BOOTSTRAPPING SECURE APACHE MESOS CLUSTERS

MESOSPHERE

ADAM BORDELON

Distributed Systems Architect

Apache Mesos committer/PMC, Apache Myriad (incubating) committer/PMC, DC/OS committer/PMC, specializing in security and storage. Enjoys music, nature, and parties.

me@apache.org

JÖRG SCHAD

Developer Advocate

@joerg_schad

VINOD KONE

Engineer

Apache Mesos Committer and Tech Lead/Manager @Mesosphere

@vinodkone

VISHNU MOHAN

Solutions Engineer

Works closely with customers in the field on Performance and Automation. When he's not analyzing sandbox logs or coding against some API for fun, he may be found rock climbing, hiking, running or scuba diving.

@vm_mesos

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

AGENDA

AGENDA

- Problem Definition, Motivations and Applications
- Scenarios and putting it all together
- Lab - https://github.com/dcos-labs/secure-mesos-workshop

MOTIVATION

MesosCon 2016: Security Best Practices

MOTIVATION

WHO?

Financial Services
(Banks, Hedge Funds)
Healthcare Services
Government(s)
Telecoms
Cloud Providers
eCommerce
Other Enterprises

WHY?

Personally Identifiable Information
Health, Finance, etc.
Legal requirements for data protection and confidentiality
Multitenancy
Admin-only operations
Users from different departments
Co-locate competitors' workloads
Prevent getting pwned by a bitcoin/ether miner

OUT OF SCOPE (MESOS-4936)

KERNEL SECURITY PRIMITIVES

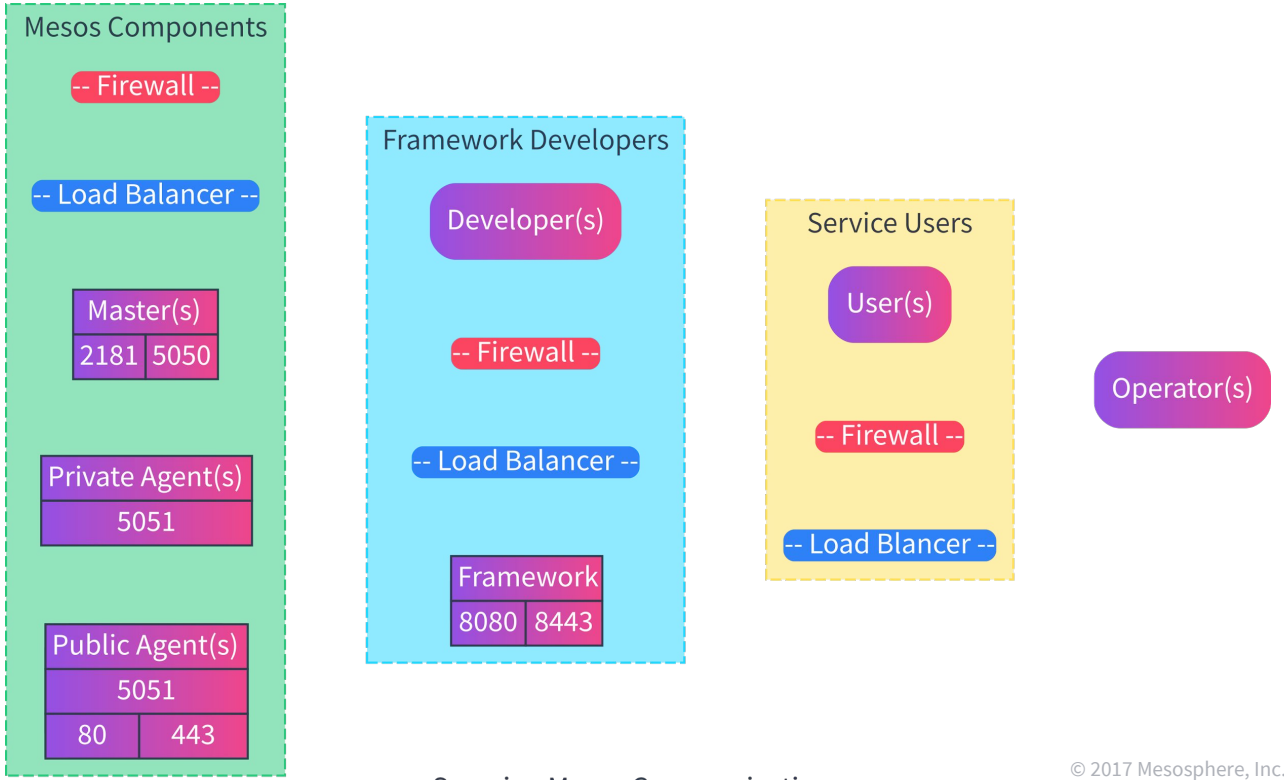
Mandatory Access Controls (SELinux/AppArmor)
Capabilities
SECCOMP
User Namespaces

