Security WG Meeting, 6/5/19

Attendees: Jim, Brandon, Tingyu (Dell), Bryon, Lenny, Mark, Jim Wang (Intel), Brad (Beechwoods), Tony (Canonical), Malini (VMWare). Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Security Issue Process
    - Updates from Malini
    - Issues list: Web page/Wiki page/Docs location
    - What's next -> implementation
        - ✓ Email address
        - ✓ Web page setup
        - Initial issues list
        - Formation of the SIR
            - Looking for people to serve on this team of 3-4
    - On hold: Exploration of improvements to this process (moved to next WG chair agenda)
        - Offer from Kate Stewart from LF and Zephyr project
        - https://cve.mitre.org/cve/request_id.html#cna_participants
        - Aware of gaps/issues, please provide Malini details.
        - Issues to be addressed in next version
            - Should our policy address releases and when we release when bug fix hits a certain level of security issue.
            - How does Kubernetes and other projects do it?
- Edinburgh "Dot Release" Updates from Tingyu/Brandon/Anthony
    - Secret Store Service work – finished
        - Refactoring to be more in line with other services
        - Moving MongoDB init into this service
        - Big PR (sorry) for review soon
    - Integrate client with Secret Store Service
        - Done - core data (already tested with new secret store service)
            - Core data getting username/password through client through new secret store service.
        - Next - metadata, export client, notifications, logging
    - Update API-gateway structure to be consistent with EdgeX core projects – ongoing
        - Again to be consistent with other EdgeX services – similar to refactor of secret store service
    - go-mod-core-security (the "client" library) - refactor to abstract away from HTTP/addition of unit tests (Look for abstractions and treat services generically with regard to secrets - not just specific to individual service needs)
        - Will be moved to edgexfoundry org soon – but renamed per message from Trevor Conn
    - Still to be done/considered

        - To be considered: move security API Gateway / secret-store into edgex-go (the "mono" repo)
            - Any one for current situation of separate repos: none. Belief it should go to edgex-go / mono repo.
                - More eyes on; catch issues sooner.
                - Location of code should affect BB tests
            - For dot release or Fuji?
                - Separate function from move
                - Function first/then move
        - Move the secret service client library from edgexfoundry-holding are to edgexfoundry organization in GitHub. Awaiting TSC vote.
            - With DevOps, get CI/CD setup
        - Update docker compose file for developer script
        - Add testing cases and docker compose file in black box testing
    - Schedule – still to be determined.
        - Dot release vs just make part of Fuji
        - Dot release at the end of July/first part of August
        - Pass decision to new Chair
        - Those in China and those making product recognize this is a platform and needs finalization.
        - 1.0 – I'd probably wait for 1.1. Especially if it is not an LTS release
        - Therefore – put it all in Fuji versus Dot release
        - Testing cases are a concern. End users may not understand default situations when security is turned on by default.
        - How do we upgrade – how do we provide instructions to users. Possible scripts - update ports, users, etc.
        - EdgeX default will be to have security (API/Secure store) on versus off as it is today.
        - Change Docker compose files around so security is used by default for Edinburgh.
- Fuji work
    - Generation of PKI – Bryon/Jim Wang have started
        - Distribution of per service Vault secrets
    - HW secure storage abstraction layer (design only) – Bryon/Jim Wang & Malini
        - How to protect the Vault Master Key
    - Ensuring the services running are those expected (and authorized) - Malini
        - Design/approach
    - Renew/refresh threat assessment - Tingyu
    - Need document defining what security is/does and can/will do – Jim White/ Tingyu
    - Potentially replacing mongo shell script with Go code – Dell Team
    - Application Services will need access to Vault (through client and Secret Store Service) for tokens/certs/secrets for HTTPS/MQTTS connectivity, cloud access, etc.

New Business

- None