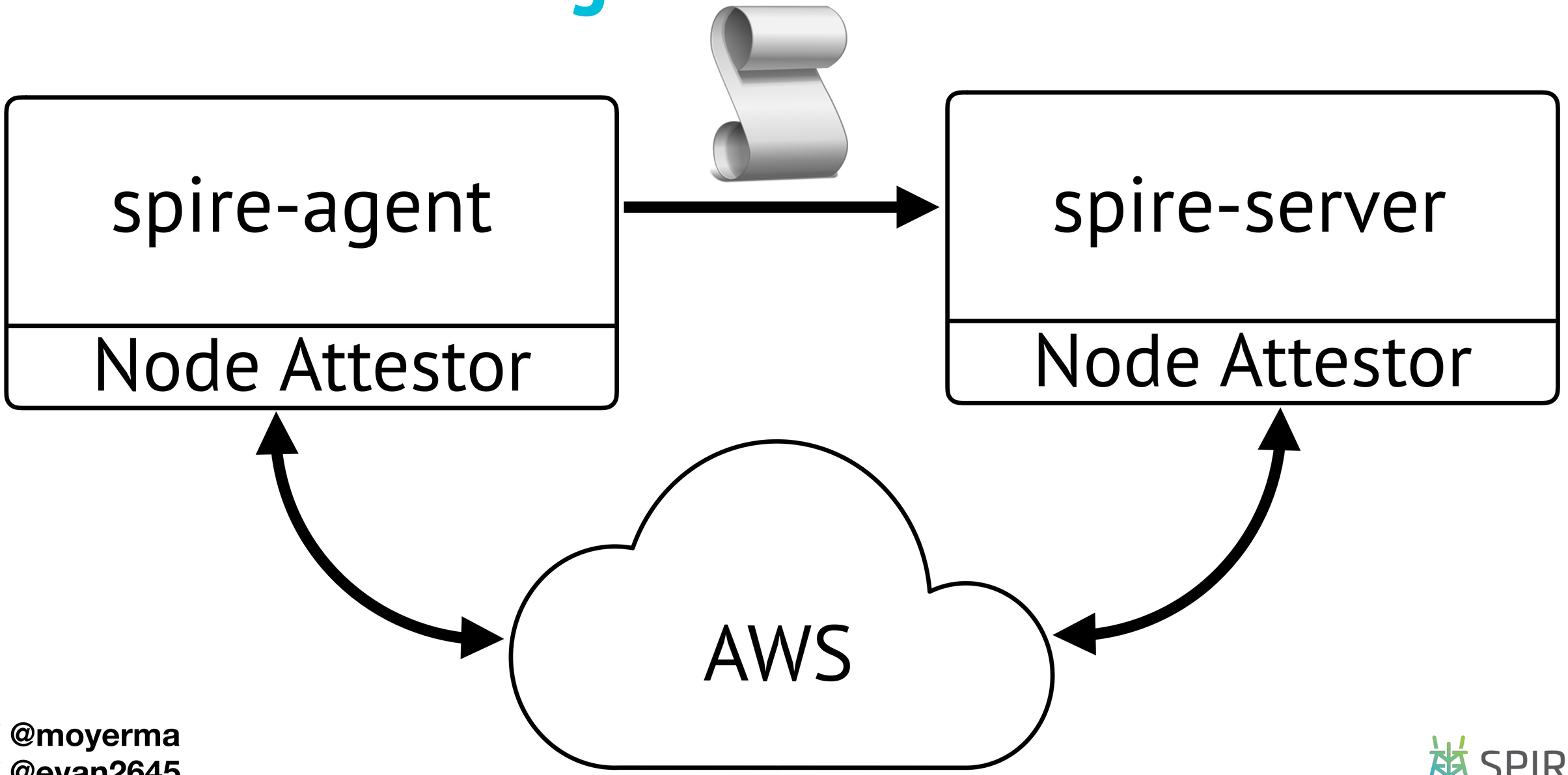
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

