Security WG Meeting, 6/12/19

Attendees: . 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
    - Secret Store Service work – complete (just need PR merged)
    - Integrate client with Secret Store Service (go-mod-secrets)
        - Replicating work with core data to other services
        - Work with DevOps on CI/CD
    - API-gateway structure to be consistent with EdgeX core projects – nearing completion
    - Still to be done
        - move security API Gateway / secret-store into edgex-go (the "mono" repo)
        - Update docker compose files (making security version the default)
        - Move MongoDB init to Go – started (acceleration of effort)
        - Add testing cases and docker compose file in black box testing
    - Schedule – at Tingyu/Malini discretion
        - Work complete for dot release but work group feeling it should just be part of Fuji
        - Does work constitute non-backward compatible change in EdgeX (requiring v2.0)
        - How do we upgrade – how do we provide instructions to users. Possible scripts - update ports, users, etc.
- Other 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