HARDWARE SECURITY PRIMITIVES

TCG & TPM
HSM

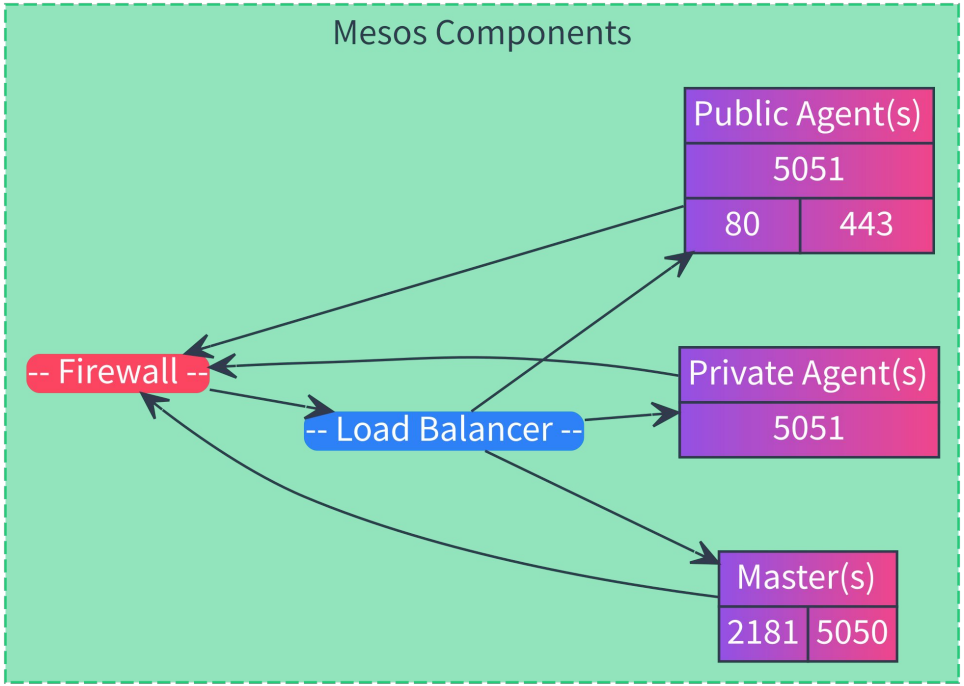
SECURE THE PERIMETER

SECURE THE PERIMETER: BUILDING BLOCKS



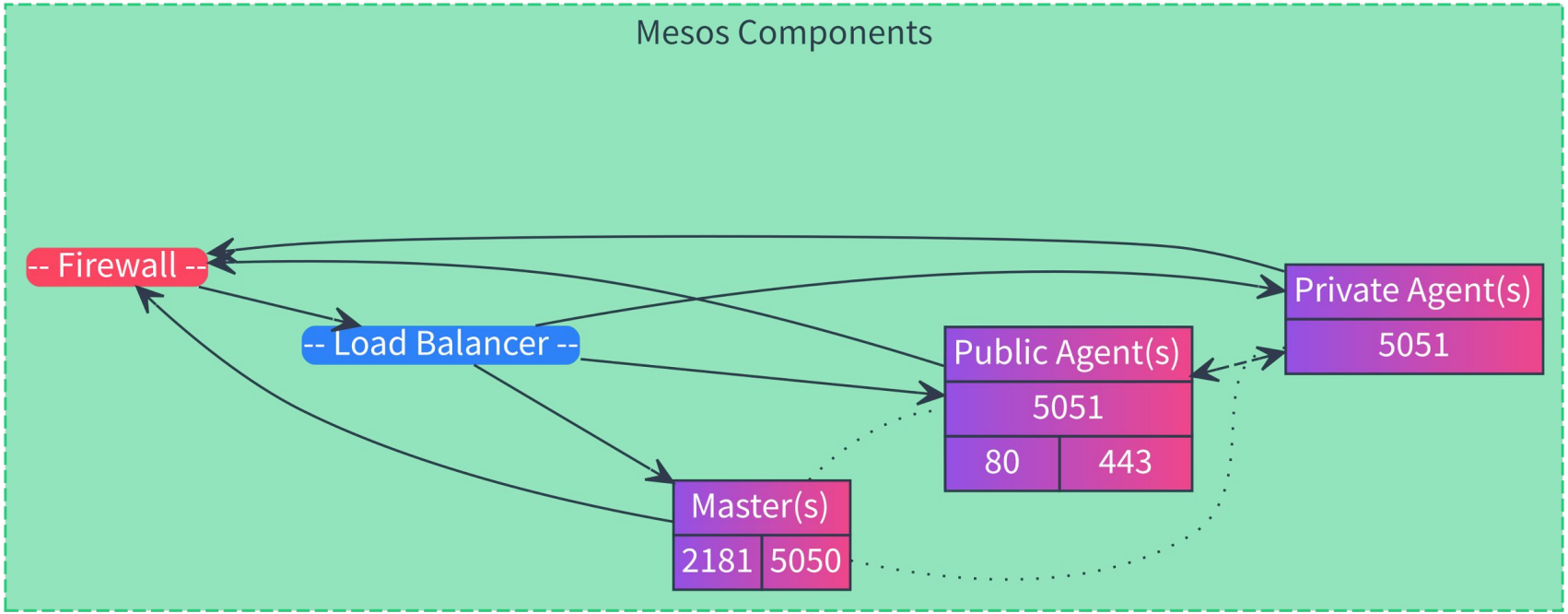
Securing Mesos Communications

SECURE THE PERIMETER: MESOS



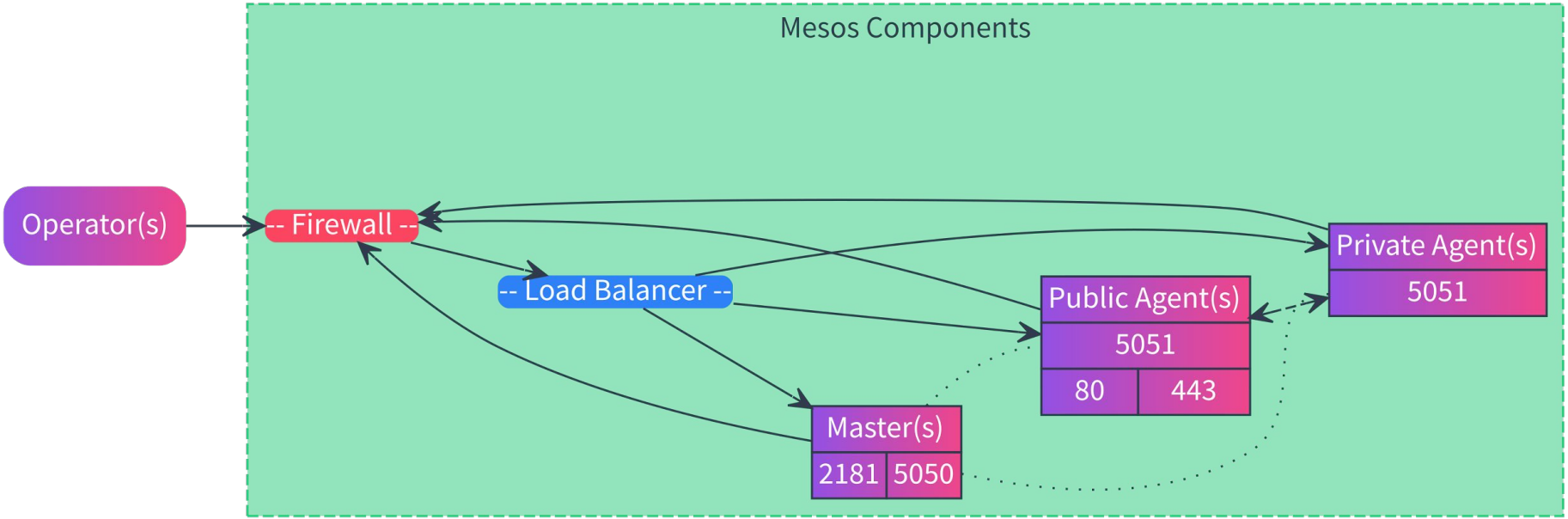
Securing Mesos Communications

SECURE THE PERIMETER: MESOS contd.



