Security WG Meeting, 4/17/19

Attendees: Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Kong on ARM – now in DevOps court
- Docs
    - Securing service secrets – version 7 had no additional comments. Are we good? Can this go to TSC?
    - Security issue process – version 5 includes issue of how to handle dependency security issues. Is this good? Can this go to TSC?
- Tingyu's design of vault initialization and DB initialization still being worked (he is out this week)
- Brandon working on Go Client Module for accessing Vault (see https://github.com/edgexfoundry-holding/go-mod-core-security)
- Fuji roadmapping
    - From https://github.com/bnevis-i/security-secret-store/pull/1 (Thanks Bryon)

Phase 0 (tasks expected to be done in Edinburgh)

1. Create Vault namespace standard for per-service and shared secrets.

Phase 1

1. Develop test infrastructure that simulates EdgeX supported bring-up models supported by System Management Agent.
2. Create PKI at runtime that is unique for each boot (remove static PKI).
3. Block startup of core services until PKI is available.
4. Remove TLS skip-verify overrides from client services.
5. Revoke previously generated tokens on every reboot.
6. Generate per-service tokens at system startup.
7. Revoke Vault root token.
8. Implement Vault cubbyhole response-wrapping.
9. Implement Vault secrets client library (integrate with registration service client library?)

Phase 2

1. Generate unique-per-installation PGP key pair.
2. Derive PGP passphrase with an HMAC-KDF using hardware fingerprint as IKM and random salt.
3. Pass PKI and Vault token secrets via tmpfs volumes.
4. Revoke CA and intermediates after creating leaf certificates.
5. Token issuance driven by service registration.
6. Automated revocation of Vault tokens for failed services.
7. Self-token-rotation (token issuing service).

Phase 3

1. TPM hardware secure storage (unauthenticated) for Vault master key.
2. Use TPM persistent handle and NVRAM for Vault master key.
3. Implement additional TPM authentication scenarios (simple PCR, PCR policy, and (HMAC-KDF?) password).
4. TPM-based PKI.
5. Once-per-boot decryption of Vault master key.
6. Token-issuing-token encryption at rest or recovery of token-issuing-token from HW secure storage.

Phase 4

1. PKCS11 hardware secure storage for Vault master key
2. Implement Mandatory Access Control for EdgeX services.

New Business

- Opens?