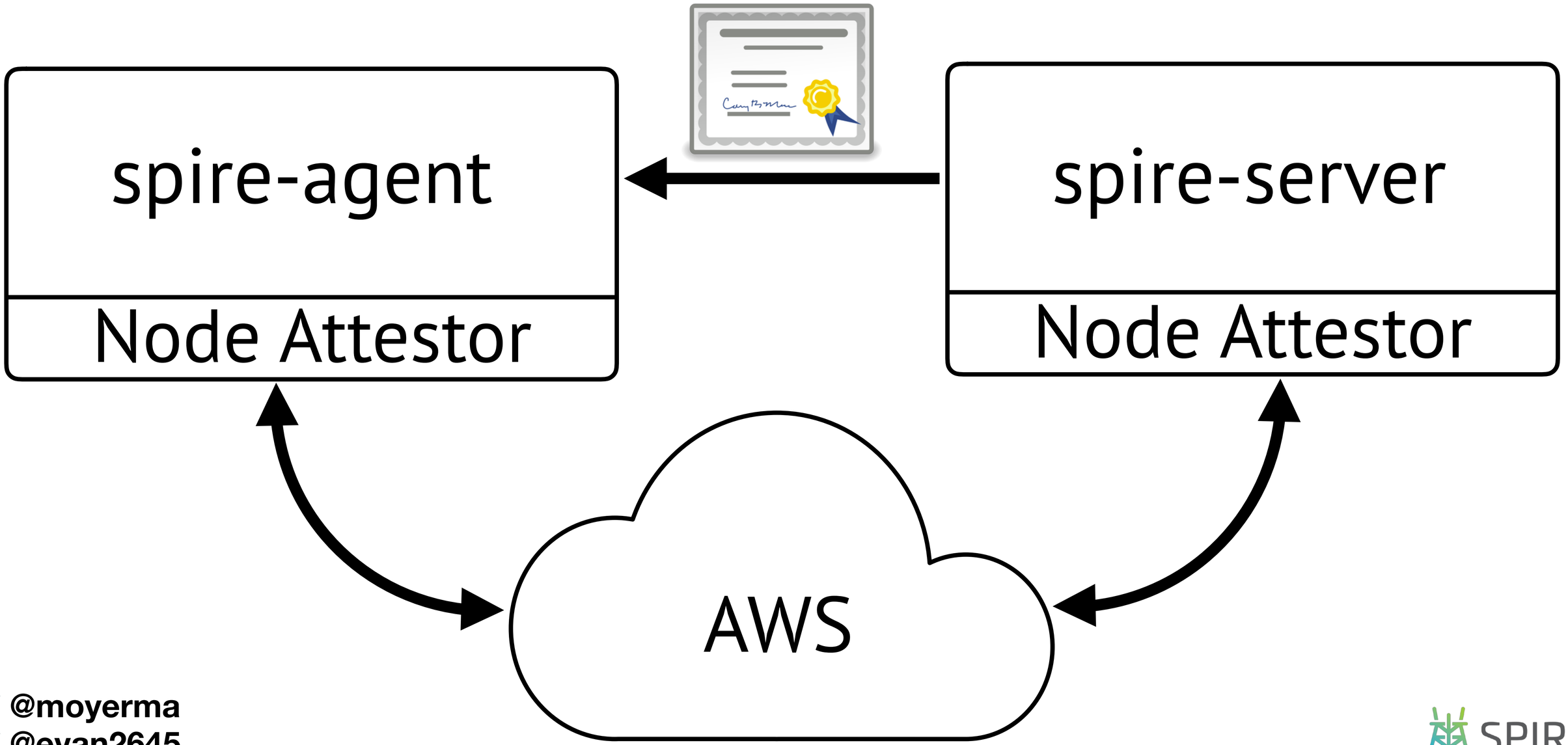
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

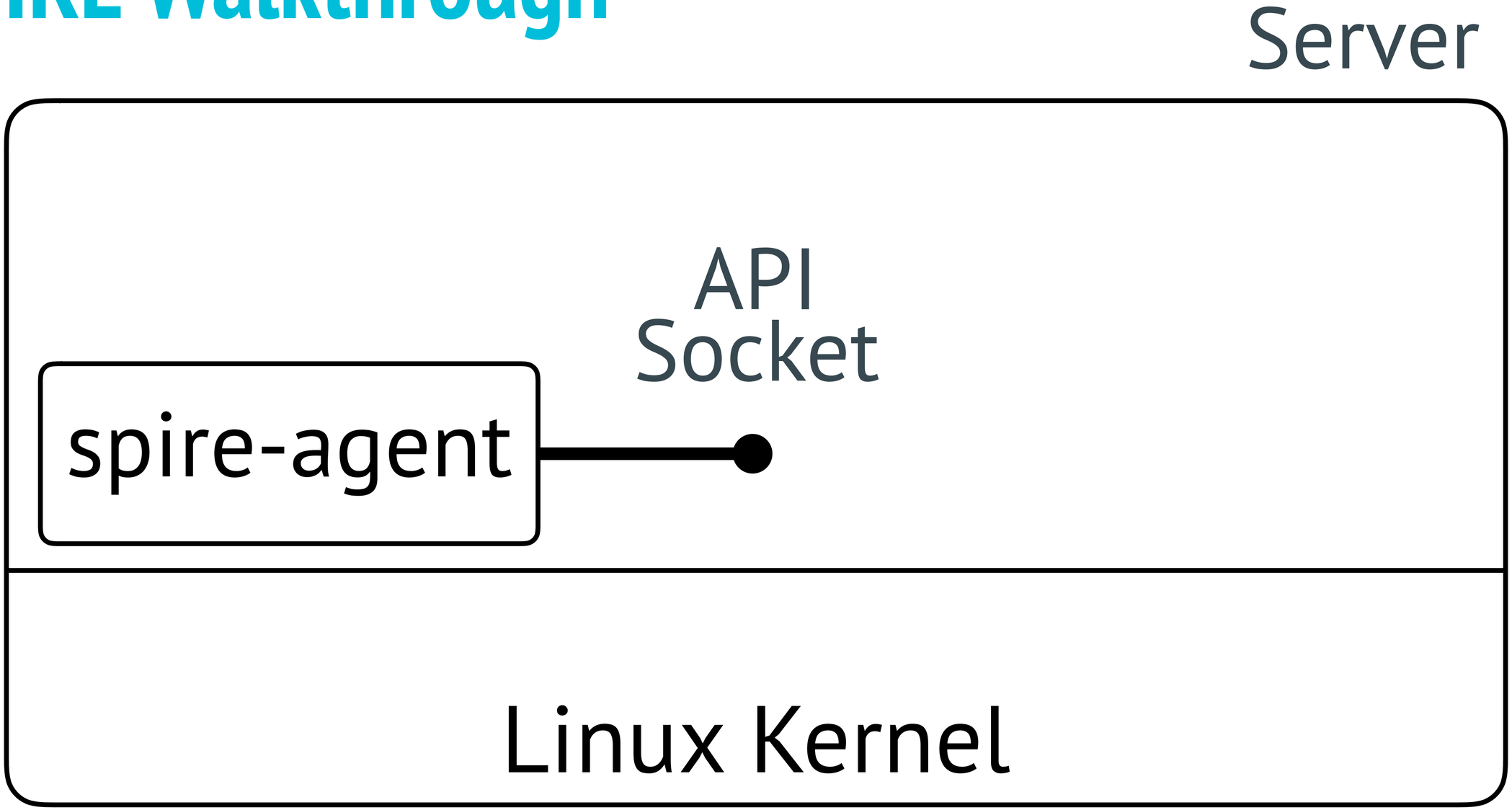
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

