Security WG Meeting – 3/6/19

Attendees: Attendees that may have joined after the start of the meeting may not have been captured and listed.

Discussion and action items as a result of meeting in RED

Old Business

- Edinburgh work status
    - Delhi fixes: complete. There were a number of important issues identified shortly after Delhi was released. These have been addressed.
    - Automated testing: complete. Blackbox tests have been implemented for both the API Gateway and Vault. More tests are needed, but the infrastructure is in place, tests are conducted nightly, and minimal testing of the services is in place.
    - Documentation: complete. Introductory documentation along with documentation for both the API gateway and secret store service was added.
    - Hardware based secret storage: ongoing. An effort to define an abstraction around hardware-based storage in support of hardware root of trust options like TPM or TEE was started. After defining this abstraction, the hope was to also produce a reference implementation which used something like a secured file for storage. This work will likely be moved to Fuji.
    - Service to service authentication/authorization: open. Today, communications between services is open. In this release, the hope was to design how service-to-service communications could occur in a more secure way. This work will likely be moved to Fuji.
        - Could we break this apart (authorization vs authentication) all in one release?
    - Move to Go modules: open (has been done??)
    - Upgrade of Kong and Vault: open. In the Delhi release, EdgeX used 0.13 of Kong. Version 1.0.3 of Kong is the latest. An issue was discovered with the plugins. This issue is still being worked with the Kong team. Vault is already at 1.0.2 since Delhi release.
        - Link to issue forthcoming
    - Protecting the Vault master token: open. Vault requires a token to unlock it and use it. This token is left unsecured in the Docker volume and is in plaintext.
    - Securing service secrets in Vault: open – see below. May be a stretch for Edinburgh, but work is beginning.

New Business

Securing Service Secrets in Vault, task list

- Namespace definition(s)
    - Is the general idea – to talk directly to Vault? Yes, at least for this release.
- General micro service Vault access and client module design
- Configuration on Vault location and access credentials needs to be provided to each using micro service
- Service bootstrapping needs to be modified to instantiate a Vault client & get access token
    - Additional considerations as part of this design:
        - PKI initialization problem (Bryon)
        - PKI gets done at container build time and it should be part of runtime initialization
        - Docker vs Snap vs other topology considerations (Ian, Toby and others)
- Client code to use Vault to get config secrets needs to be implemented
- Add code to system management general client (vs SMA as we really want to protect the services from serving up secrets) responders so that secret settings are not sent to SMA
    - Don't change SMA just change service in how they respond
- Testability – consideration - how do we add automation for testing this?
- Usability – it's important that this be easy to implement and to use in other services from a developer's perspective (Rodney & Trevor)

Tingyu is working on the name spacing and a general module (client) design for use in the micro services. Target is to have something to review in one or two week's time.

- About a 50/50 split on opinion to require securing service secrets for v1.0. Jim to circle back with a larger swath of the community and project leadership
- Suggestion: maybe we can look at 3rd party option to make it quick/easy (Toby) – and that is why hardware storage was an important step to provide before this (Tony). Jim/Tingyu to layout some strategy options and ideas in the future meetings.

CVE needs to be considered (Bryon) – separate discussion that has come up in various release issues this dev cycle. We really need something in place for EdgeX LTS.

- CVE – this is an all EdgeX issue – not just related to security store.
    - Needs be part of the LTS policy
    - Need a process and how to get bug fig and LTS dot release or patch
    - What we could do is set up a security email address and a group to address security bug reported to the community
    - Release can include a plan to address CVE issues
    - Jim to try to formulate crawl steps for this body to review and work for Edinburgh

Question on Code quality checks and static analysis – is an issue being worked by James Gregg (not for Edinburgh release says Lisa)