CASABLANCA SECURITY ENHANCEMENTS FOR 5G USE CASE

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

Meeting Minutes May 31, 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, NF Requirements

Meeting Minutes – May 17, 2018

Attendees

- Pierre Close (AT&T)
- Gunner Forssell (Ericsson)
- Jonathan Gathman (AT&T)
- Marge Hillis (Nokia)
- Linda Horn (Nokia)
- Samuli Kuusela (Ericsson)
- Vesa Lehtovirta (Ericsson)
- Zygmunt Lozinski (IBM)
- Natacha Mach (Orange)
- Gervais-Martial Ngueko (AT&T)
- Pawel Pawlak (Orange)
- Alex Salvarani (Nokia)
- Randy Stricklin
- Stephen Terrill (Ericsson)
- Amy Zwarico (AT&T)

Apologies to those I missed or misspelled. Let me know and I can update the list.

Discussion Points – May 17, 2018

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 components and NFs shall support TLS for security of HTTP connections.
  - ONAP shall not support HTTP for communications between ONAP components or between NFs and ONAP components, except for NF certificate enrollment over CMPv2.
- CMPv2 uses HTTP and must be allowed for certificate enrollment.
- Performance is no longer an issue and is not a valid excuse for not using TLS.
- Project impacts: VNF Requirements, VES Listener document, DCAE

Discussion Points – May 17, 2018

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.
    - **AI: Determine** if DCAE already supports this or if there is work needed in Casablanca for this item. **Status: In Progress** Email sent to DCAE; awaiting response.
  - 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. Some instructions are already available on the wiki.
    - No work needed in Casablanca for this item.
  - 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 their security policies. This topic is not for Casablanca.
    - No work needed in Casablanca for this item.

Discussion Points – May 17, 2018

TLS

- NF Authorization
  - CADI can be used for authorization after certificate is authenticated.
    - 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.
  - CADI may be too much overhead for NF authorization; 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 – May 17, 2018

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.

Meeting Minutes – May 21, 2018

Attendees

- Olaf Burdziakowski (Nokia)
- Gunner Forssell (Ericsson)
- Marge Hillis (Nokia)
- Linda Horn (Nokia)
- Thomas Ingemarsson (Ericsson)
- Samuli Kuusela (Ericsson)
- Alexander Pantus (Ericsson)
- Alex Salvarani (Nokia)
- Stephen Terrill (Ericsson)
- Maciej Wejs (Nokia)
- Amy Zwarico (AT&T)

Apologies to those I missed or misspelled. Let me know and I can update the list.

Discussion Points – May 21, 2018

TLS

- NF Authorization
  - NF Authorization can be achieved via NF onboarding and service instantiation processes.
    - A list of VES events that the NF emits is provided, 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.
  - The typical way for DCAE to authorize ONAP users and components is via CADI.
    - There is some concern that it is not scalable to manually provision every NF instance and its roles and permissions into CADI prior to the first NF TLS connection into ONAP.
    - Can we provision NF roles, permissions and instances into AAF automatically at onboarding and service instantiation time?
      - At onboarding, NF provides artifacts with list of events the NF emits. A role could be created in AAF per NF Type with permissions that include sending these VES events to DCAE. What projects are impacted for this; SDC, AAF?
      - At instantiation, the unique NF instance ID becomes known. This "user" could be added to AAF and assigned to the role created at onboarding. SO workflow and/or DCAE would need to include updating AAF. What projects are impacted for this; AAF, SO, DCAE?
      - What is the "user" for a NF? UUID? NF Name in AAI? Choice determines when CADI must be updated; e.g. instantiation, restart, SW upgrade.
    - **AI: AAF team** to identify what information is needed for CADI to authorize a NF and what can be automated. **Status: In Progress** Jonathan and Amy to develop a proposal.