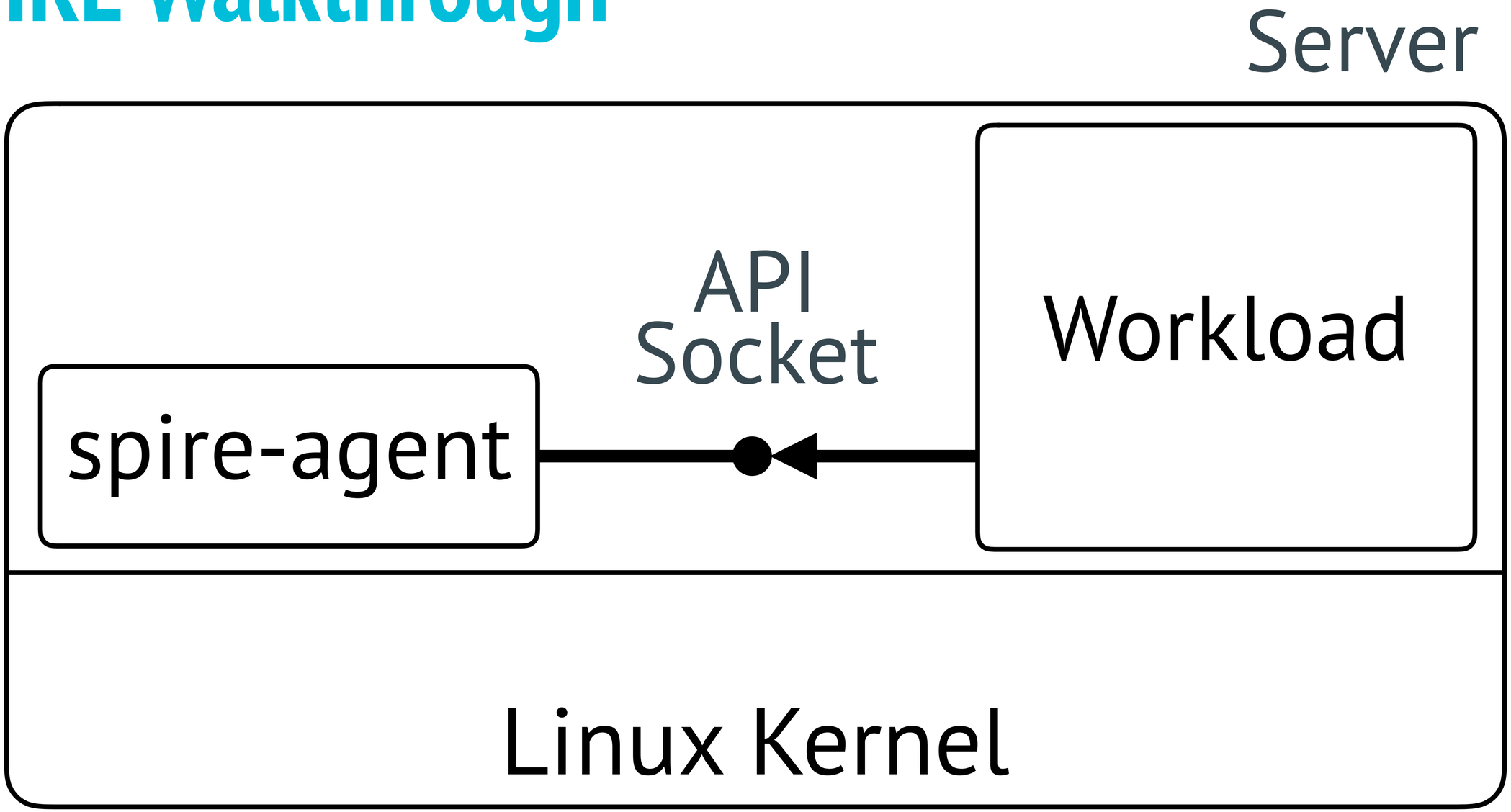
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

