EdgeX Security WG Meeting

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

January 11, 2023

Attendees

TSC Update

- STRIDE Threat Model hopefully merge today or in the next day or two
• Fix for GHSA-xrjj-mj9h-534m and GHSA-69ch-w2m2-3vjp bubbling through with go-mod-secrets update
• Microservice authentication UCR voting underway (docs#920). ADR updates next.
• OpenZiti and Vault JWT authentication prototypes are well along
  ○ JWT prototype: 80MB RAM saved (160->80), 329MB images saved (docker, 353->24)
  ○ OpenZiti: no numbers yet (docker stats, docker images) before and after

Opens
• Clint to demo OpenZiti
  ○ Have added OpenZiti to go-mod-bootstrap

```
for serviceKey, serviceInfo := range config.GetBootstrap().Clients {
    var url string
    var err error

    if len(serviceInfo.ZeroTrustOptions) > 0 {
        idFile, ok := serviceInfo.ZeroTrustOptions["IdentityFile"]; ok {
            _, err := ziti.LoadContext(idFile)
            if err != nil {
                panic(err)
            }
        }
    }
}
```

```
[Clients]
[Clients.core-metadata]
Protocol = "http"
Host = "localhost"
Port = 59881

[Clients.core-metadata.ZeroTrustOptions]
IdentityFile="c:/temp/svc.core-command.identity.json"
```

○ With this change, outgoing requests will go over a zero trust transport.
○ For listeners:

```
.CORSExposeHeaders = "Cache-Control, Content-Language, Content-Length, Content-Type"
.CORSMaxAge = 3600
[Service.ListenOptions]
IdentityFile="c:/temp/svc.core-command.identity.json"
ServiceName="svc.core-command"
```
Connecting to UI over zero trust network:

Note: despite connecting to port 4000, there is no listening port on 4000:
Discussion to follow
- Limitation: Can’t Zitify non-edgeX services like Redis, Mosquitto, etc easily without using LD_PRELOAD.
  - Leaves a hole for cross-network communication
  - Could send the external services via a tunneler
- Using Vault to control access to zero trust overlay
  - Need to distribute PKI
- Overlay will require controller and a router
  - Clint’s perspective: would naturally assume an OpenZiti network already exists
- THINK ABOUT
  - What if EdgeX provided multiple compose files that needed to be run to bring up an EdgeX system
    - Base services: redis, mosquitto, consul, etc
    - Zero trust: openziti router and controller
    - EdgeX services themselves: data, metadata, command, …
  - Current limitation: Openziti must always read key and certificate off of disk. If get key/cert from vault, need to buffer it on disk.

Standing Agenda
- Review Security Board
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
  - Last checked: August 3, 2022 – as expected
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
- 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.