Discussion Points – May 21, 2018

TLS

- NF Authorization (continued)
  - Could we use Pluggable Authentication to authorize NFs instead of CADI?
    - CADI would be configured to point back to DCAE for authorization.
  - Need to consider the complexity of the authorization solution to:
    - DCAE
    - Onboarding process
    - Instantiation process
    - Service Provider
  - Need to consider the automation of the solution:
    - We can not have manual steps at run time (during instantiation) and that is the first time ONAP knows the NF instance ID (user)
    - We could tolerate manual steps at design time.
  - Need to consider how we could phase the final “ideal” solution over time if it can’t all be completed in Casablanca.
    - Identify some steps that make sense.

Discussion Points – May 21, 2018

TLS

- DCAE Authentication by NF
  - NF must be able to authenticate the DCAE certificate for mutual TLS authentication.
  - If DCAE and NF certificate are signed by the same CA (ONAP or Service Provider (SP) CA) then there is no problem.
  - If NF certificate is signed by Vendor Factory CA and DCAE certificate is signed by ONAP/SP CA, then ONAP/SP Root CA certificate must be in NF trust store.
    - ONAP/SP Root CA certificate can be manually pre-provisioned in NF before any TLS connection is set up. But this does not work for Plug and Play (PnP) of PNFs.
    - NF could accept the Root CA certificate one time the first time the TLS connection was set up; for example during PNF PnP when the PNF Registration event is sent from the NF to DCAE.
      - What happens when NF sends the PNF Registration event a second time? Is the Root CA certificate still valid?
      - 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.
  - To avoid this situation, ONAP could require that NFs perform operator certificate enrollment before the first TLS connection.
  - **AI: Check** SOL002 and SOL004 to see if this problem has already been solved. **Status: Closed May 24** SOL002 and SOL004 do not address these kind of certificate issues.

Discussion Points – May 21, 2018

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?
  - LDAP is the 3GPP standard according to TS 33.310.
    - Many Service Providers have LDAP systems in place.
  - However, LDAP is difficult to manage and the world is moving away from it to simpler protocols.
    - Consider HTTP Server as an alternative.
    - 3GPP standard needs to be updated and/or softened with regard to LDAP.
  - VNF Requirements do not specify what protocols must be supported for Identity and Access Management (IDAM).
    - **AI: Propose** protocols for IDAM to Amy Zwarico. **Status: Closed** LDAP and HTTP recommended. See details in May 24 meeting minutes.
    - Consider what vendors and service providers currently support as well as where the industry is heading.
    - LDAP should be one of the supported protocols to support legacy systems.

Discussion Points – May 21, 2018

Certificate chaining

- Recommend that ONAP components and NFs support 3 levels of certificate chaining; Root CA, Sub CA, End-entity. This is already supported in ONAP.
- No work needed in Casablanca for this item.

VNF Certificates

- Need a scenario specified for how and when VNFs get their certificates.
  - Must happen before the first TLS connection.
  - What is used as the CN? Choice of CN determines when a new certificate is needed.
    - If it is UUID, then a new certificate is needed every time VNF is restarted or SW upgraded. Certificate enrollment must be part of instantiation.
    - If it is VNF Name, then the certificate must be persistently stored over VNF restart and SW upgrade.

Meeting Minutes – May 24, 2018

Attendees

- Masoud Asadi (Ericsson)
- Pierre Close (AT&T)
- Gunner Forssell (Ericsson)
- Jonathan Gathman (AT&T)
- Marge Hillis (Nokia)
- Linda Horn (Nokia)
- Thomas Ingemarsson (Ericsson)
- Samuli Kuusela (Ericsson)
- Natacha Mach (Orange)
- Jonathan Olsson (Ericsson)
- Alex Salvarani (Nokia)
- Kazi Wali Ullah (Ericsson)
- Maciej Wejs (Nokia)
- Amy Zwarico (AT&T)

Apologies to those I missed or misspelled. Let me know and I can update the list.

Discussion Points – May 24, 2018

Recommended Protocols in NF for Identity and Access Management (IDAM).

- When certificates are used, LDAPv3 shall be supported as the primary method of authorization of a NF in ONAP.
- When certificates are used, HTTP shall be used as an alternative method of authorization of an NF when LDAP is not available.
- LDAPv3 format or HTTP format shall be used to access file repositories of TLS certificates.
- LDAPv3 and HTTP formats shall be supported for checking the revocation status of TLS certificates.