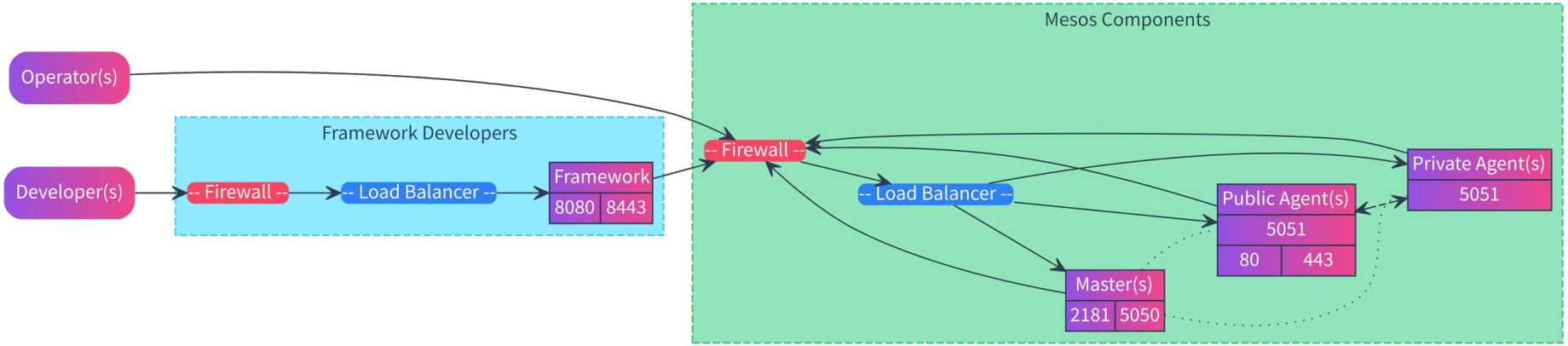
Securing Mesos Communications

SECURE THE PERIMETER: OPERATORS



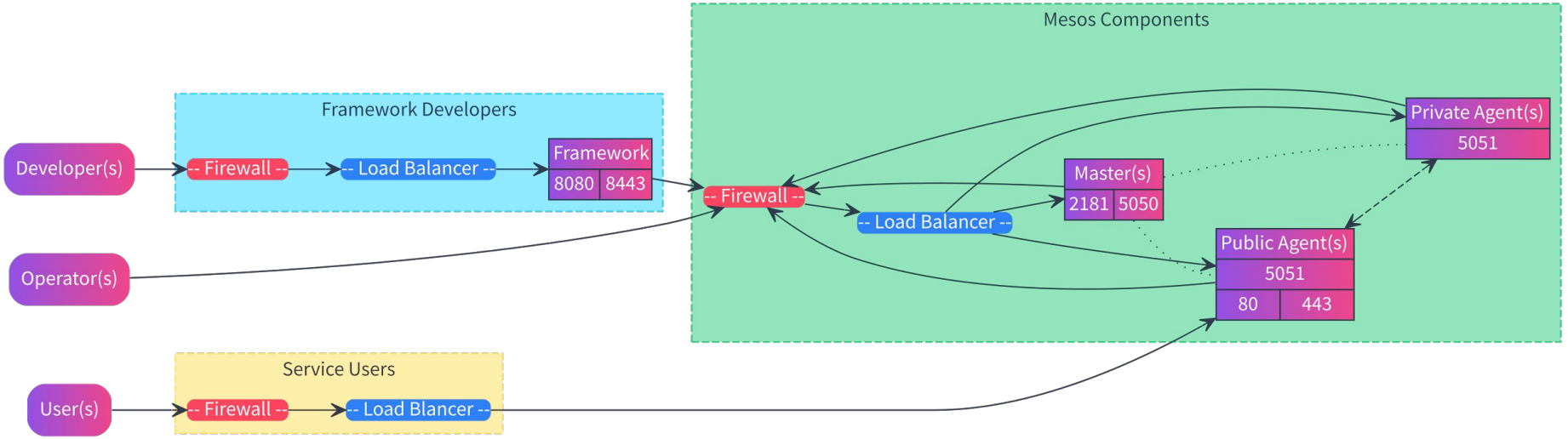
Securing Mesos Communications

SECURE THE PERIMETER: FRAMEWORK DEVELOPERS/USERS



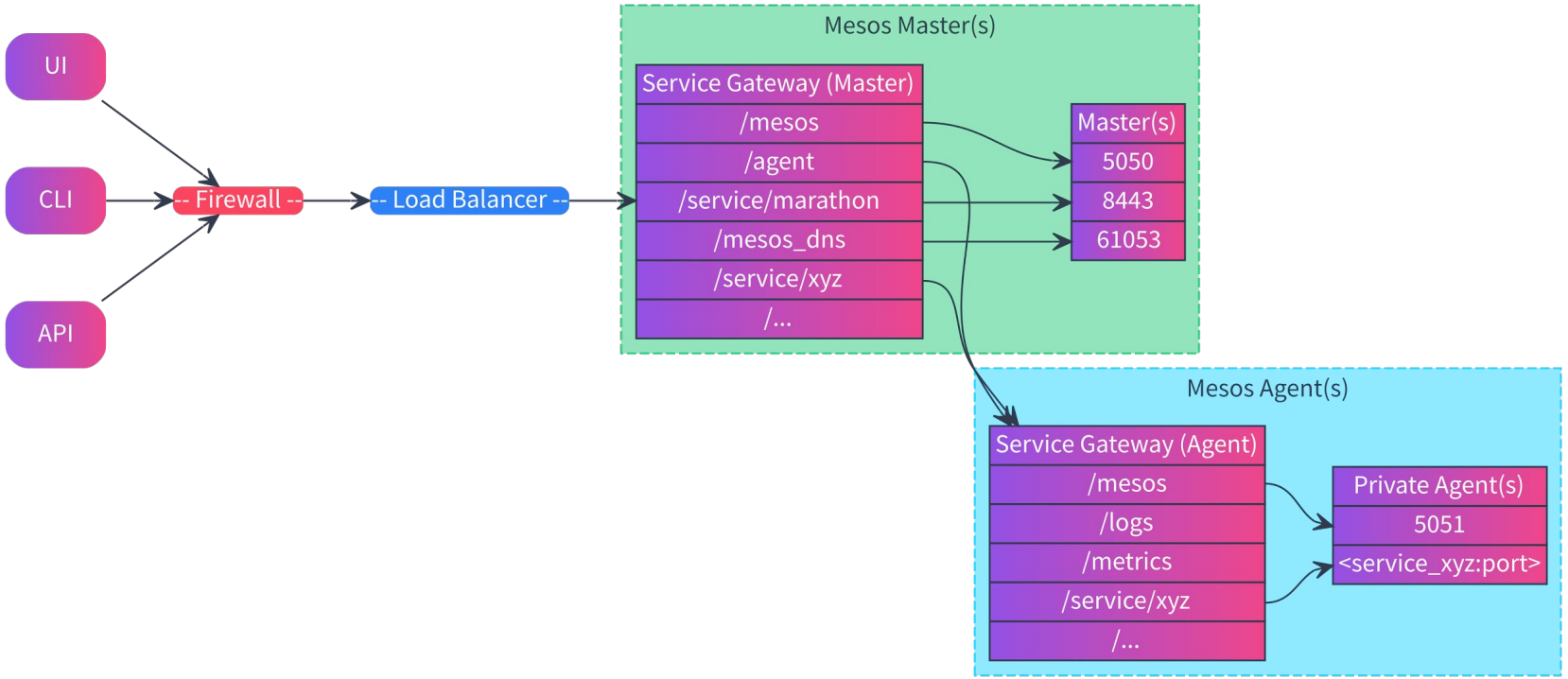
Securing Mesos Communications

SECURE THE PERIMETER: SERVICE USERS



Securing Mesos Communications

SECURE THE PERIMETER: OPTIONAL - SERVICE GATEWAYS



Mesos Service Gateway

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

TLS
(All the Things!)

