Security WG Meeting, 5/15/19

Attendees: Jim, Brandon, Trevor, Tingyu (Dell), Bryon, Lenny, Beau, Jim Wang (Intel), Ed S (IoTech), Ike.
Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Edinburgh Update (Tingyu/Brandon)
    - Vault initialization program
        - PR open against master – working issues (abstraction; code style)
    - MongoDB init script
        - Wrapper around original script to handle getting tokens
        - PR to be opened soon
    - Core Services - Access Vault via Go Vault Module
        - Library/module to be used by any secret-needing service
        - Configuration to use or not use vault
        - Working - Micro service command line parameter specifies use of Vault for secrets (flag like "security-service-required")
            - If true – security service must be available, and secrets being obtained from Vault. After that, original bootstrapping.
            - If false – original bootstrapping applies.
        - Need overrides in Docker Compose file – enabled by default and put that in the compose file (especially for Developer edition of compose file)
            - Will effect the blackbox tests (if on by default this will break the tests)
- Fuji Scoping (as a result of F2F meetings in Seoul)
    - In
        - Generation of PKI
            - Distribution of per service Vault secrets
        - HW secure storage abstraction layer (design only)
            - How to protect the Vault Master Key
        - Ensuring the services running are those expected (and authorized)
        - Renew/refresh threat assessment
        - Need document defining what security is/does and can/will do
    - 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

- any