LDAP

- PROS
  - 3GPP standard according to TS 33.310
  - Supported by all PKI products today
  - Flexible
  - Scalable
- CONS
  - Complex

HTTP

- PROS
  - Simple
  - Low cost and maintenance
- CONS
  - Not supported by all PKI products, although widely supported

Discussion Points – May 24, 2018

Other Protocols to consider for Identity and Access Management (IDAM).

- Should TACAS, TACAS+, DIAMETER, RADIUS protocols be considered?
  - If authorization of ONAP Controller in NF uses the Controller certificate (e.g. TLS), these protocols are not an alternative to LDAP or HTTP because they don't handle certificate functions such as revocation.
    - Certificates optionally have Distribution Points (DPs) where an authenticator can check if a certificate has been revoked. DPs support LDAP and HTTP formats.
  - If authorization of ONAP Controller in NF does not use Controller certificate (e.g. SSH), these protocols may be useful.

Provisioning SSH Public Keys in NF

- Recommendations for SSH authentication:
  - When SSH/SFTP is used, public key authentication shall be supported by NF to authenticate ONAP access; password authentication shall not be supported for SSH/SFTP access into the NF.
- SSH is used for Configuration Management (CM) and Life Cycle Management (LCM) with NetConf, Ansible or Chef.
  - For VNFs, SSH public keys are passed during instantiation.
  - For PNFs, how are SSH public keys provisioned? There is a bootstrapping problem if SSH is used as the Configuration Management transport protocol. Possible provisioning options :
    - Pass it during PnP in the DHCP response
    - Provision it during PnP from the Initial EM (PnP Server)
    - Provision it manually on-site during installation

Discussion Points – May 24, 2018

Recommendations for NetConf transport protocol – TLS or SSH

- ONAP shall support both TLS and SSH as the transport protocol for NetConf.
- TLS shall be the preferred transport protocol for NetConf.
- How would the Controller know which to use for a NF? Recommendations:
  - It shall be possible to specify the configuration management protocol supported by a NF at design time (NetConf/TLS, Netconf/SSH, Ansible/SSH or Chef/SSH).
  - If a configuration management protocol is not specified for a NF, ONAP shall try NetConf/TLS first as the default.
    - This is so Service Providers do not have to configure things which are default.
  - As an option, ONAP Controllers could also try other CM protocols in some priority order if NetConf/TLS fails. This is left to the Controller designers to decide.

NetConf/TLS

- PROS
  - Uses certificates for authentication; don't need to provision SSH public key for CM; eliminates the bootstrapping problem.
- CONS
  - Not widely used with NetConf now; may have trouble finding a third party NetConf product that supports TLS.
  - Still have to solve the SSH public key provisioning problem for Ansible for LCM; but can use NetConf/TLS to configure the SSH public key for Ansible so no bootstrapping problem.

Discussion Points – May 24, 2018

VNF Certificates

- Need a scenario specified for how and when VNFs get their certificates.
  - Must happen before the first TLS connection.
  - Recommend that VNF certificate enrollment happens automatically as part of instantiation.
- VNF Certificate Enrollment Options
  - VNF SW image comes with a default certificate to use for enrollment. Rejected as not secure.
  - Check SOL005. It has standards for generating keys and certificates for VNFs.
  - One time password for VNF to use during enrollment. **AI: Ericsson** to present a proposal for this option on May 31. **Status: Closed** Ericsson presented on May 31 and presentation is posted to wiki.
  - ONAP (potentially SO with the help of CertMan) generates a key pair, performs enrollment and installs a PKCS#12 bundle on the VNF. **AI: AT&T** to present a proposal for this option. **Status: In progress** AT&T to present on Jun 7.
    - Does SO have the authority to generate a key pair and perform cert enrollment for the VNF?
    - How is the PKCS#12 installation done; what component, protocol, API is used?
- What is used as the CN for a VNF? Choice of CN determines when a new certificate is needed.
    - If it is UUID or some identity that changes for each instantiation, then a new certificate is needed every time VNF is restarted or SW upgraded. Certificate enrollment must be part of instantiation. This is ideal - simple.
    - If it is VNF Name or some identity that is persistent when a VNF is re-instantiated, then the certificate must be persistently stored over VNF restart and SW upgrade. Not ideal - complex.