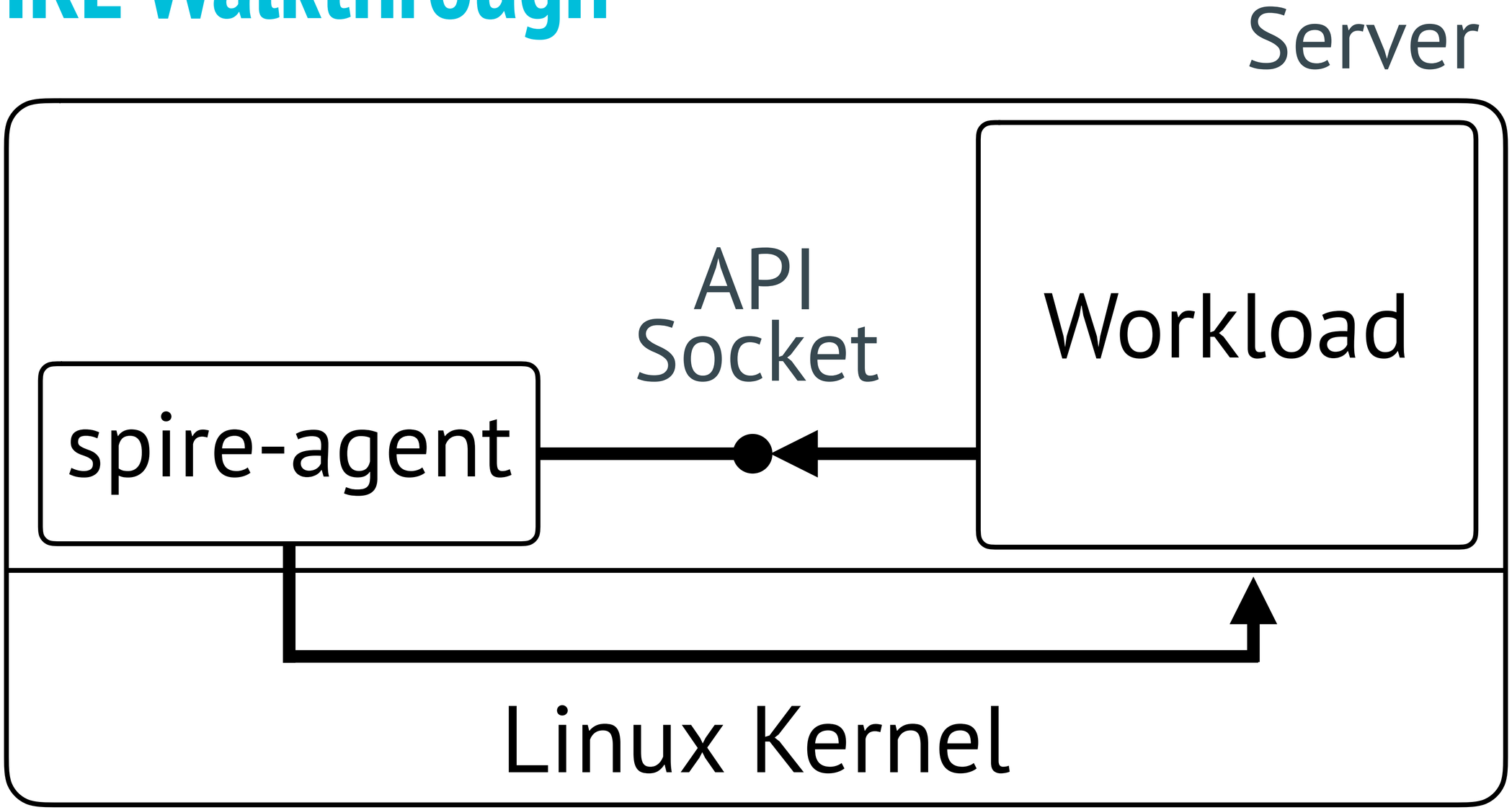
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

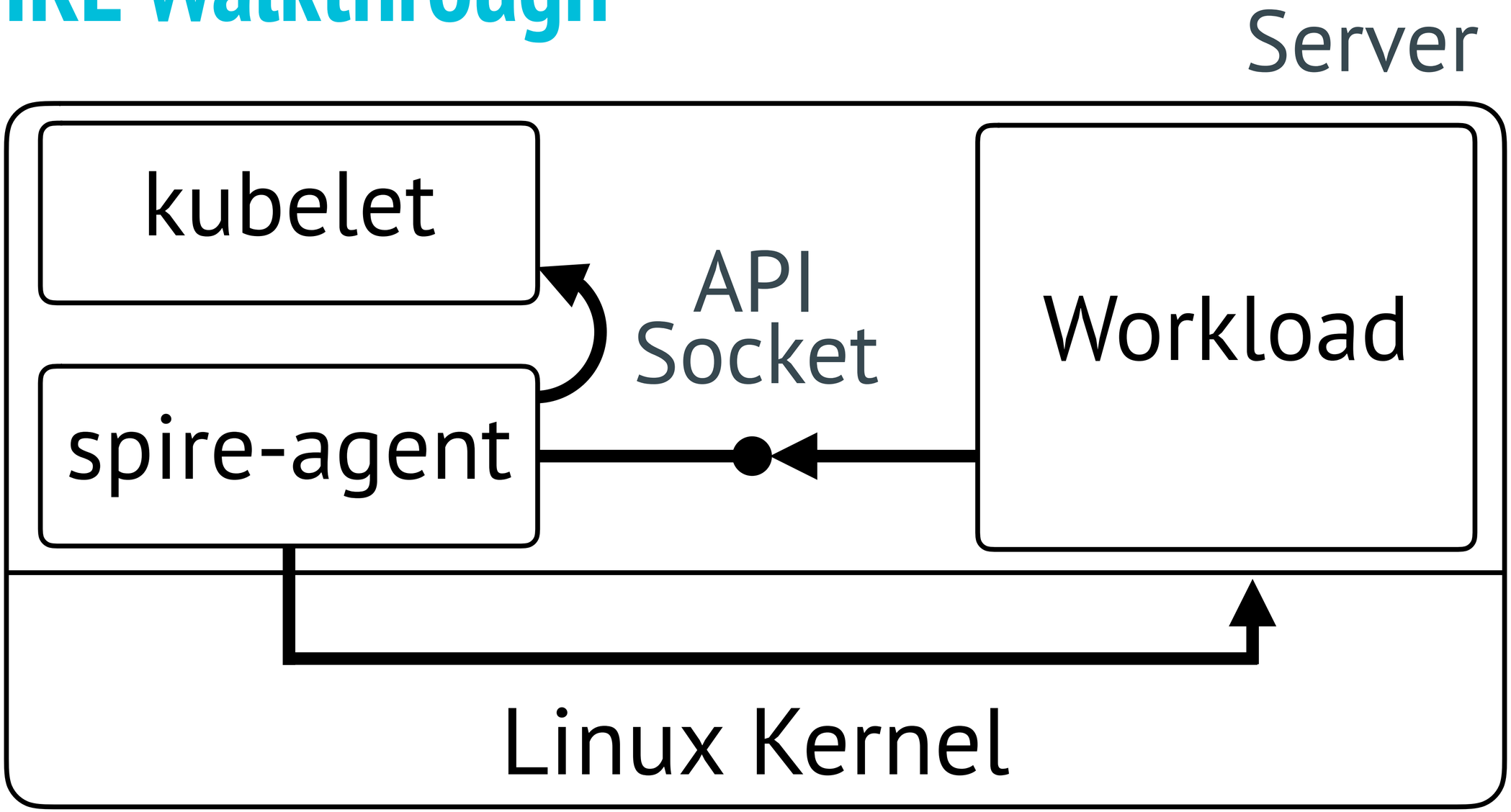
SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

