Security WG Meeting, 5/22/19

Attendees: Jim, Anthony, Brandon, Trevor, Tingyu (Dell), Lenny, Bryon, Jim Wang, Beau, Mark A (Intel), Ian (Canonical), Rodney (Beechwoods), Malini (VMWare). Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Security Issue Process
    - Approved by TSC. Official policy located here (for now): https://wiki.edgexfoundry.org/display/FA/Security
    - What's next -> implementation
        - Email address
        - Web page setup
        - Initial issues list
        - Formation of the SIR
    - Exploration of improvements to this process
        - Offer from Kate Stewart from LF and Zephyr project
        - https://cve.mitre.org/cve/request_id.html#cna_participants
- Other LFEdge – not part of EdgeX effort – working on security efforts
    - How can we use what they have worked on?
    - How do we start these conversations?
- Edinburgh Update
    - Moving service access to Vault to a Dot release. Issues in getting it done for this release.
    - Plan of work
        - Client side work
        - c.1. Moving the secret service client library from edgexfoundry-holding are to edgexfoundry organization in GitHub.
            - With DevOps, get CI/CD setup
        - c.2. Apply the secret service client to coredata service for POC.
        - c.3. Retry logic update within the coredata service to adopt the new secret client.
            - When using Vault – if getting secrets fail after retries – stop the service
        - c.4. Add security command line option within coredata service and update the retry logic.
        - c.5. Integration testing with secret service.
        - c.6. Apply the approach to other (database using) microservices (command, metadata, notifications, logging, export client, etc.)
            - Look for abstractions and treat services generically with regard to secrets (not just specific to individual service needs)
        - Server side work
        - s.1. Update secret store and API-gateway structure to be consistent with EdgeX core projects.
        - s.2. Add unit testing cases for secret service.

    - s.3. Update docker compose file for developer script
    - s.4. Add testing cases and docker compose file in black box testing
  - Schedule
    - Dot release at the end of July/first part of August
    - Will this be a dot release if we change APIs? Does it break APIs
    - Will there be a clean upgrade path? What is the migration path?
    - Integration of PKI setup
    - Make sure we don't just do code for dot release if it is going to be scrapped
    - For now: keep working toward dot release until new Chair can work with TSC on position of release.

- Fuji work (as a result of F2F meetings in Seoul)
  - In
    - 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
  - Out
    - Service to service security
      - Implementation of service-to-service communications
    - Securely providing service updates
    - How to securely provision new devices/sensor
    - Device identification and authentication/authorization
    - Hyperledger/blockchain/digital ledger integration
    - Protect data at rest
      - In DB like Mongo
      - In log files
    - Privacy concerns (HIP-A, GDRP, …)

New Business

- Consider: Security API Gateway / secret-store into edgex-go?