TLS: MESOS CONFIGURATION

BUILD

```
./configure --enable-libevent --enable-ssl
```

Must compile libmesos this way too, for schedulers/executors

ENVIRONMENT VARIABLES

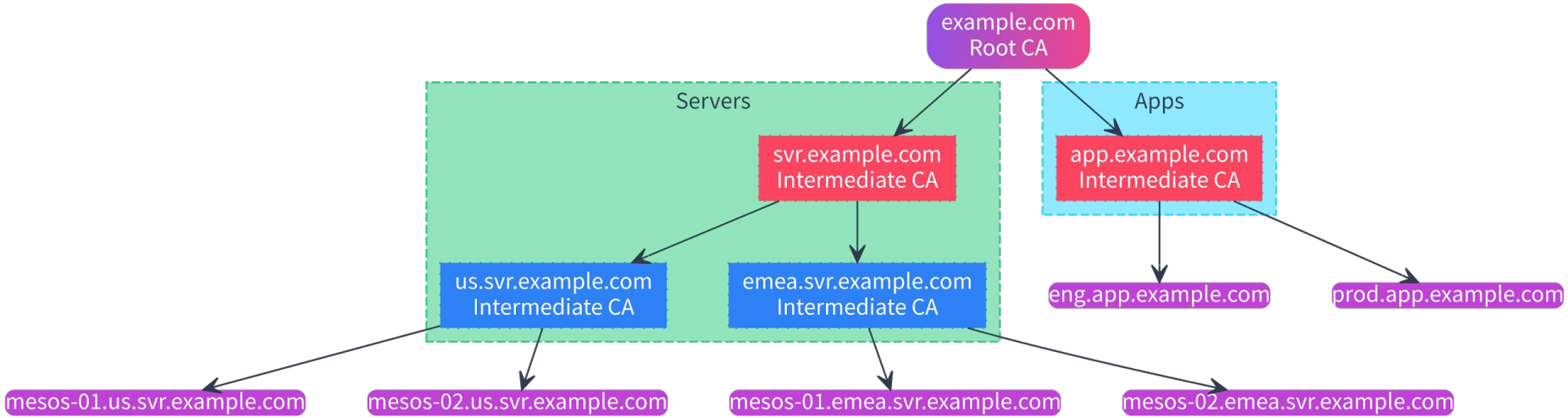
```
LIBPROCESS_SSL_ENABLED=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_SUPPORT_DOWNGRADE=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_KEY_FILE=(path to key)
LIBPROCESS_SSL_CERT_FILE=(path to certificate)
LIBPROCESS_SSL_VERIFY_CERT=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_REQUIRE_CERT=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_VERIFY_DEPTH=(N) [default=4]
```

TLS: MESOS CONFIGURATION contd.

ENVIRONMENT VARIABLES (contd.)

```
LIBPROCESS_SSL_VERIFY_IPADD=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_CA_DIR=(path to CA directory)
LIBPROCESS_SSL_CA_FILE=(path to CA file)
LIBPROCESS_SSL_CIPHERS=(accepted ciphers separated by ':')
[default=AES128-SHA:AES256-SHA:RC4-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AE
S128-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA]
LIBPROCESS_SSL_ENABLE_SSL_V3=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_ENABLE_TLS_V1_0=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_ENABLE_TLS_V1_1=(false|0,true|1) [default=false|0]
LIBPROCESS_SSL_ENABLE_TLS_V1_2=(false|0,true|1) [default=true|1]
LIBPROCESS_SSL_ECDH_CURVE=(auto|list of curves separated by ':')
[default=auto]
```

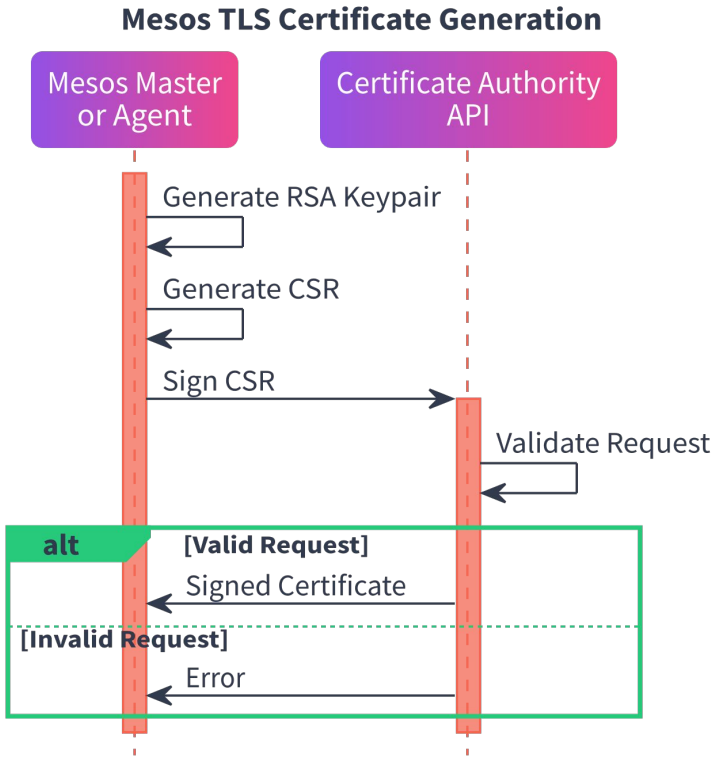
PKI: CERTIFICATE INFRASTRUCTURE



PKI Certificate Infrastructure

But how does the key+cert get to the master/agent? To the scheduler?

TLS: CERTIFICATE GENERATION - CERTIFICATE AUTHORITY



MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

MODULES

MODULES: OVERVIEW

Mesos modules provide a way to easily extend Mesos by creating and using shared libraries that are loaded on demand.

Modules can be used to customize Mesos without having to recompile/relink for each specific use case.

Modules can isolate external dependencies into separate libraries, thus resulting into a smaller Mesos core. Modules also make it easy to experiment with new features.

Modules can be specified for master, agent and tests. Modules can also be used with schedulers that link against libmesos.

MODULES: TYPES

- Allocator
- Authentication
  - Authenticatee and Authenticator modules allow for third parties to quickly develop and plug-in new authentication methods. An example for such modules could be to support PAM (LDAP, MySQL, NIS, UNIX) backed authentication.
- Authorizer
- Secrets
  - Mesos containerizer: Isolator (many non-secret uses)
  - Docker containerizer: pre-launch hook
  - Secret Generator/Resolver (first class secrets!)
- Master Contender and Detector
- Container Logger
- QoS Controller, Resource Estimator

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

AUTHENTICATION

AUTHENTICATION: OVERVIEW

Authentication permits only trusted entities to interact with a Mesos cluster.

Authentication can be used by Mesos in three ways:

1. To require that frameworks be authenticated in order to register with the master.
2. To require that agents be authenticated in order to register with the master.
3. To require that operators be authenticated to interact with the many HTTP endpoints.

Authentication is disabled by default. When authentication is enabled, operators can configure Mesos to either use the default authentication module or to use a *custom* authentication module.

