# **EdgeX Security WG Meeting, 01/29/2020**

Attendees: Tingyu, Akram, Anthony, Trevor, Michael Estrin ( DELL), Jim White( IoTech), Bryon, Jim Wang, Beau, Eno ( Intel), Malini, Diana ( VMWare), Colin ( KONG)

Others may have joined after the meeting

## **Agenda**

- Security in EdgeX API v2

- Token expiration issues (raised from PR-45 of go-mod-secret)

- Security audit: Snyk report & process

Security in EdgeX API v2

Core WG recording:

<https://zoom.us/rec/play/upIkde_9pj43GYGT5QSDAPFxW9W_e_6s1yIWqKZfyBy2U3QCN1X1YucWZbayaqK5xURe2GVvti2ymcgf?continueMode=true>

[9:51](https://vmware.slack.com/archives/GGUB6EZUZ/p1580233911000400)

Slides: <https://github.com/edgexfoundry/edgex-go/pull/2285>

Request-id -- did not see in examples -- Estrin -- exists, in the common section.

With a batch request -- each sub-request should have its own request-id

A common token across batch requests -- auth and authz common to all - RBAC

Bryon -- no auth yet in it -- crawl/walk/run?

Estrin leveraging Kong to gate access to API

Part of V2 was to support different transport mechanisms -- http,messaging

In that context contracts

DTOs for everything,

Batch is a standin for alternate transport mechanism

Request envelope may include some identification token

Two requests we have currently: use case request & batch request

Options to have security enhancement on two requests:

* On use case request: include request id already in the spec. Add one more property.
* On batch request:

Tingyu -- device SDK -- associate a unique-id, within V2 design, will the device-id be added into the DTO.

Estrin -- correlation-id will be separate. Answer - yes,

When adding anything new, the system will assign an id and return it in the response. That id would be specific to the device/thing being added.

What about message bus: AuthU to AuthZ through token

Estrin -- upon reflection -- provide identity/token -- **add that as a property of the request envelop**

Use an http header to carry that token

Bryon -- we should also look at request signing -- to protect from tokens being stolen

Estrin -- json tokens provide that feature(an example implementation) .. there may be others

Malini:

**Denial-of-service type attacks related questions**

What about timeouts on batch/serial/parallel requests

Number of sub-requests

Length of response

Estrin: asks the security team to come up with some ideas on how we want to deal with this

Using middleware we could keep track of these - at a use case level, user level

Jim White: suggests looking at Oasis, see how others are dealing with this in terms of patterns, implementation -- security shell independent of protocol.

Investigation.

Opportunity -- service-to-service

Malini - certainly the middleware chaining/layering makes it more extensible

Tingyu - metering, filtering

Estrin -- strongly suggest pulling down the code and try it

Offers recording a demo for our use -- to help us get familiar

Jim White -- please make the recording

Tingyu -- The PR has 132 files -- lots to review

## Security audit: Snyk report & process

Tern open source project, Vmware launched for license compliance. Provides a bill-of-materials (BoM). <https://github.com/vmware/tern>

Example Tern output [Tern Consul 1.6](https://docs.google.com/document/d/1Z7xi8fB0bd4jh_Or_63dwfieLYYYlppE_g4MmEuPmmw)

Allows us to check if some CVEs of concern are addressed in a docker repo image.

Snyk report in edgexfoundry/docker-edgex-consul:1.1.0

Vulnerability in curl 7.64.0-r1 (out-of-bounds, Double Free, Buffer Overflow)

Bryon summarized well -- do not need to bother devops to get some quick feedback.

Snyk we run once a week.

## Token expiration issues (raised from PR-45 of go-mod-secret)

[https://github.com/edgexfoundry/go-mod-secrets/pull/45#discussion\_r370856002](https://github.com/edgexfoundry/go-mod-secrets/pull/45" \l "discussion_r370856002)

Tingyu -- we initially thought it was minor - coding style

Discussion -- token expiration edge case -- either because Vault was down or the service was down and did not seek to renew token -- handle in a more complete/broader way as a pattern across edgeX. This PR can be closed as handling everything in scope and not cover this edge case.

In total expiration -- need to recreate a token. Orchestration solutions typically handle service restart.

Bryon - Vault tells you when you present a token that it is expired or not 403. -- no more renewable. hard

500 errors are soft errors.

Wang: only solution then might be to reboot/restart system.