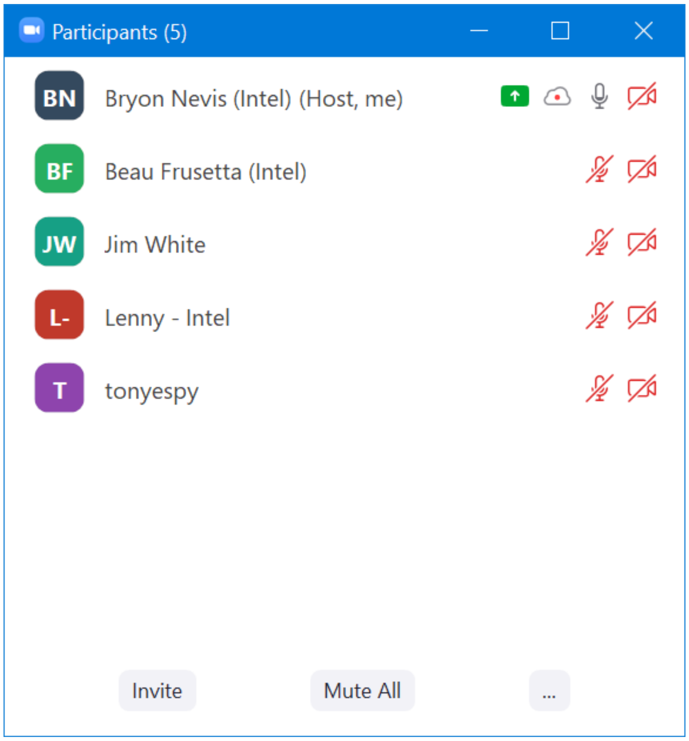
EdgeX Security WG Meeting

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

September 29, 2021

Attendees



Participants (5)

BN Bryon Nevis (Intel) (Host, me)

BF Beau Frusetta (Intel)

JW Jim White

L- Lenny - Intel

T tonyespy

Standing Agenda

- Review Security Board
    - HELP needed for documentation!

Icebox	New	Backlog	WIP	Done
9	2	3	4 / 4	err

- Securing Consul Board

Ph-3 ToDo	Ph-2 ToDo	WIP	Done

7	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)

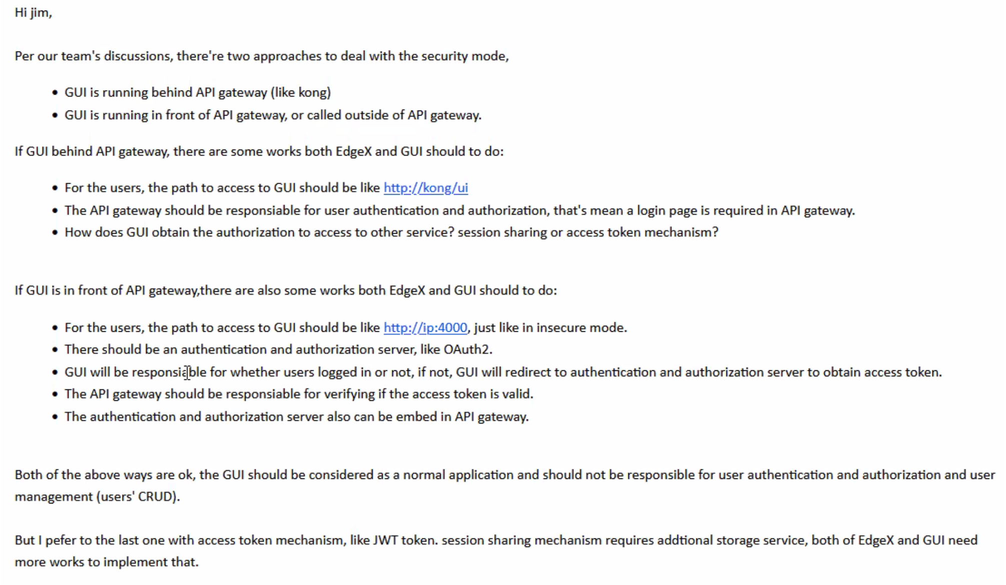
Critical	High	Medium	Low
72	52	29	32

  - Wait for DevOps alpine upgrade.

- Review action items from previous week

Agenda

- Progress:
  - Enabled linters unused, deadcode, ineffassign, gosimple, varcheck
  - Remaining linters to enable: staticcheck, errcheck, gosec
- 9/29: ADR for delay start service secret store token w/demo https://github.com/edgexfoundry/edgex-docs/issues/278
  - Discussed extensively see recording.
- Discuss GUI team's response to security for GUI
  - Jim presented



Hi jim,

Per our team's discussions, there're two approaches to deal with the security mode,

- GUI is running behind API gateway (like kong)
- GUI is running in front of API gateway, or called outside of API gateway.

If GUI behind API gateway, there are some works both EdgeX and GUI should to do:

- For the users, the path to access to GUI should be like http://kong/ui
- The API gateway should be responsiable for user authentication and authorization, that's mean a login page is required in API gateway.
- How does GUI obtain the authorization to access to other service? session sharing or access token mechanism?

If GUI is in front of API gateway,there are also some works both EdgeX and GUI should to do:

- For the users, the path to access to GUI should be like http://ip:4000, just like in insecure mode.
- There should be an authentication and authorization server, like OAuth2.
- GUI will be responsiable for whether users logged in or not, if not, GUI will redirect to authentication and authorization server to obtain access token.
- The API gateway should be responsiable for verifying if the access token is valid.
- The authentication and authorization server also can be embed in API gateway.

Both of the above ways are ok, the GUI should be considered as a normal application and should not be responsible for user authentication and authorization and user management (users' CRUD).

But I pefer to the last one with access token mechanism, like JWT token. session sharing mechanism requires addtional storage service, both of EdgeX and GUI need more works to implement that.

  - AR: Create ticket to figure out how consul UI protects the consul token.

- NEXT WEEK

    - More data on being able to switch in- and out- of insecure Consul mode
    - Review work left for final stretch for Jakarta

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 9/15: ALL: Review #3709 proposal
- 9/15: Lenny: Submit issue for resiliency on Consul token
- 9/15: Bryon: Go back and check with users who requested remote gateway user management and see if they are OK with installing a persistent key of their choice to do this? If not, may have to not rotate kong admin key every boot.
- 9/28: Bryon: Create ticket to figure out how consul UI protects the consul token.