EdgeX Security WG Meeting

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

May 11, 2022

Attendees

![Attendee List]

Agenda

- Clint Dovholuk @ NetFoundry presenting OpenZiti as a possible solution to EdgeX microservice security.
Warning – ‘Secure networking is an Oxymoron’

“The most dangerous phrase in the language is ‘we’ve always done it this way.’”
- Grace Hopper

NetFoundry and OpenZiti change impossible into standard

**SaaS platform:** Consumption-based, fully managed SaaS, backed by SLAs and field-proven performance. Providers can white label to start selling immediately.

**Open source:** Provides ultimate extensibility to embed in anything – app, host, network. NetFoundry continues to be the leading contributor.

*Use both as software.* API-first and cloud native without infrastructure or cloud dependencies.

This enables both your journey and destination.
“THE BEAST” VS “MAD MAX”

APP EMBEDDED SUPERPOWER: ADDRESSABILITY

Before OpenZiti:
FROM: 192.168.2.3
CO: my.application.server
TO: 100.64.0.15

After OpenZiti:
FROM: Clint
TO: Jenkins
APP EMBEDDED SUPERPOWER: SEVERSIDE TOO!

APP EMBEDDED SUPERPOWER: SERVER TO CLIENT
ChaChaPoly1305 (libsodium) - no current algorithm flexibility
EXISTING ZITIFIED APPS

Apps Successfully Zitified

- ZSSH
- ZSCP
- Mattermost
- Webhooks Github/Gitlab
- Generifed JDBC Wrapper - ZDBC
- Kubeztl
- Helmz
- Prometheus

Blog:
https://ziti.dev/blog/zitifying-ssh/

Uses:
Golang SDK

By:
Jon Kochanik

GitHub:
openziti-test-kitchen/zssh/tree/main/zssh
- Augments scp/sshd. Replaces local scp client app
- Covers basic functionality not advanced usage
- Features Use of Addressable Terminators
  zscp ziti-identity-name/remote-file /local-path

EXISTING ZITIFIED APPS

Apps Successfully Zitified

- ZSSH
- ZSCP
- Mattermost
- Webhooks Github/Gitlab
- Generifed JDBC Wrapper - ZDBC
- Kubeztl
- Helmz
- Prometheus

Blog:
<coming soon>

Uses:
Golang SDK

By:
Nick Piers / Clint Dovholuk

GitHub:
openziti-test-kitchen/prometheus
- Monitor workloads via zero trust connection
- Rebuild/fork of prometheus project
- Installable via helm
  - helm repo add netfoundry
  - https://netfoundry.github.io/charts/
Has a C SDK (est 1MB overhead)
Has a GO SDK
Has flexible policies that can check for antivirus present, mac addresses, etc.

Enrollment process:

- Can bring your own CA
- Can integrate with SPIFFE
- Controller is the root of trust that bootstraps a full PKI
- Quickstart creates a PKI
- Create an identity which is a JWT
- JWT is distributed out of band
- JWT is one time use
- Create private key on the client. Connects to well-known endpoint to trust the server. Uses JWT to authorize CSR and returns certificate. Identities are X.509 based.
- With SPIFFE in play can use 3rd party CA feature, can make Ziti automatically trust the SPIFFE cert.
- Benefits of Ziti used with spire
  - Privacy of the ziti network overlay
  - Lacks of ports
  - Portability (outbound internet)
- Edge routers are the nodes that have the open ports. These are mTLS authenticated.
All communication go through the Edge Router. Clients connect to the edge routers that talk the fastest. The Edge router gets you to the Ziti network fabric. Can have a fabric of one edge router if needed.
Have had a conversation about Nats.io potentially adopting openziti.

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)
- 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.