EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

April 13, 2022

Attendees

<table>
<thead>
<tr>
<th>Participant</th>
<th>Role/Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN</td>
<td>Bryon Nevis (Intel) (Host, me)</td>
</tr>
<tr>
<td>JW</td>
<td>Jim White</td>
</tr>
<tr>
<td>L</td>
<td>Lenny - Intel</td>
</tr>
<tr>
<td>T</td>
<td>tonyespy</td>
</tr>
<tr>
<td>FT</td>
<td>Farshid Tavakolizadeh - Canonical</td>
</tr>
<tr>
<td>JW</td>
<td>Jim Wang (Intel)</td>
</tr>
</tbody>
</table>

Agenda

- SPIFFE/SPIRE Delayed Start ADR Status Update
  - configuration.toml updates rolled out in edgex-go
  - Conditional compilation updates working their way through
    - Blocked on Lenny’s PR
    - Next step would be makefile changes to disable spiffe in the core services
  - Still investigating compatibility with Snap deployment
    - Not entirely sure if can do the workload attestation in snaps because the snap mount path includes the revision number in the path – can the SPIFFE server support path wildcarding?
    - To run experiments to see if wildcard paths are supported
  - Summary: on track for docker…. TBD for snaps
- EdgeX Ireland shuts down after 168h when security is enabled (hits Vault default_lease_ttl) [https://github.com/edgexfoundry/edgex-go/issues/3963](https://github.com/edgexfoundry/edgex-go/issues/3963)
  - Description of the default_lease_ttl and max_lease_ttl [https://learn.hashicorp.com/tutorials/vault/tokens#ttl-and-max-ttl](https://learn.hashicorp.com/tutorials/vault/tokens#ttl-and-max-ttl)
  - Failure scenario:
    - Vault service tokens hit lease ttl and are automatically expired
    - Expiration of vault token causes consul token to be revoked
    - Go-mod-configuration's Writeable watcher fails because Consul token is no longer valid
    - Ireland not fixable; Jakarta has security token retry logic
  - Proposed fix
    - Add a timer to security-secretstore-setup to push new tokens out to the secrets volume prior to expiry of default_lease_ttl
    - Look into making it easier to extend the default lease
    - Make security-secretstore-setup behavior dynamic based on the lease_ttl that is currently in use
    - Try to have a fix prototyped for April 20
    - Triage as part of pre-planning on the 20th.
    - Will need to have a Jakarta LTS release

- Bin list
  - May 11: NetFoundry is starting a project called OpenZiti that provides a link library to secure service communications via a link library with multiple language bindings.
  - Rebuild Jakarta docker images to refresh base images post-Kamakura
  - AR: Bryon. Tabulate the current state of the Jakarta images
  - Nik Huge - present enhancement request for identity at the edge?

**Standing Agenda**

- [Review Security Board](#)
- [Securing Consul Board](#) (skip)
- [Review CIS docker scan](#) (will skip unless something changes) (click latest run, go to classic, view console output).
  - Last checked: Tue Nov 16 05:36:01 UTC 2021
- [Review Snyk (Jenkins)](#) (will skip unless something changes) ([Imagelist](#))
  - [https://app.snyk.io/vuln/SNYK-GOLANG-GOLANGORXTENSITYINTERNALLANGUAGE-2400718](https://app.snyk.io/vuln/SNYK-GOLANG-GOLANGORXTENSITYINTERNALLANGUAGE-2400718)
- build(deps): bump github.com/go-playground/validator/v10 from 10.10.0 to 10.10.1 #706 merged yesterday
- Review action items from previous week

Action Items

- 7/14/21: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.