Security WG Meeting, 5/29/19

Attendees: Jim, Tingyu, Brandon, Anthony, Trevor (Dell), Malini (VMWare), Rodney (Beechwoods), Bryon, Emad, Jim, Lenny, Beau (Intel), Colin (Kong), Ian, Tony (Canonical), Ike, rdodeja, Eno. 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
  - How does Kubernetes and other open source projects handle it. Malini is working on something for EdgeX. PR ongoing to provide Docs, threat modeling, etc.
  - Aware of gaps/issues, please provide Malini details.
  - Should our policy address releases and when we release when bug fix hits a certain level of security issue.
  - Recommendation from Rodney for serious bugs that we are not allowed to release.
- Edinburgh "Dot Release" Updates from Tingyu/Brandon/Anthony
  - go-mod-core-security work
    - Integration with core data (happy path)
    - 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)
  - Secret Store Service work
    - Refactor to align with Go service standards
    - Complete namespace/secrets structure
      - Tingyu to present design
    - Service keys in namespace should align with those for Consul (from core contracts).
    - Concerns about API changes and where this work lands with regard to dot release, full release, etc. – all to be determined when functionality has been completed.
    - Clarify the last sentences on the last page regarding one copy of the credentials per service.
    - Change interface to structure

  - Still to be done/considered
    - Consider: Security API Gateway / secret-store into edgex-go
    - Client side work
      - Moving the secret service client library from edgexfoundry-holding are to edgexfoundry organization in GitHub.
        - With DevOps, get CI/CD setup
      - 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
      - Add security command line option within coredata service and update the retry logic.
    - Server side work
      - Update API-gateway structure to be consistent with EdgeX core projects.
      - Add unit testing cases for secret service.
      - 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

- Fuji work - no updates today
  - 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

New Business

- None