The default Mesos authentication module uses the Cyrus SASL library. By default, Mesos uses `CRAM-MD5` authentication. Other options include `ANONYMOUS`, `PLAIN`, `GSSAPI` etc.,

AUTHENTICATION: CREDENTIALS, PRINCIPALS AND SECRETS

When using the default `CRAM-MD5` authentication method, an entity that wants to authenticate with Mesos must provide a ***credential***, which consists of a ***principal*** and a ***secret***.

The principal is the identity that the entity would like to use; the secret is an arbitrary string that is used to verify that identity. Principals are similar to user names, while secrets are similar to passwords.

Principals are used primarily for authentication and authorization; note that a principal is different from a framework's user, which is the operating system account used by the agent to run executors, and the framework's roles, which are used to determine which resources a framework can use.

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

AUTHORIZATION

AUTHORIZATION

The authorization subsystem allows the operator to configure the actions that certain principals are allowed to perform.

A reference implementation local authorizer provides basic security for most use cases. This authorizer is configured using Access Control Lists (ACLs).

- Role vs. Principal
- ACLs
  - Subject
  - Action
  - Object

AUTHORIZATION

AUTHORIZABLE ACTIONS

- register_frameworks
- run_tasks
- teardown_frameworks
- reserve_resources
- unreserve_resources
- create_volumes
- destroy_volumes
- get_quotas
- update_quotas
- get_endpoints
- update_weights

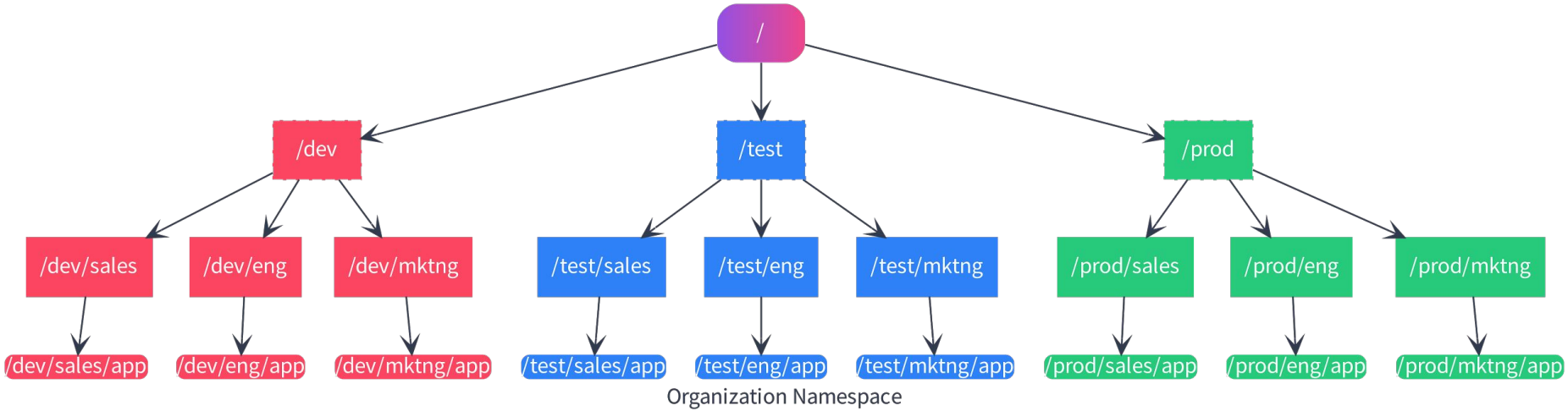
AUTHORIZABLE ACTIONS (contd.)

- view_roles
- view_frameworks
- view_executors
- view_tasks
- access_sandboxes
- access_mesos_logs
- register_agents
- get_maintenance_schedules
- update_maintenance_schedules
- start_maintenances
- stop_maintenances
- get_maintenance_statuses

