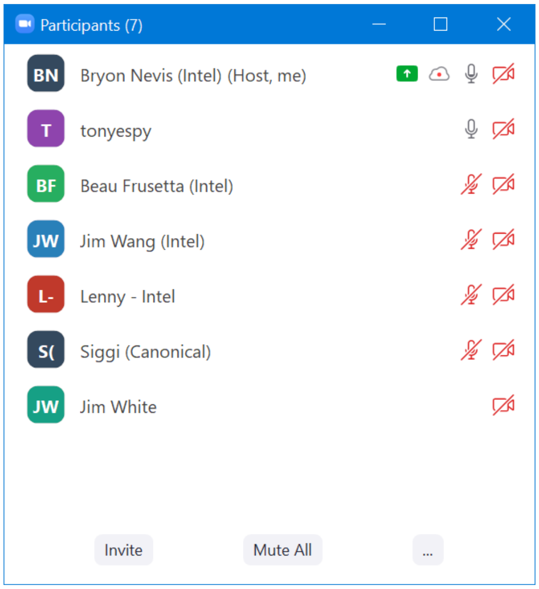
# EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

August 4, 2021

## Attendees



- BN Bryon Nevis (Intel) (Host, me)
- T tonyespy
- BF Beau Frusetta (Intel)
- JW Jim Wang (Intel)
- L- Lenny - Intel
- S( Siggi (Canonical)
- JW Jim White

## Standing Agenda

- Review Security Board

| Icebox | New | Backlog | WIP | Done |
|---|---|---|---|---|
| 9 | 1 (+1) | 12 | 3 / 0 | 3 |

- Securing Consul Board

| Ph-3 ToDo | Ph-2 ToDo | WIP | Done |
|---|---|---|---|
| 4 | 1 / 2 | 0 / 0 | 3 |

- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)

| Critical | High | Medium | Low |
|---|---|---|---|
| 0 | 16 (-24) | 11 (-8) | 4 (-2) |

- Device-coap updates done.
- sys-mgmt-agent needs update to docker 20.10.7
  - Agree sys-mgmt-agent issues are non-exploitable?
- Issues with golang/x/crypto unfixable for now due to dependency chains (shouldn't affect us)

- Review action items from previous week

# Agenda

- Discussion about EdgeX user management.
  - Eaton considering use of EdgeX; would like to have a more formal user management system that goes beyond the JWT-based mechanism we have. Want a service to "add users more efficiently" in a way consumable by end users. Jim White will invite to future security WG meeting to discuss more. Tony Espy would like to compare what they want with the automation that has been done for snaps to see how close we currently are (see Snap README). This discussion may also intersect with dynamic services since we are talking about adding permissions to Vault as well.
- Discussion about EdgeX GUI in secure mode.
  - Potential blocker - who authenticates the GUI (standalone auth, auth through kong)? Maybe UI has no authentication at all, but requires a token to make calls through Kong, and nothing works without it.
  - Will need TLS to protect any credentials.
  - Need to figure out why GUI didn't run into issue with lack of CORS support
  - Need to decide if they want "users" vs just a token, whether or not the UI supports multiple roles.
  - Would want to design so that GUI could run outside of Kong;
  - Would want to optimize if GUI runs on the same host as an EdgeX host.
  - If run outside of Kong, would have to manage their own TLS.
  - Treat as "external all the time" for internal design of GUI would likely be cleanest.
  - Suggest if wanted to include GUI as more than a developer tool, we should do threat modeling on the GUI as we haven't scrutinized it before.
- Security WG cancelled for next week.

# Action Items

- ~~7/14: Bryon: Update known security issues with Snyk findings~~
- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- ~~7/21: Tony: File issue to allow configuration.toml setting to change default token TTL. (cmd/security-secretstore-setup/res/filetokenprovider.toml)~~
- ~~7/28: Lenny: Add release note for device-coap base image bump~~
- ~~7/28: Jim: Investigate if curl still needed in secretstore-setup.~~
- ~~7/28: Bryon: TSC. Update security known issues with current Snyk “highs”.~~