**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220062-r2***

e-meeting, 14 - 25, February 2022

**Source: MITRE**

**Title: New Solution: Confidentiality, and Integrity Protection for Container Images**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This pCR proposes to solve TR 33.848 [1] Key Issue #27: Secrets in NF container images***

# 2 References

[1] 3GPP TR 33.848 v0.10.0 "Study on Security Impacts of Virtualisation"

# 3 Rationale

Secrets stored on NF container images (e.g., hardcoding passwords, keys) presents a risk in the supply chain where adversaries can steal or modify secrets. However, at times it is advantageous or necessary to include secrets in the container image packages. In these cases, proper security procedure should be followed to provide reasonable confidentiality and integrity of container image packages. To this end, this solution aggregates mitigation techniques including cryptography, HMEEs, NFV attestation, and VNF host-sealing on VNF packages. This solution provides protection mechanisms from VNF package creation to VNF instantiation. This solution is intended to be part of a defense in depth strategy for packaging and delivering VNF packages that may have container images with secrets.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security"

[5] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement"

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[7] "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable"; Shahzad and Litchfield 2015; <https://arxiv.org/ftp/arxiv/papers/1606/1606.01356.pdf>

[8] "OpenStack"; <https://www.openstack.org/>

[9] ETSI GR NFV-SEC 016: "Network Functions Virtualisation (NFV); Security; Report on location, timestamping of VNFs".

[10] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[11] ETSI GR NFV-SEC 011: " Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[12] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[13] 3GPP TS 23.502: "System architecture for the 5G System (5GS)".

[14] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[15] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[16] 3GPP TS 28.533 "Management and orchestration; Architecture framework".

[17] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[18] IETF RFC 4210: "The Kerberos Network Authentication Service (V5)".

[19] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[20] IETF: RATS Working Group: Remote Attestation Procedures Architecture, <https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.txt>

[A] S. Lal, S. Ravidas, I. Oliver and T. Taleb, "Assuring virtual network function image integrity and host sealing in Telco cloud," *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1-6, doi: 10.1109/ICC.2017.7997299.

[B] ETSI GS NFV-SOL 004: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; VNF Package and PNFD Archive specification".

[C] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification"

[D] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; VNF Descriptor and Packaging Specification".

[E] IETF RFC 5652 (September 2009): "Cryptographic Message Syntax (CMS)".

[F] IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".

[G] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.X Solution #Y: Confidentiality, and Integrity Protection for Container Images

6.X.1 Introduction

This solution addresses Key Issue 27: Secrets in NF container images. Secrets stored on NF container images (e.g., hardcoding passwords, keys) . However, at times it is advantageous or necessary to include secrets in the container image packages. In these cases, proper security procedure should be followed to provide reasonable confidentiality and integrity of container image packages. To this end, this solution aggregates mitigation techniques including cryptography, HMEEs, NFV attestation, and VNF host-sealing on VNF packages. This solution provides protection mechanisms from VNF package creation to VNF instantiation.

Confidentiality of container images can be achieved by encrypting packages while in storage, in-transit, and in-use. Encrypting container image packages reduces the risk of leaking secrets in the VNF image.

Integrity of container images means the VNF image was not tampered with, and the source is as expected. This can be achieved by hashing and signing the container image then verifying the signature and hash when ready for VNF instantiation.

This solution begins with the security procedures for encrypting and signing VNF container packages – a minimum requirement to protect NF stored secrets. This solution goes on to describe additional hardening techniques to secure the VNF container package such as VNF host sealing [A], Hardware Mediated Execution Environments (HMEE), Trusted Platform Modules (TPM), and NFV attestation. The result of the solution is a defense in depth strategy for packaging and delivering VNF packages that may contain secrets.

6.X.2 Solution details

As a baseline, this solution uses encryption and digital signatures to reduce the risk of disclosing secrets packaged in/with VNF container images, as described in clause 6.X.2.1.