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

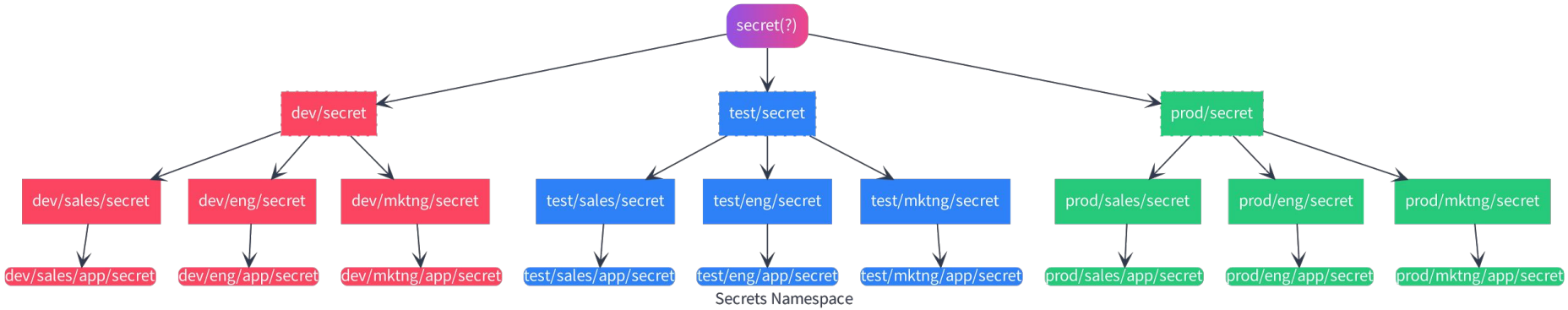
NAMESPACES

ORGANIZATION NAMESPACE



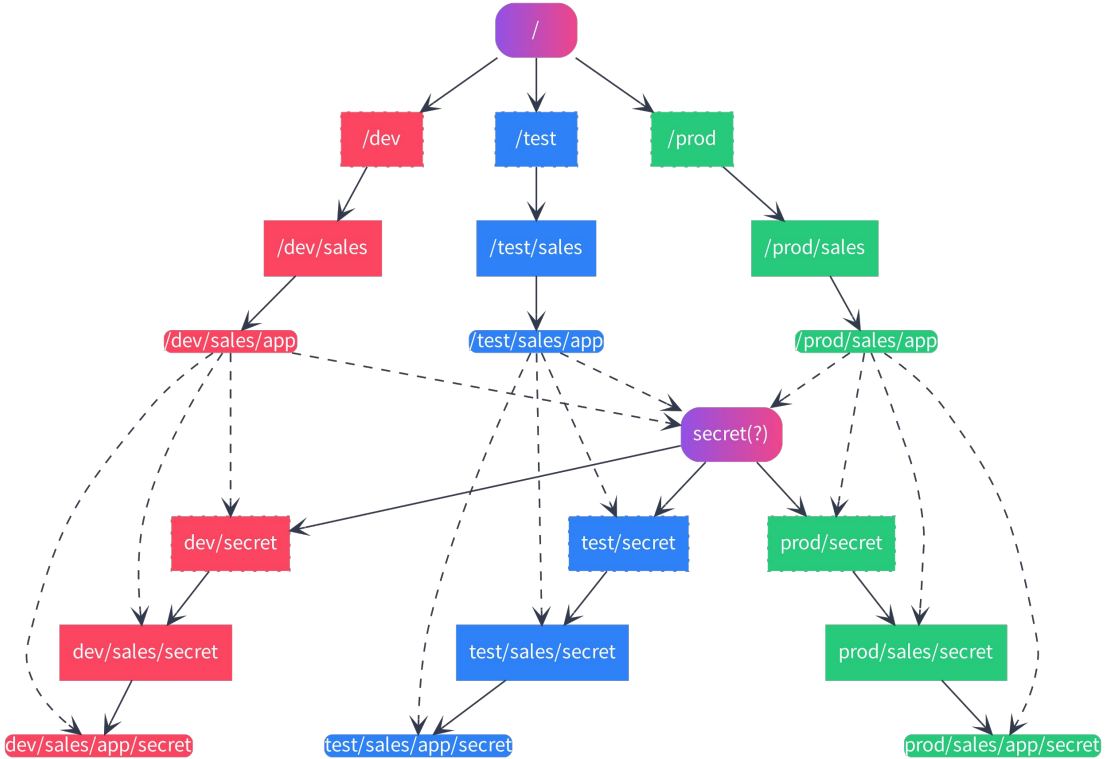
Organization Namespace

SECRETS NAMESPACE



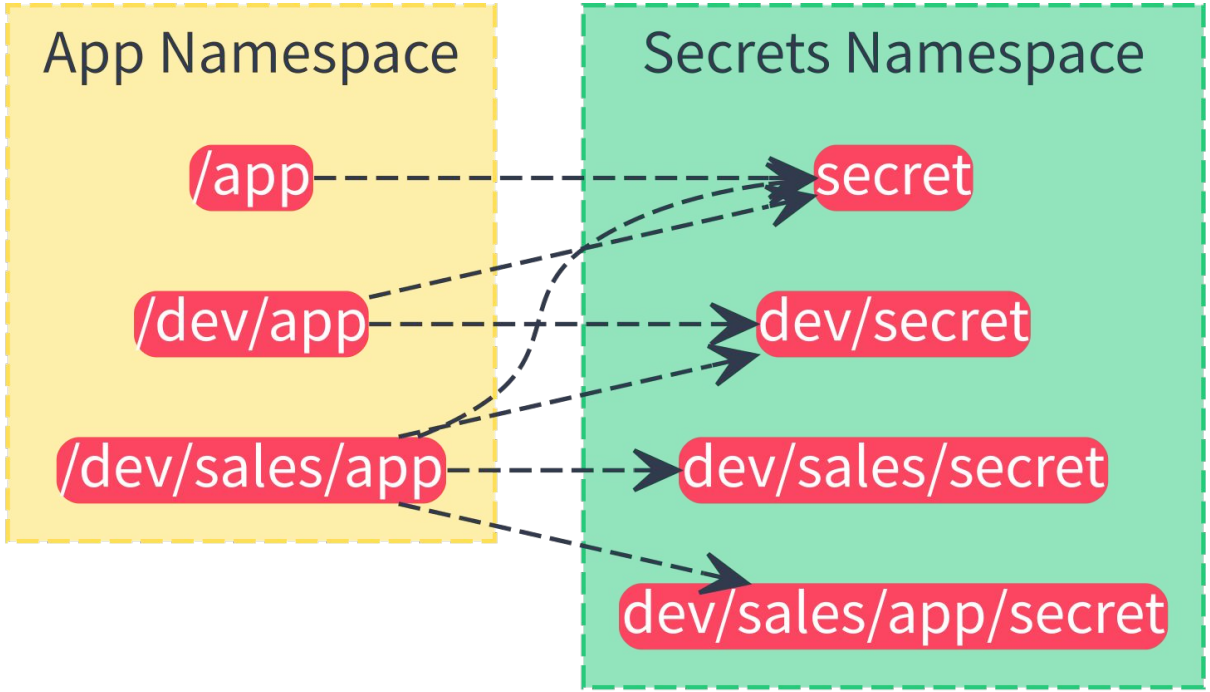
Secrets Namespace

ORG::SECRETS NAMESPACE ACCESS MAPPING



Organization::Secrets Namespace Access Mapping

ORG::SECRETS NAMESPACE ACCESS MAPPING (FLATTENED)

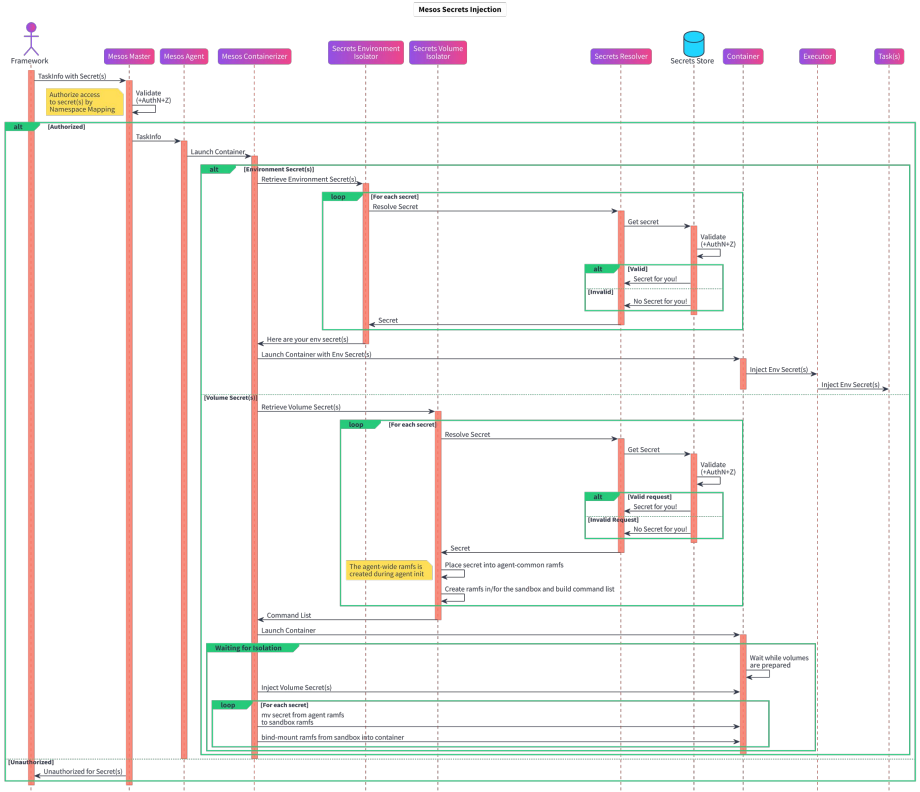


Organization::Secrets Namespace Access Mapping

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

SECRETS

SECRETS: SEQUENCE DIAGRAM



MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

LAB!