SPIRE Walkthrough



@moyerma
@evan2645

SPIRE

What is this all about?

Community Security Modeling Exercise

- Study SPIRE and describe its security model.

- Kicked off December 2017 in collaboration with:

Justin Cappos (NYU)

Enrico Schiattarella

Goals

1. Understand the expected security properties of a SPIFFE implementation.
2. Explore what vulnerability classes exist in a SPIFFE system.
3. Identify how SPIRE (the implementation) can be improved.
4. Identify how SPIFFE (the specification) can be improved.

Non-Goals

1. Identify specific implementation vulnerabilities in SPIRE.
2. Formally prove anything about SPIFFE/SPIRE.


What security properties
do we expect?

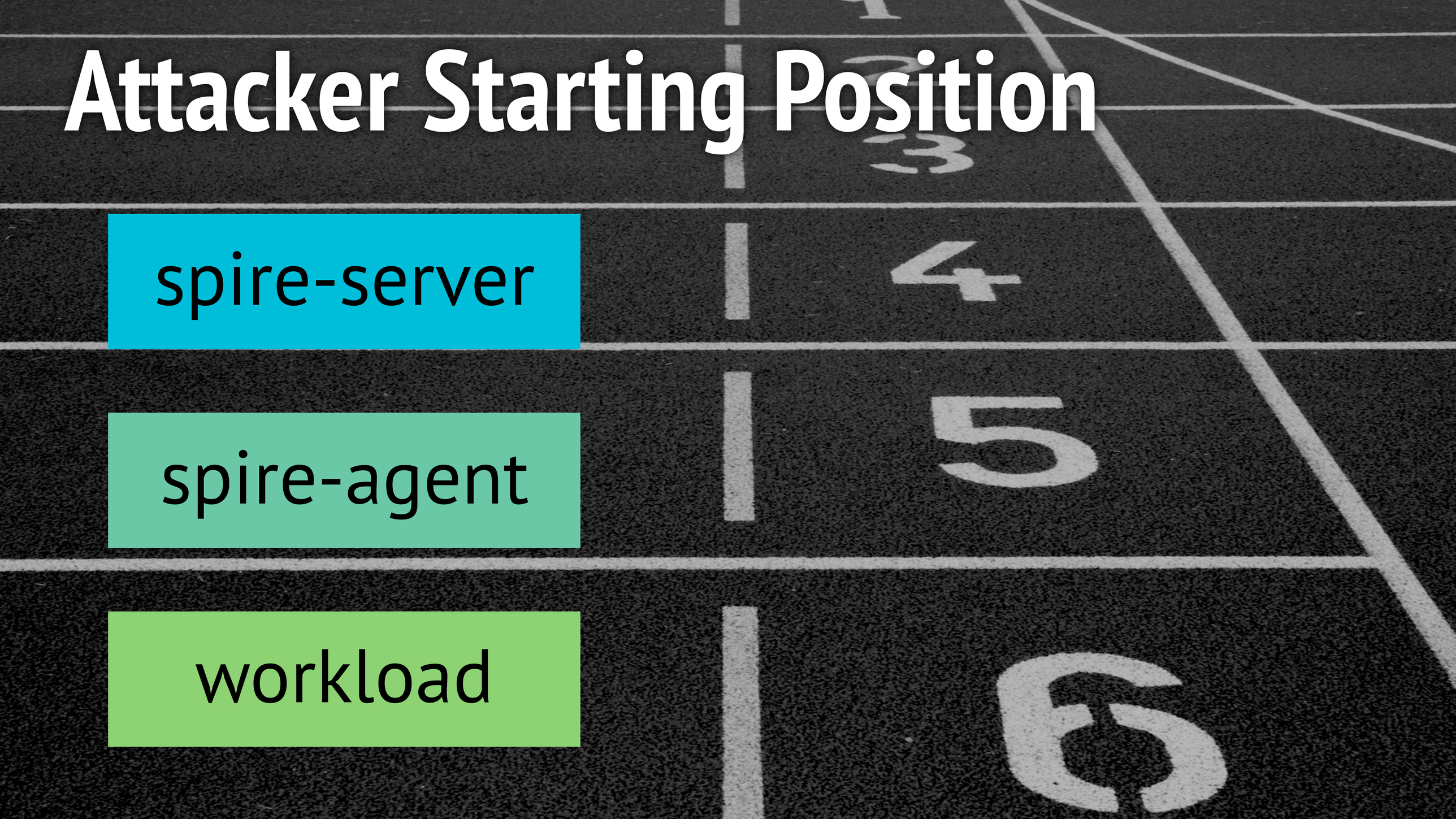
Attacker Goals

- Impersonate a workload, node agent, or server.
- Deny service to workloads or node agents.
- Create a new (forged) identity.

Attacker Goals (cont.)

