# EdgeX Security WG Meeting 04/08/2020

Attendees: Beau, Bryon, Colin, Jim White, Tonyes,Trevor, Anthony ,Diana , & Malini.

Tingyu on vacation today.

Others may have joined after the meeting

## Agenda

- Hanoi Planning Items
- Is Redis Secure?
- Snyk Reports
- EdgeX-UI: hardcoded passwords

## Hanoi Planning Items:

Jim request: please write up a slide per bullet, capturing:

1) what the feature is in layman's terms.
2) who/why we want it - to guage priority
3) Effort involved - broad strokes like t-shirt size (large, medium, small) design, development, test, documentation

Bryon organized items in to buckets and shared the below

1) Secure EdgeX Bootstrapping, consul, vault, secure from the get go
2) TLS enabled based infrastructure -- currently only for vault and a kong cert. THis is passing everything securely to consul, postgres, kong admin port. When we upgrade to Redis V6, it uses TLS
3) Feature - bring your own cert (Bryon ranks this as ZBB? Does anyone need it?)
4) Eliminate hard coded password for Postgres

   Tony - how do the other Mongo/Redis handle this

   Postgres can load

   Colin - Kong 2.03 also uses file to upload password 2.01 supports passing in password through docker compose file.

Consider switching to 2.03 for Geneva. Colin thinks that should be easy enough. But there are some challenges.
Doing an upgrade is difficult. Postgres volume having the password. May need to provide both paths -- something to take into consideration.

5. Secure Microservice communication
    a) Secure service location
    b) Identity and auth
    c) Confidentiality and integrity

Trevor: will this bring us to the point of running microservices on separate box (HIGH)
Tonyespy: scope this. Single consul instance, single vault instance..

If we bound our distributed services to just device service being on a separate box, then distributed services all around is a more future facing thing. Hardware root of trust would be then higher in priority.

6. container security enhancement
7. Hardware secret storage (Jim White: ZBB? TonyEspy: higher?)

In various stages

    a) Draft proposal - based on David Fiera (?) design was modified. Bryon -will make ADR
    b) Some hooks exist -- PR close
    c) An implementation -- will not be upstreamed
    d) Will ARM come and help? This is an area of interest for them.

8. Other stuff: CORS headers, process vetting, misc bugs, image signing, pluggable password generator

## Snyk Reports:

Thanks James Gregg. No new issues that need addressing

## Redis Security:

Andre is working on it and believes it is on track for Geneva.  This will also determine whether we mark MongoDB as deprecated (for Hanoi there will then be documentation, docker-compose, blackbox  etc change items).
Jim followed up with him and Trevor helped Andre.
Malini check up

## EdgeX UI:

Thanks to Tony Espy for bringing up this issue : hardcoded passwords

VMware/China team will address this. Possibly use environment variables to pass in credentials.

Snyk on UI?

Should we do any other review?

Tony recently started looking at it. Snap. Had to run the DB initialization

Jim White: it has been cleaned up a lot and they are addressing issues

Jim will follow up with James on Snyk.  DONE -- James confirms that we are running Snyk on edgex-ui