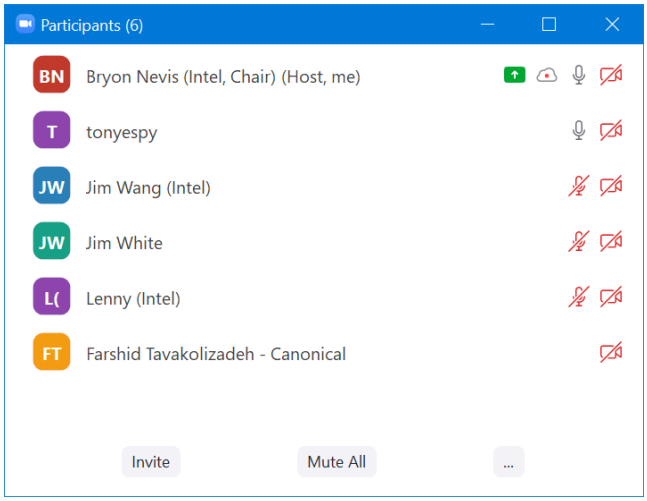
EdgeX Security WG Meeting

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

January 19, 2022

Attendees



Agenda

- Opens
    - None
- Delayed start service ADR - still in POC phase
- Securing north-south message bus communication
    - https://github.com/edgexfoundry/edgex-docs/pull/656
    - Suggestion is to have a component such as app-services to provide a message bus bridge from an external message bus to an internal message bus or from an external message bus to a command service REST interface. Credentials to authenticate to external message bus would be placed in the EdgeX secret store. Recommend against exposing the EdgeX internal message bus externally due to credential management problem. There is a desire to make sure authentication to central message bus is done from a central service rather than being duplicated across several services.
- Base image patching policy
    - Problem statement:
      EdgeX is building containers with inherited base image vulnerabilities
    - Why?

        - We switched from “scratch” to “alpine” for many images in order to be able to integrate entrypoint hooks for startup sequencing
        - Affected images don’t contain the latest (patched) package versions
        - Base images are based on Alpine 3.14
        - Alpine has no proactive security response team, updates are community supported (http://crunchtools.com/comparison-linux-container-images/), no published-in-advance release schedule. 3.14 image tag hasn’t had a “dot release” since November 2021
        - Container build instructions do not contain “apk update” instructions
            - “apk update” would create reproducibility issues—could result in breaking changes between validation and release
            - “apk update” will increase image size by increasing size of non-cacheable layers
        - Holes
            - We are not pinning the “apk add” instructions (may affect reproducibility)
    - Solution options
        - Document status quo: to produce a vulnerability-free image, users are required to either (a) fork EdgeX and add “apk update” to Dockerfiles, or (b) derive a base image from the official base image that performs an “apk update” to the published image.
        - Add a standardized ARG to the Dockerfile (e.g. ENV=production) that performs the “apk update” when the ARG is set. Require user to build EdgeX from source with a Makefile flag that sets ARG=production. (Also allow users to specify registry target for built images, and do an automatic push of the built image.)
        - Do the above unconditionally. Document that EdgeX images are up-to-date only at the time they are pushed to Docker Hub.
            - Optionally create cron job that rebuilds LTS images on a regular cadence (weekly?) and re-pushes images to Docker Hub.
        - Fully-parameterized base image, passed as ARG. Dockerfiles do not assume presence of package manager but use base image unmodified. Use one of above options to build the base image, or user can bring their own that meets documented minimum tooling requirements. (Pro: maximizes caching of base layers while allowing for base package updates. Con: will have to rework sys-mgmt-agent since it uses nonstandard base image.)
        - Split the security-enabled and non-security-enabled EdgeX and go back to scratch for the non-security-enabled EdgeX images
        - Other options?
    - Longer-term options
        - Alternative images with fewer (i.e. “no”) packages e.g. busybox or base images with more aggressive update schedules (e.g. ubuntu base image) (https://github.com/edgexfoundry/edgex-go/issues/3690)

    - Next steps
        - Research alternative base image (#3690)
        - Roll out “apk update” methodology to update base image to latest package versions. (Watch for CI/CD/Testing issues to see if this causes problems.) (https://github.com/edgexfoundry/edgex-go/issues/3865)
        - Monitor impact to average image size before and after the change.

- Bin list
    - Frashid - snap enhancement for delayed reconfig?
    - Nik Huge - present enhancement request for identity at the edge?

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: Tue Nov 16 05:36:01 UTC 2021
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
    - Awaiting version bump: https://github.com/edgexfoundry/go-mod-core-contracts/pull/663
    - Alpine 3.14 findings - will wait for dot release since 3.14 is an LTS
- Review action items from previous week

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.