- Modify permissions associated with an identity.
- Trick a party into using the wrong identity.
- Compromise the software running on a system.

Attacker Starting Position



Attacker Superpowers

- Container escape vulnerability.
- Network-level interception/manipulation capability.
- Malformed certificate or CSR (short of RCE).
- Ability to overwhelm server with requests.

Attacker Superpowers (cont.)

- Remote code execution reachable from…
  - Go CSR parser.
  - Go X.509 certificate parser.
  - Pre-authenticated protocol stack (TLS, HTTP, gRPC)

Attacker Superpowers (cont.)

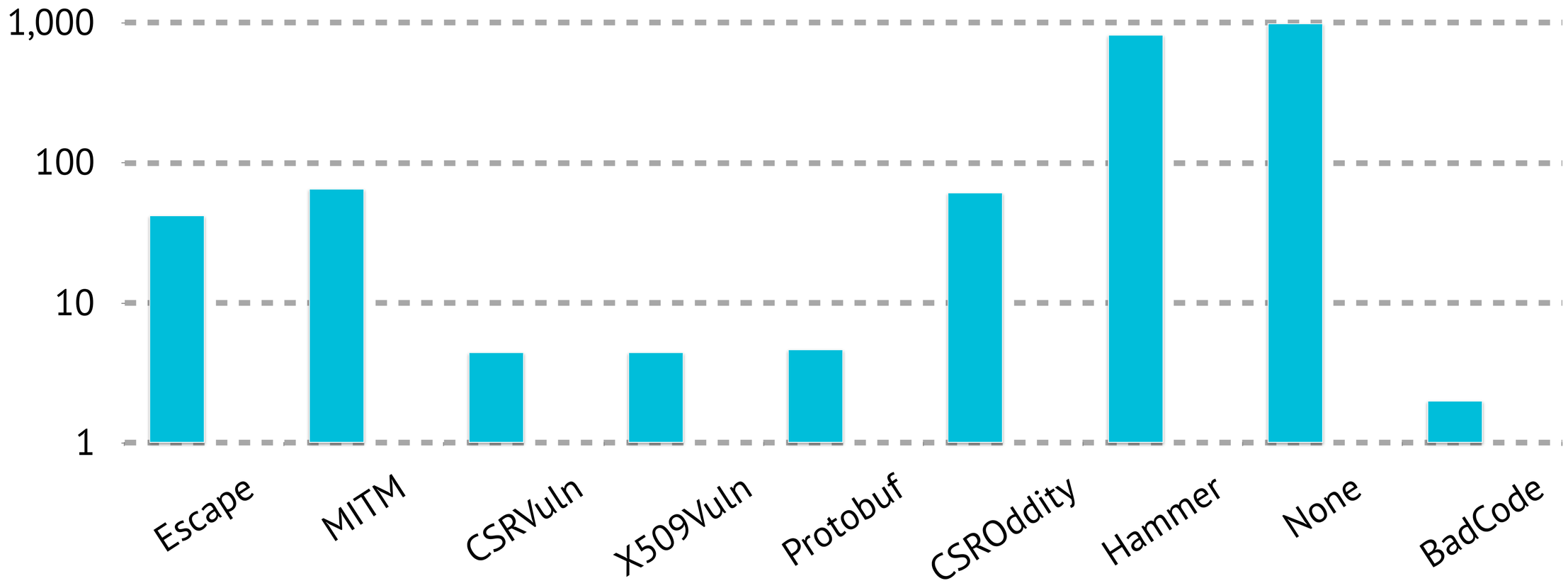
- Exploit for explicitly mitigated problem.

(State) Space Explorers

The Matrix

- We explored combinations of:
  - Attacker Goal
  - Starting Position
  - Victim Component
  - Attacker Capabilities
- This involved a lot of *talking*.
- The results went into a *big spreadsheet*.