Thursday, September 14 • 2:50pm - 3:30pm (http://sched.co/BYa7)
Container Networking for Micro-Services: An Apache Mesos and DC/OS Networking Deep Dive - Deepak Goel & Jörg Schad, Mesosphere

Thursday, September 14 • 4:00pm - 4:40pm (http://sched.co/BYa0)
Apache Mesos and Security: The Joy of Mesos with Calico - Diego Oliveira & Acácio Alves dos Santos, PagSeguro

Thursday, September 14 • 4:00pm - 5:30pm (http://sched.co/BnUy)
Building Your First Stateful DC/OS Service - Ben Wood, Mesosphere (limited spots, pre-registration suggested)

Thursday, September 14 • 4:50pm - 5:30pm (http://sched.co/BYaW)
What Security People Want: Making DevSecOps Happen with Containers - Tsvi Korren, Aqua Security

Thursday, September 14 • 7:00pm - 8:30pm (http://sched.co/Bogm)
Town Hall: Apache Mesos (includes Networking and Storage topics) - Jie Yu, Mesosphere

Thursday, September 14 • 7:00pm - 8:30pm (http://sched.co/C8tP)
Town Hall: DC/OS - Judith Malnick, Mesosphere

Friday, September 15 • 11:00am - 11:40am (http://sched.co/BYjH)
Multi-Tenancy in Apache Mesos - Ben Mahler, Mesosphere & Jay Guo, IBM

Friday, September 15 • 4:50pm - 5:30pm (http://sched.co/C1ZL)
An Overview of Mesos Containerization and the Default Executor - Gilbert Song & Anand Mazumdar, Mesosphere

MesosCon 2017: Bootstrapping Secure Apache Mesos Clusters

Q&A

VISIT OUR BOOTH

Learn more by visiting:
mesos.apache.org
dcos.io
mesosphere.com

References

- MesosCon 2016: Mesos Security Best Practices
- Apache Mesos Documentation
- Authentication
- Authorization
- HTTP Endpoints
- TLS
- Secrets
- Modules
- Design Docs
- Improve container security for Mesos containerizer [MESOS-4936]

THANK YOU!

Slides:

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

BACKUP SLIDES

MesosCon 2017:
Bootstrapping Secure
Apache Mesos Clusters

CONCLUSIONS & FUTURE WORK

TLS: BACKGROUND

The Mesos Master listens on port `5050` and the Mesos Agent listens on port `5051`

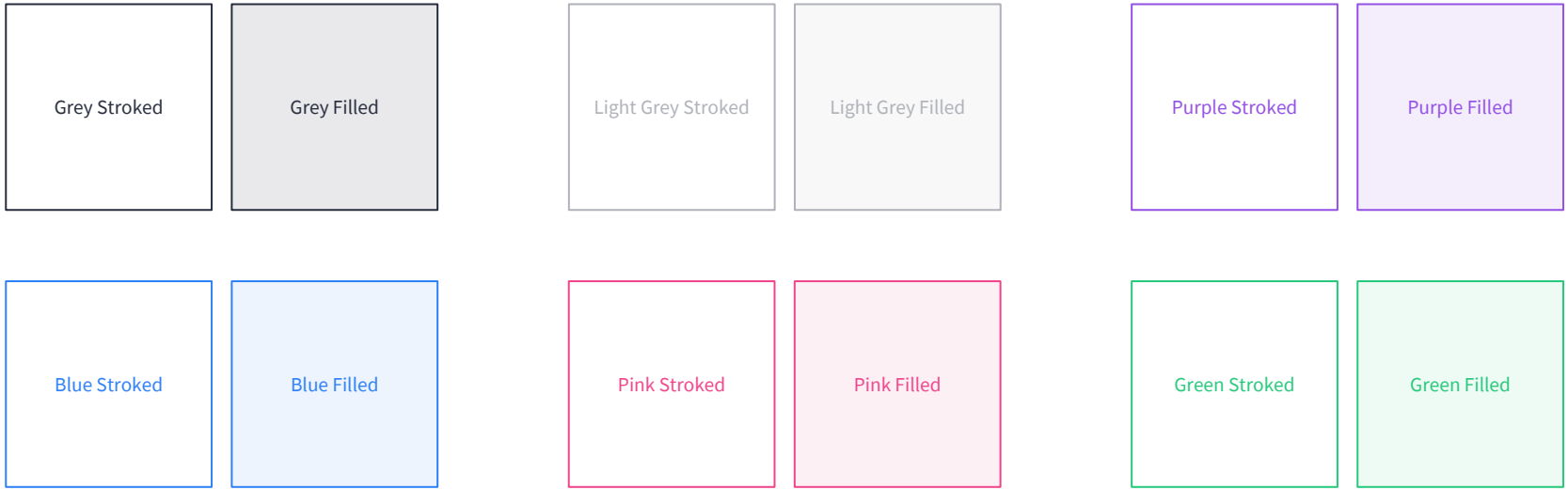
By default, all the messages that flow through the Mesos cluster are unencrypted, making it possible for anyone with access to the cluster to intercept and potentially control arbitrary tasks.

SSL/TLS support was added to libprocess in Mesos 0.23.0, which encrypts the low-level communication that Mesos uses for network communication between Mesos components. Additionally, HTTPS support was added to the Mesos WebUI.

There is currently only one implementation of the libprocess socket interface which relies on the `libevent-openssl` library that wraps openssl.

