# **EdgeX Security WG Meeting, 02/12/2020**

Attendees: Trevor, Tingyu, Michael Estrin, Doug Gardner, Anthony Bonafide, Lenny, Beau, Jim, Diana, Malini, Bryon, Eno

Others may have joined after the meeting

## **Agenda**

* Security in EdgeX API V2 Presented by Bryon – follow up
* Security audit: Snyk report & process
* Issue #2344 background & request to discuss

1. Security in EdgeX API V2 Presented by Bryon

* Slides available at <https://docs.google.com/presentation/d/1S56M5-kSFDOdN0T0IELHDdhuy-JbNOdqoDPwfx-Mi8c/edit#slide=id.p>

Bryon to look at Michael Estrin suggestion provided a little earlier this morning and see how it fits in with his security suggestions

“It occurred to me at some point in the last week that you should consider a transport request as the basic unit of communication. A single transport request for an alternate transport (e.g. pub/sub, asynchronous messaging, email, etc.) may contain one or more use-case requests -- similar to any HTTP endpoint.

Encourage you to wrap security around transport request. Authentication could be handled at that level with the resulting identity used at a use-case request level to authorize individual use-case requests.”

Other concerns that were brought up:

Timeline, Security Requirements, Role of Kong, API definition and what goes down on the wire

Tony :

* Timeline
* Have the V2 API doc call out that we are addressing deployment on a possibly multi-node system to tackle future concerns of high availability

Responses with respect to Timeline

Michael Estrin: If we bolt security later, take much more effort. Now we are in green field mode, easiest time to tackle definition and implementation.

Security team: Want to leave in appropriate security hooks going out the door.

Jim: Lets see what we need and determine whether V2 comes out in Geneva or Hanoi.

Michael Estrin: API is what you plan to send on the wire and how .. so if we had a field that contains a signature later .. that would be changing what is going down the wire. Could argue both ways. At the very lease client and server would need to be different to handle the response.

Jim - this proposal suggests addressing security to be handled by EdgeX so we do not need to address authN and authZ by each transport layer (HTTP/Kong, MQTT etc etc)

ME: is it a requirement to handle security in a transport agnostic way?

Tony: fundamental question -- uptil now we have relied on external systems to address, do we want to revisit that decision.

ME: signed/unsigned requests around json web signature as orthogonal

To date the third party components we have leveraged only have provided rudimentary security, not provided AuthZ. If you do not make security a goal for V2 now, you most likely will change the fundamental structure later, contents that you will send down the wire. Is that a change to the API. Can argue it is different because what is coming down the wire is different.

Tony - last week we discussed 4 different alternatives but did not conclude with a decision.

ME: what we send down the wire is part of the contract

Bryon: Kong still serves a useful purpose, it acts as a reverse proxy, separating the internal and external networks. Multiple layers of protection

Jim: If we look at companies that provide security apparatus -- ForgeRock, this envelop has to be everywhere .. for requests coming from outside.

Bryon -- there might be a back channel request to Kong to check on the user and their access. Pivotal framework expects everything to come from the external endpoint, no talking between internal services.

Tony: your signed requests is not providing what Kong provides.

Bryon: Correct - Kong is sort of doing “request filtering” based on the auth token

Tony: how does request signature work with external clients

Bryon: the external entity has to get out of band a TLS certificate, so they can use the private key from there to sign their requests

Jim: What if time is not an issue? Remove the Geneva timeline consideration

-- addressing Tony concern about time

Tony: V2 is experimental

EM: we are doing a green field implementation, now is the time to define and decide on things.

Jim: definition of now: Is it Geneva or Hanoi. We all agree security is important.

Tony: Scope? Are we talking of security on a single box?

Bryon: Not a single box but a single install, scope of a docker compose.

Tony: On box, if your box is secure, this level of security is over kill.

Bryon: counter to that -- we are choosing protocols, implementations that allow for distribution.

Tony: Call that out in the scope documents, more distributed, more HA

Would be nice to claify how this all works with Kong.

Tingyu: Reasonable request but lots of work.

JIm: Bryon and Michael -- come back with your best option

Security audit: Snyk report & process

* Currently major issues are from Consul, Mongo and volume
  + Immediate mongo upgrade possible/feasible ?
  + If upgrade, do we need to upgrade in FUJI or later version?
    - Will need to discussion further offline
* Working in progress on Mongo issue
  + Diana: Mongo started with restriction free control.
  + Unsure if it is accessible from external sites -- firewall rules that might be in place on the host
  + Solution thoughts:

For production we could use in “ secure mode” the credentials from vault.

For development mode -- is there a way to detect in development mode and then it is easy enough to take environment variables for username/password to use.

Docker-compose can be used to hold username/password for the credentials.

Tingyu -- duplicate the nightly build for developers without username/password.

Jim: we did that sort of thing in the past.

Tony: for developer - run Mongo natively without container

Just document it for developers

Diana: how do we detect developer mode in container

Conclusion: secure for production. Provide documentation for developer to use without being hampered by username/passwords.

Issue #2344 background & request to discuss

<https://github.com/edgexfoundry/edgex-go/issues/2344#issuecomment-583589139>

Set standards what are security issues and what is not

To provide guidance across the project

Do we consider the schema a security aspect

Do we consider the url as a security aspect

Loggin the commands

One of the commands you can sentd to Redis is the auth command which includes the credentials