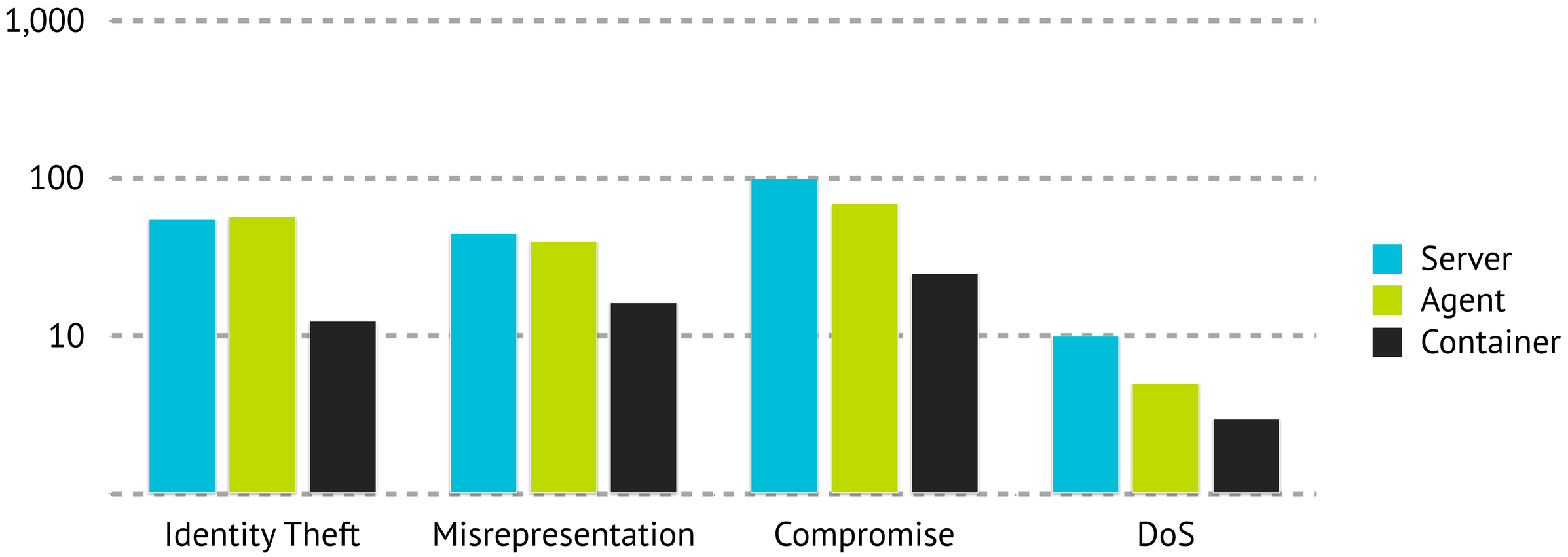
Relative Likelihood



@moyerma
@evan2645

SPIRE

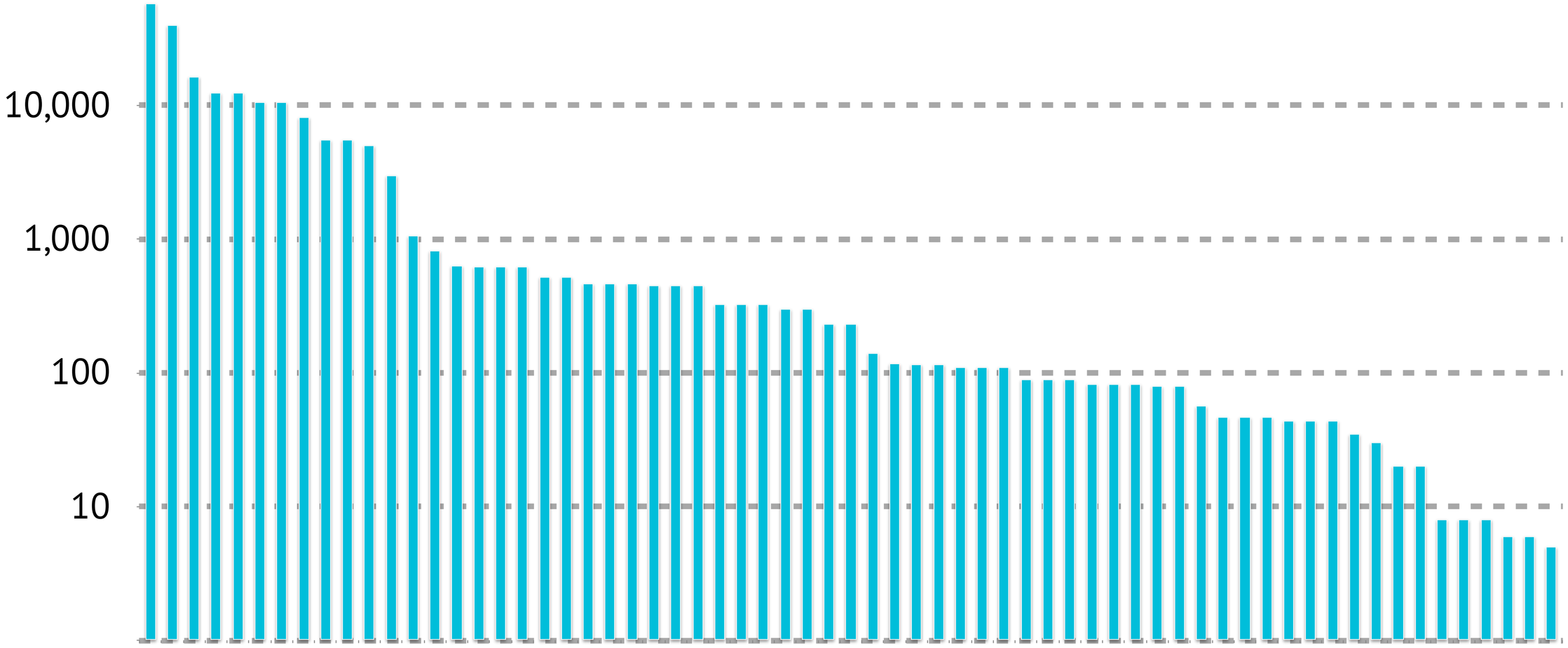
Relative Severity



@moyerma
@evan2645

SPIRE

Joint Ranking



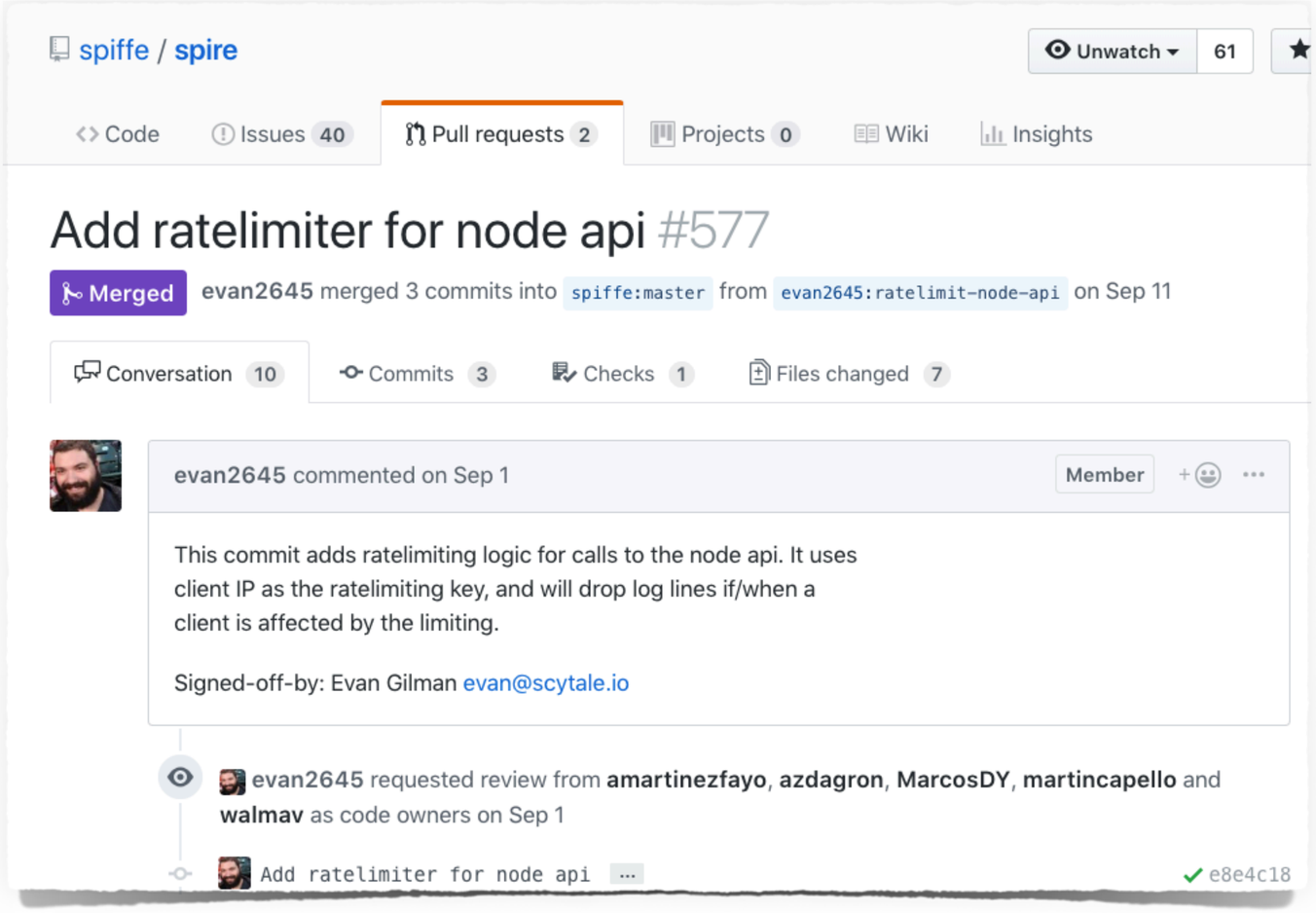
@moyerma
@evan2645

SPIRE

Findings

Finding: Add Rate Limiting in spire-server

- SPIRE server should have some rate limiting controls:



@moyerma
@evan2645

SPIRE

Finding: Eliminate CSR Parsing

- SPIFFE could drop CSR parsing altogether.
  - CSR (PKCS #10) format is complex.
  - CSR parsers are in general are likely less exercised than certificate parsers.
  - Security of SPIFFE doesn’t rely on its signing guarantees.

Finding: No Big Surprises

- Overall, the design of the system enables the desired security properties.
- Doesn't mean there aren't issues we overlooked, but this is a good sign.

Scrutinizing SPIRE to Sensibly Strengthen SPIFFE Security

Matt Moyer, Evan Gilman

@moyerma
@evan2645