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

March 16, 2022

Attendees

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN</td>
<td>Bryon Nevis</td>
</tr>
<tr>
<td>L.</td>
<td>Lenny</td>
</tr>
<tr>
<td>FT</td>
<td>Farshid</td>
</tr>
<tr>
<td>JW</td>
<td>Jim Wang</td>
</tr>
<tr>
<td>T.</td>
<td>tonyespy</td>
</tr>
</tbody>
</table>

Agenda

- Discussion (JimW): Configuration options for SPIFFE trust domain
  - Env var is needed to configure SPIRE support containers
  - EdgeX services have a choice:
    - Configuration.toml with env var override?
    - Env var override all the time?
  - Decision: Add SPIFFE trust domain to configuration.toml, default to edgexfoundry.org, override if necessary
    - Add TrustDomain key to RuntimeTokenProviderInfo
    - Rename spiffe-token-provider toml to use SPIFFE.TrustDomain instead of Spiffe.TrustDomain.Hostname
    - Change spire server/agent components to use SPIFFE_TRUSTDOMAIN instead of SPIFFE_TRUST_DOMAIN.
    - While we’re at it. Use SPIFFE.EndpointSocket instead of the extra layer.
• Config for go-mod-secrets
  ■ [Secretstore]
  ■ [SecretStore.RuntimeProvider]
  ■ TrustDomain = edgexfoundary.org
  ■ SECRETSTORE_RuntimeProvider_TRUSTDOMAIN=edgexfoundry.org

• Config for security-spiffe-token-provider:
  ■ [SPIFFE]
  ■ [SPIFFE.TrustDomain]
  ■ Hostname = edgexfoundry.org
  ■ [SPIFFE]
  ■ TrustDomain = edgexfoundry.org

• Containers (for configuring spire server components)
  ■ SPIFFE_TRUST_DOMAIN=edgexfoundry.org
  ■ SPIFFE_TRUSTDOMAIN=edgexfoundry.org

• Expose Consul [https://github.com/edgexfoundry/edgex-go/issues/3744](https://github.com/edgexfoundry/edgex-go/issues/3744)
  ○ No progress on option 1 (expose Consul via Kong)
  ○ Consul does not automatically generate a self-signed TLS certificate (option 2)
  ○ edge-compose#221 opened to revert prior change (option 3)
  ○ Escalated PR merge failure to TAF team.

• Bin list
  ○ 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](#))
  ○ 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.