Clauses 6.X.2.2-6.X.2.4 describe hardening techniques that further reduce the possibility of NF secrets exposure and VNF images corruption.

Clause 6.X.2.5 demonstrates an example VNF deployment scenario where the NFVI host (CSP), VNF provider, and service provider are all separate entities.

#### 6.X.2.1 Container Package Confidentiality and Integrity using Encryption and Digital Signatures

The VNF package is an archive file that contains the necessary files for a service provider to deploy a VNF, such as the VNF container image, configuration scripts, VNF testing files, manifest file, etc. (more details on the VNF package can be found in ETSI GS NFV-SOL 004 [B]). The VNF provider is responsible for securing the VNF package before sending it to the service provider.

The procedures and requirements for protecting the confidentiality, authenticity, and integrity of VNF packages are described in ETSI GS NFV-SEC 021 [C], ETSI GS NFV-SOL 004 [B], and ETSI GS NFV-IFA 011 [D], and summarized below:

1. The VNF provider and the service provider share secrets (e.g., keys, certificates), primarily to establish a secure communication channel. If using Public Key Infrastructure, then this step can be used to distribute public keys and certificates (e.g., X.509 certificate). A standard format for encryption and digital signatures is used, namely CMS [E] or PKCS#7 [F], and their text representation format IETF RFC 7468 [G].
2. The VNF provider encrypts and signs the VNF package and sends it to service provider. Contents in the VNF package are protected using public key cryptography. For example, the VNF provider encrypts the VNF package with the public key of the service provider and is decrypted by the service provider with their private key. Every file within the VNF package is integrity protected using the VNF provider signature. Manifest files are used to store the expected digest for each file within the VNF package.
3. The service provider verifies the VNF package signature and that its contents are as expected. Every file in the VNF package is verified with their expected digests. This step provides the service provider integrity of the VNF package. Functionality of the VNF package contents (e.g., container image) is also tested at this point. The VNF provider should provide necessary testing files in the VNF package.

Note: Clause 6.8 describes how Attribute Based Access Control can be used to restrict administrative access to NFV resources. Additionally, annex A describes some security principles for administration of the NFVI.

1. The service provider encrypts and signs the VNF package before storing it in the NFV-MANO catalogue(s). Keys used in this step are different from the keys provided by the VNF provider.
2. During instantiation of the VNF, the package is retrieved from the NFV-MANO catalogue(s), then decrypted and the signature is verified.
3. Individual contents from the VNF package are verified by comparing an expected digest to the actual calculated digest. Expected digests are calculated by the VNF provider and placed in a signed file (i.e., manifest file), in step 2.

#### 6.X.2.2 VNF host sealing

In [A], VNF host sealing is defined as *the process which uses trusted platform module (TPM) to bind some VNF instance to a specific compute host which satisfies the given set of system configuration policies.* Policies are tied to the VNF image metadata and include host system requirements such as OS, container engine, and location. Policies should meet the security requirements outlined by the service provider (e.g., in [A], to attest that the VNF is deployed on a qualified host machine, the authors use the TPM system measurements, PCRs, [host OS: Ubuntu; Linux Kernel version: 3.19.0-39; hypervisor: KVM]).

Binding the VNF to a specific host machine or set of machines can help assure that the VNF is deployed in the legal jurisdiction of the service provider. This is especially important when the service provider contracts a Cloud Service Provider (CSP) for NFVI. For example, VNF package metadata can include the allowed location, and based on this the set of allowed hosts is confined/ sealed to that location.

#### 6.X.2.3 HMEE

Hardware Mediated Execution Environments (HMEE), described in clause 6.5, provide a trusted execution space that provides confidentiality and integrity of data-in-use. Sometimes container images do not initially contain secrets and acquire them after VNF deployment (e.g., user accounts, user data), it is important to protect secrets while in use. Using an HMEE for sensitive workloads can protect the VNF secrets from malicious cloud administrators or unauthorized access.

