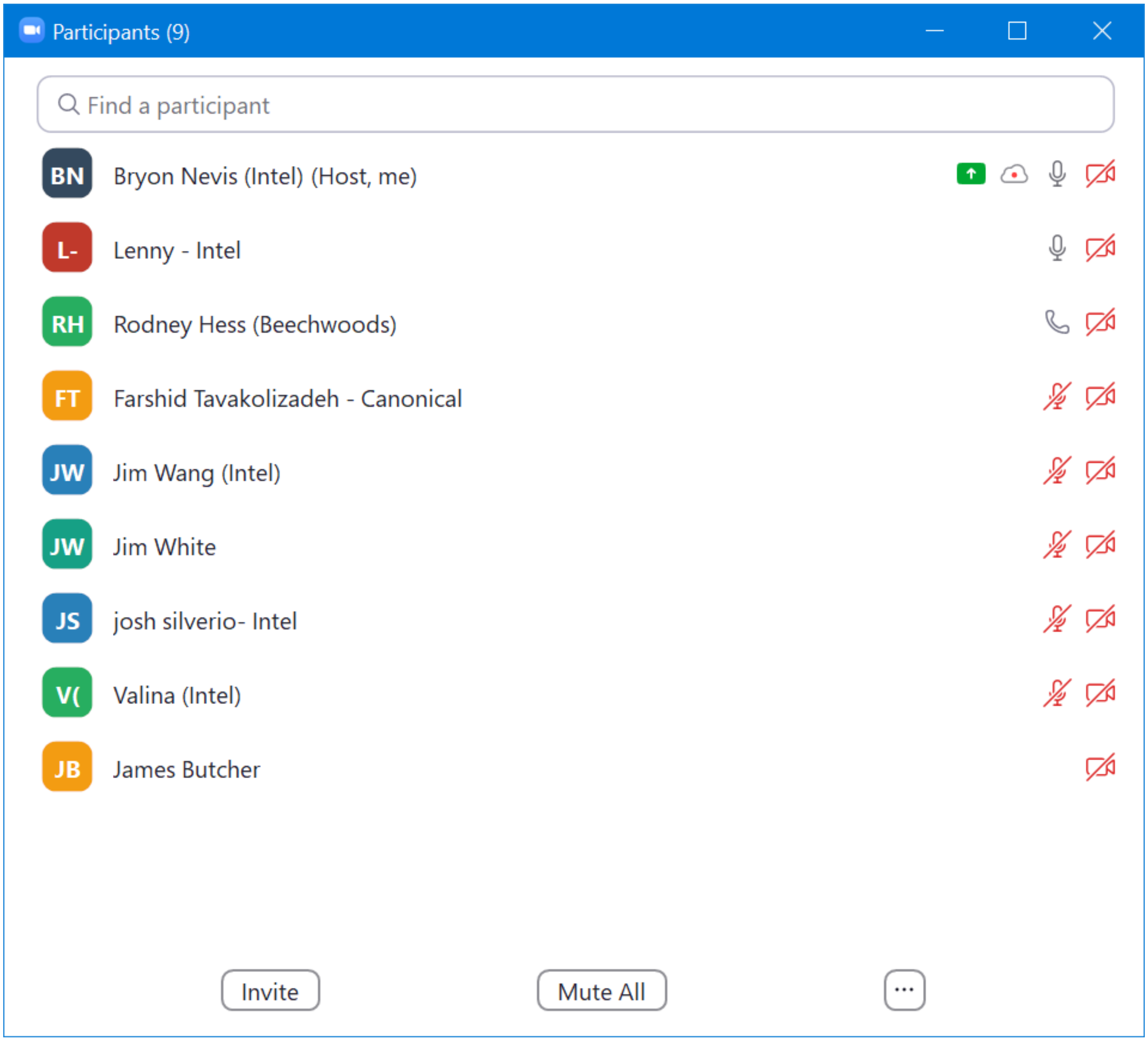
EdgeX Security WG Meeting

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

August 31, 2022

Attendees



BN Bryon Nevis (Intel) (Host, me)

L- Lenny - Intel

RH Rodney Hess (Beechwoods)

FT Farshid Tavakolizadeh - Canonical

JW Jim Wang (Intel)

JW Jim White

JS josh silverio- Intel

V(Valina (Intel)

JB James Butcher

Agenda

- Update on secure MQTT

  - This enhancement changes the way that compose-builder functions with MQTT is specified as part of the builder options. Modifies bootstrapper and secret store setup as well.
  - Implementation is mostly complete, testing in edge-compose; PR expected this week or early next week.
  - Minor question on what to do with eKuiper. Need to inject eKuiper configuration with MQTT instead of Redis. Should be done as a followup PR.
- Question on adding registry ACL roles
  - Bug: ADD_REGISTRY_ACL_ROLES doesn't seem to have an effect if it is changed after the initial start of EdgeX
  - Reference: https://docs.edgexfoundry.org/2.2/security/Ch-Configuring-Add-On-Services/
  - Jim Wang will confirm bug.
- Inspection of IOTech Threat Model
  - Jim White will attempt to convert to markdown for review in Github.
  - Will plan to upload original sources into edgex-docs. Place alongside existing secret store threat model (https://docs.edgexfoundry.org/2.2/threat-models/secret-store/threat_model/) and add an index to refer to our threat models.
  -

    Assumptions: Make sure report has single host.

    Config mitigation:

    - Remove docker network reference
    - Now have per service ACLs

    Consul data Spoof mitigation

    - Change to rely on docker/snap root access to be spoofed

    Config file disclosure

    - N/A

    Spoofing Redis (both directions)

    - Creds don't apply
    - Need root access
    - Optional: Use TLS if distributed

    Broker Access

- Restricted to authorized services,
- Np mitigation for authorized

Redis DoS

- Add Scheduler pruning data. frequency can be adjusted as needed.

ID Threat is missing for Redis

- Review why

Vault Spoofing

- Change to use service token

Vault DoS

- Auth required
- No mitigation for Authorized users

Vault data access

- Add service token
- Add local access only

Standing Agenda

- Review Security Board
- Securing Consul Board (skip)
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
  - Last checked: August 3, 2022 – as expected
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
- Review action items from previous week

Action Items

- 7/14/21: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 6/22/22: Bryon: Update known security issue wiki (add GHSA?)