Discussion Points – May 24, 2018

NF Authorization

- DCAE must ensure that NF is authorized to send VES events to DCAE. It is not enough to authenticate the NF certificate for the TLS connection.
- The typical way for DCAE to authorize ONAP users and components is via CADI.
  - Recommend that NF roles, permissions and instances are provisioned into AAF automatically at onboarding and service instantiation time.
    - At onboarding, NF provides artifacts with list of events the NF emits. A role could be created in AAF per NF Type with permissions that include sending these VES events to DCAE. What projects are impacted for this; SDC, AAF?
    - At instantiation, the unique NF instance ID becomes known. This "user" could be added to AAF and assigned to the role created at onboarding. SO workflow and/or DCAE would need to include integration with AAF. What projects are impacted for this; AAF, SO, DCAE?
  - What is the "user" for a NF? UUID? NF Name in AAI?
    - Choice determines when AAF must be updated; e.g. instantiation, restart, SW upgrade.
    - At each instantiation, create user and potentially roles and permissions.
    - At each termination, remove user and potentially roles and permissions.
- **AI: AT&T (Amy and Jonathan)** to present a proposal at a future meeting.

Meeting Minutes – May 31, 2018

Attendees

- Masoud Asadi (Ericsson)
- Pierre Close (AT&T)
- Marge Hillis (Nokia)
- Linda Horn (Nokia)
- Thomas Ingemarsson (Ericsson)
- Samuli Kuusela (Ericsson)
- Vesa Lehtovirta (Ericsson)
- Zygmunt Lozinski (IBM)
- Henry Thorpe
- Amy Zwarico (AT&T)

Apologies to those I missed or misspelled. Let me know and I can update the list.

Next Meeting Thu Jun 7, 2018 at UTC 13:00, Eastern 8:00

Discussion Points – May 31, 2018

Ericsson presented a proposal for PNF and VNF certificate enrollment. See the presentation posted to the wiki for details. Next 2 slides contain a brief summary of the discussions.

- PNF Certificate Enrollment
  - Occurs during Plug and Play (PnP) and follows 3GPP TS 32.508.
  - PNF uses its vendor certificate for identity, authentication and authorization to the CA. Vendor Root certificate must be pre-provisioned in the CA. This procedure is outside of ONAP (unless the CA is the ONAP CA used for development and testing).
  - Should scenarios that occur outside of ONAP, but are needed for NF operation, be documented somewhere in ONAP? Examples: PNF PnP, certificate operations (enrollment, renewal, CRL)
- ONAP CA certificate functions
  - ONAP CA is only used for development and test; Service Provider CA is used for production.
  - 3GPP devices use CMPv2 for certificate operations to a CA.
  - What certificate functions/protocols does the ONAP CA need to perform for NFs in the dev/test environment?
    - enrollment via CMPv2 – would be nice to have
    - CRL and renewal – maybe not necessary

Discussion Points – May 31, 2018

- VNF Certificate
  - VNF Certificate Enrollment follows ETSI standards: SOL002, SOL003, SOL005, IFA006, IFA007.
  - PKCS#12 container can be installed on the VNF at instantiation time OR
  - VNF can perform certificate enrollment with a One Time Password (OTP):
    - The OTP, which is a Pre-Shared Key (PSK), is generated by the CA and provisioned on the VNF at instantiation.
    - VNF uses the OTP for identity, authentication and authorization during enrollment with the CA.
    - CMPv2 is used for enrollment; PSK is used to sign the Certificate Signing Request (CSR).
    - Pre-provisioning is necessary to generate the PSK before the VNF is instantiated. This is just one part of the larger network planning exercise that must be completed before a gNB is deployed.
- Secure Boot
  - 3GPP NFs validate the SW running on the HW during startup.
  - A trusted anchor, including the public key, is used to validate the signed SW.
  - Only validated SW is allowed to run.
  - Initial boot SW and all subsequent SW upgrades are validated.