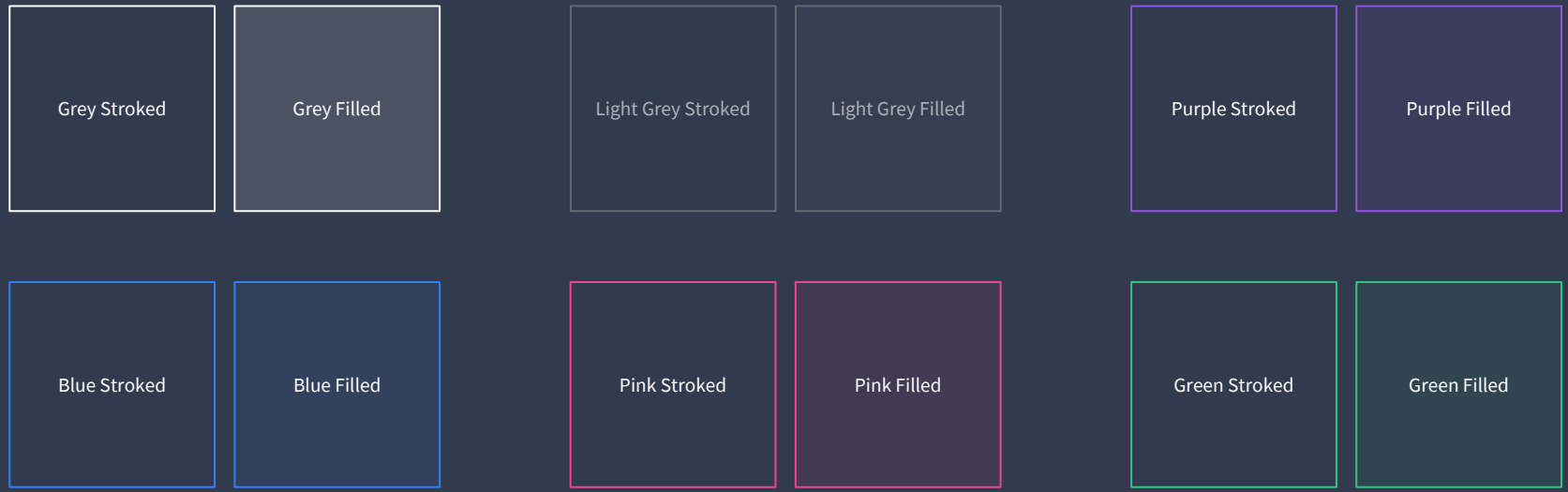
Shapes

SHAPE STYLES



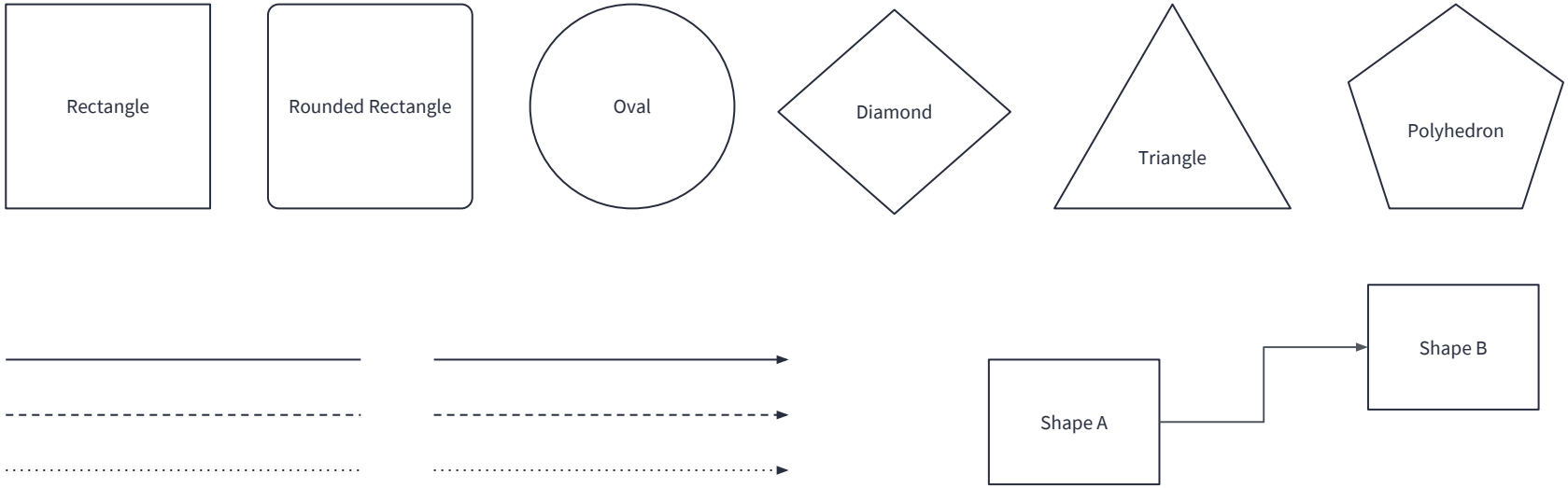
Shapes

INVERTED SHAPE STYLES



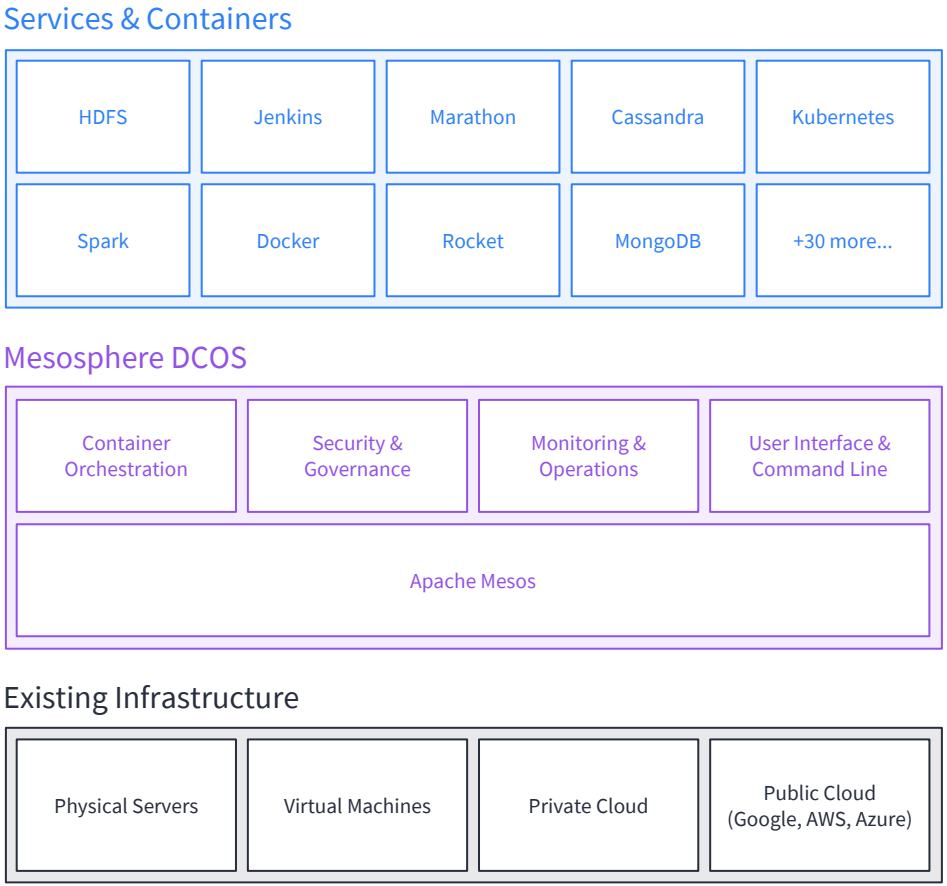
Shapes

SHAPE STYLES



Product Overview

MESOSPHERE DCOS



Typography

FONT FAMILIES

OSWALD

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
0123456789!@#$%^&*()_+=

SOURCE SANS PRO

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopq
rstuvwxyz0123456789!@#$%^&*()_+=

Typography

TEXT STYLES

MAIN BODY TEXT

Main Body Text. Collaboratively administrate empowered markets.

SMALL BODY TEXT

Small Body Text. Efficiently unleash cross-media information without cross-media value.

MINI BODY TEXT

Mini Body Text. Efficiently unleash cross-media information without.

HEADING TEXT

HEADING 1

Heading 2

Heading 3

Heading 4

Typography

INVERTED TEXT STYLES

MAIN BODY TEXT

Main Body Text. Collaboratively administrate empowered markets.

SMALL BODY TEXT

Small Body Text. Efficiently unleash cross-media information without cross-media value.

MINI BODY TEXT

Mini Body Text. Efficiently unleash cross-media information without.

HEADING TEXT

HEADING 1

Heading 2

Heading 3

Heading 4