Additionally, the HMEE can be used to provide a root of trust in the NFVI and ultimately take part in the chain of trust in NFVI attestation.

#### 6.X.2.4 NFV attestation

NFVI attestation, as in clause 6.6.3.1, is the process used to verify the physical devices used to support the VNFs. VNF packages should be given to the NFVI host after successful NFVI attestation. Container images that rest in the service provider or CSP image repository should remain confidential in secure storage until ready for deployment. After successful NFVI attestation, NFV MANO should initiate VNF attestation, as in clause 6.6.3.2.

#### 6.X.2.5 An example VNF deployment scenario

An example VNF deployment scenario using the described techniques in clause 6.X.2.1-6.X.2.4 is shown in Figure 6.X.2.5-1.



**Figure 6.X.2.5-1: An example flow of a VNF package from the VNF provider to deployment in an NFVI hosted by the CSP; dashed line: non-MANO domain; solid line: MANO domain**

1. In the initial step, a secure communication channel between the Service provider and the Cloud Service Provider (CSP) is established. Next, the service provider gathers information specific to the CSP compute that will be used to seal the VNF package to that specific host machine(s). In addition, NFVI details pertinent to the development and support of the VNF container image (e.g., Container engine, OS) are given to the service provider.

Security related material used to establish a secure communication channel in later steps is also exchanged in this step. For example, a connection between the remote attestation server and the TPM trusted client.

1. The service provider and VNF provider share any security related material necessary for protection of data while in-transit and mutual authentication. Service provider shares with VNF provider any NFVI details received from the CSP required for VNF development.
2. The VNF package is created and configured for the service provider and the host platform. Each file within the VNF package is integrity protected using the VNF provider signature. The expected digest of each file is included in the manifest file within the VNF package. If using Public Key cryptography, the VNF package is encrypted with the service provider’s public key.

Note: The VNF provider should not include default service provider accounts or service provider secrets in container images.

1. The VNF provider sends the VNF package to the service provider. Any 3rd party vendors involved in the supply chain do not have access to the encrypted package and cannot modify the contents without knowing the VNF provider signature.
2. The service provider opens the VNF package and verifies the signature on the contents is correct, meanwhile discarding any unmatched signatures or unsigned contents. Next, service provider performs validation testing on the contents, using test files included in the VNF package. Finally, the service provider encrypts the contents and stores them in the NFV-MANO catalogue(s). Keys used to protect the VNF contents in the NFV MANO domain are different than the VNF provider keys and should be known only to the service provider administrators.
3. A verifier, remote attestation server, external to CSP and within the NFV MANO performs remote attestation of the CSP NFVI to verify its integrity. A trusted client on the CSP receives TPM measurements used to prove the integrity of the machine, these measurements are sent to the verifier. If NFVI attestation is unsuccessful, then steps 7-9 are not performed.
4. If NFVI attestation is successful and the service provider wishes to deploy/ instantiate a VNF, it retrieves the VNF package contents from it’s NFV-MANO catalogue and verifies that the contents have not been modified or tampered. Then, the service provider performs VNF host-sealing by appending specific host info to the VNF package metadata. Then, the service provider encrypts the VNF package with the CSP’s public key. Using a secure channel, the service provider sends the VNF package to CSP.

Alternatively, the remote attestation server can serve as a trusted key broker whereby the keys used to open a VNF package are provided to the CSP/NFVI after successful NFVI attestation and VNF host-sealing.

1. The results from NFVI attestation are used to verify that the host used to seal the VNF package in step 7 is as expected. If the host compute is not as expected, then the VNF should not be deployed until the correct host is discovered. The contents of the VNF package should remain in secure storage until ready for use.
2. Using the container image received from the service provider, CSP can instantiate the VNF on the NFVI. VNF attestation can be initiated by NFV-MANO at this stage.

6.X.3 Evaluation

Editor’s Note: Further analysis and evaluation is FFS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*