CASABLANCA SECURITY ENHANCEMENTS FOR 5G USE CASE

- 5G Use Case A : Deployment
- 5G Use Case C : Optimization

Meeting Minutes May 17, 2018

Casablanca 5G Use Cases with Security Impacts

5G Use Case A Deployment :

PNF Plug and Play (PnP) Registration

- JSON encoded asynchronous Registration event sent via HTTP/TLS from PNF to DCAE.

Configuration Management (CM)

- SSH from ONAP Controller to NF for CM using NetConf or Ansible.

5G Use Case C Optimization :

Bulk Performance Measurements (PM)

- JSON encoded asynchronous Bulk PM (Option 1) or File Ready (Option 2 & 3) event sent via HTTP/TLS from NF to DCAE.
- SFTP or HTTPS from ONAP File Collector to NF for Bulk PM file transfer (Option 2 & 3).

Real Time Performance Measurements (RTPM)

- GPB encoded asynchronous RTPM event streamed via TLS/TCP from NF to DCAE.

Fault Management (FM)

- JSON encoded asynchronous Fault event sent via HTTP/TLS from NF to DCAE.

Security capabilities needed in ONAP for Casablanca

HTTP

- Recommend that ONAP eliminate username and password for HTTPS.

TLS

- DCAE is able to authenticate Vendor or Service Provider X.509v3 certificate for TLS connection.
- ONAP User is able to install Vendor Root CA certificate as trust anchor in ONAP.
- ONAP supports 3 level chain (Root CA, Sub CA and End-Entity certificates).
- Vendor is able to install ONAP Root CA as trust anchor on NF for mutual TLS authentication.

CA

- Provide CA services to NFs in ONAP for development and testing; enrollment, authentication.
- Support CMPv2 for NF for certificate enrollment and end-entity key renewal in ONAP for development and testing.
- Support integration with Service Provider CA/PKI in ONAP.

SSH/SFTP

- Create RSA public/private key pair for ONAP Controllers and File Collector (Option 2) to use for SSH/SFTP access into the NF for CM/PM.
- Provision SSH username/public key on NF for Ansible or NetConf access from ONAP Controllers for CM and SFTP from ONAP File Collector for Bulk PM (Option 2).
- Recommend that client should not accept username and password for SSH authentication.

Impacted ONAP Projects: AAF, DCAE, Controllers

Discussion Points

General

- Goal for these meetings is to identify:
  - Assumptions that impact ONAP security capabilities and NF requirements
  - Recommendations for the Security Subcommittee
  - Requirements for ONAP and NFs
  - Project impacts for Casablanca

HTTP

- Agreed to the following Recommendations:
  - ONAP shall not support username and password authentication for HTTPS; certificate authentication only.
  - ONAP shall not support HTTP for communications between ONAP components or between NFs and ONAP components, except for NF certificate enrollment over CMPv2.
  - ONAP components and NFs shall support TLS for security of HTTP connections.
- Performance is no longer an issue and is not a valid excuse for not using TLS.
- CMPv2 uses HTTP and must be allowed for certificate enrollment.

Discussion Points

TLS

- NF Authentication
  - DCAE must be able to authenticate NF’s Vendor or Service Provider X.509v3 certificate for TLS connection.
    - DCAE needs its own end-entity X.509v3 certificate.
    - DCAE needs to use CADI to authentication the NF certificate.
  - Root CA certificate for the NF end-entity certificate must be installed in the DCAE trust store.
    - This can be done manually if the Root CA certificate is not already part of the trust store.
    - CADI can be used to manually install the Root CA certificate, but is not required.
    - Instructions for installing Root CA certificates in the trust store must be provided in Casablanca.
  - CADI can be used for further certificate authentication if desired.
    - A list of valid Sub CA Subject names can be provisioned in the DCAE trust store and CADI can verify that the NF end-entity certificate was signed by a valid Sub CA. This is optional.
  - Sub CA certificate is not required in DCAE trust store.
    - However, some Service Providers may choose to require this extra level of security in their own commercial deployments of ONAP, depending on its security policies. This topic is not for Casablanca.

Discussion Points

TLS

- NF Authorization
  - CADI can be used for authorization of NF, however we do not recommend/require that CADI is used for NF authorization; too much overhead, it is not scalable to provision every NF instance and its permissions into CADI.
  - Authorization of NF can be achieved via NF onboarding and service instantiation processes.
    - This provides a list of VES events that the NF emits, NF instance ID, NF IP address and other information that is stored in AAI and can be used by DCAE to verify that the NF is authorized to send certain asynchronous events to DCAE.
    - Are there DCAE impacts for this?
- DCAE Authentication by NF
  - NF must be able to authenticate the DCAE certificate for mutual TLS authentication.
  - ONAP Root CA certificate must be installed as trust anchor on NF when the DCAE end-entity certificate is signed by ONAP CA.
    - Root CA certificate can be manually pre-provisioned in NF before any TLS connection is set up.
    - NF could accept the Root CA certificate one time the first time the TLS connection was set up; for example during Plug and Play of a PNF when the PNF Registration event is sent from the NF to DCAE. What happens when NF sends the PNF Registration event a second time?
  - NF can configure TLS to accept a Root CA certificate the first time or not. Choice is left to the vendor and/or service provider, depending on its security policies.

Discussion Points

CA

- Assumptions
  - ONAP CA is used to sign DCAE and NF end-entity certificates during development and testing.
  - For commercial deployment, it is expected that each Service Provider has its own CA/PKI and the Service Provider Root CA/Sub CA is used to sign DCAE and NF end-entity certificates.
  - 3GPP compliant NFs use CMPv2 for certificate management; enrollment, key renewal.

SSH/SFTP

- Authorization of ONAP access in NF
  - How does the NF authorize the ONAP components (e.g. Controller) to ensure that the access is limited to allowed operations, directories, etc. inside the NF; for example, will LDAP be supported?
  - Needs further discussion in a future meeting.