**3GPP TSG-SA3 Meeting #99e S3-201133**

**e-meeting, 11 -15 May 2020 Revision of S3-20xxxx**

**Source: China Mobile, Huawei, Hisillicon**

**Title: Adding test case into clause 5.2.5.5.3.3.5**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

It is proposed to add threat reference test case into clause 5.2.5.5.3.3.5.

# 2 Rationale

This contribution describes the threat reference and the test case for VNF package and VNF image integrity.

# 3 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.5.5 Security functional requirements and related test cases for GVNP of type 1

5.2.5.5.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases, independent of a specific virtualised network product class of type 1. According to security threats and security requirements in the above clauses, there are threats relating to ETSI-defined interfaces and Security functional requirements related to virtualization layer, hardware and resource isolation etc. (ref. clause 5.2.4.2.2 and clause 5.2.5.2). So, the proposed security requirements for GVNP of type 1 are classified in three groups:

- Security functional requirements deriving from 3GPP specifications and detailed in clause 5.2.5.5.2

- General security functional requirements which include requirements not already addressed in the 3GPP specifications but whose support is also important to ensure a network product conforms to a common security baseline detailed in clause 5.2.5.5.3, clause 5.2.5.5.4, clause 5.2.5.5.5 and clause 5.2.5.5.6.

* Security functional requirements related to virtualization layer, hardware and resource isolation, among others. These requirements can be called security functional requirements deriving virtualisation for simplify and detailed in clause 5.2.5.5.7.

The threat comparation between GVNP of type 1 and physical network products are summarized in clause 5.2.4.3.2.10. Except threats relating to ETSI-definer interfaces, other threat categories can apply to threat categories for GVNP of type 1. So, the security requirements of the above first and second group will base on the security requirements in clause 4.2 of TS 33.117 [4] to identify the different security requirements for GVNP of type 1.

Editor’s note: whether the security functional requirements and related test cases of 3GPP virtualized network product classes are to be contained in TS 33.117 [4] or not is FFS.

5.2.5.5.2 Security functional requirements deriving from 3GPP specifications and related test cases

5.2.5.5.2.1 Security functional requirements deriving from 3GPP specifications – general approach

The clause 4.2.2.1 in TS 33.117 [4] describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class. The general approach is generic and applies to security functional requirements deriving from 3GPP specifications and the corresponding test cases of GVNP type 1.

5.2.5.5.3 Technical baseline for general security functional requirements

5.2.5.5.3.1 Introduction

The technical baseline is a generic set of security requirements to be fulfilled by all virtualized network products.

In particular these requirements counter the security threats identified in clause 5.2.4.2.2 and they basically aim to guarantee the network product confidentiality, integrity and availability.

5.2.5.5.3.2 Protecting data and information

All text from TS 33.117 [4], clause 4.2.3.2 applies to GVNP of type 1.

5.2.5.5.3.3 Protecting availability and integrity

5.2.5.5.3.3.1 System handling during overload situations

All text from TS 33.117 [4], clause 4.2.3.3.1 applies to GVNP of type 1.

5.2.5.5.3.3.2 Boot from intended memory devices only

All text from TS 33.117[4], clause 4.2.3.3.2 applies to GVNP of type 1.

5.2.5.5.3.3.3 System handling during excessive overload situations

All text from TS 33.117 [4], clause 4.2.3.3.3 applies to GVNP of type 1.

5.2.5.5.3.3.4 System robustness against unexpected input

All text from TS 33.117 [4], clause 4.2.3.3.4 applies to GVNP of type 1.

5.2.5.5.3.3.5 Virtualized Network product software package integrity

All text from TS 33.117 [4], clause 4.2.3.3.5 applies to GVNP of type 1.

In addition, VNF package and VNF image integrity shall be validated when on board, and VNF image integrity shall be validated when in instantiated. The detailed security requirements and related test cases are as following.

5.2.5.5.3.3.5.1 VNF package and VNF image integrity

*Requirement Name*: VNF package and VNF image integrity

*Requirement Description*:

1) VNF package and image shall contain integrity validation value (e.g. MAC).

2) VNF package shall be integrity protected prior to on board. NFVO shall validate the VNF package integrity.

*Threat Reference*: TR 33.926 [3], Clause5.3.4.1, "Software Tampering "; TR 33.848, Clause5.18, “Key Issue 17: Software Catalogue Image Exposure”

*Test case*:

**Test Name:** TC\_VNF PACKAGE AND IMAGE­\_ INTEGRITY

**Purpose:**

1. To test whether the VNF package has been integrity protected or not.

2. To test whether the VNF image has been integrity protected or not.

**Procedure and execution steps:**

**Pre-Condition:**

- The virtualized network product document describes information regarding integrity protection of VNF package and VNF images, including details of how the integrity check is carried out, who makes the digital signatures of VNF package, what evidence is created to prove that the integrity check has been executed and what the result of the check is etc.

- A valid VNF package and a not-valid VNF package (e.g. a tampered image in VNF package) are available.

- A valid VNF image (i.e. a correct HASH value is attached) and a not-valid VNF image (i.e. an incorrect HASH value is attached, e.g. the VNF image can be tampered when the VNF image is sent from the NFVO to the VIM or when the VNF image is stored in the iamge repository) are available in the image repository of VIM.

- There are NFVO and VIM, or simulated NFVO and VIM.

**Execution Steps**

**Execute the following steps:**

1. Review the documentation provided by the vendor describing how VNF package integrity is verified;

2. During VNF package onboarding, the tester uploads a valid VNF package into a NFVO. The NFVO verifies the integrity of the VNF packge by validating the digital signature of the VNF package using the certificate of VNF vendor according to the documentation;

3. DuringVNF package onboarding, the tester uploads a not-valid VNF package into a NFVO. The NFVO validates the digital signature of the VNF package using the certificate of VNF vendor;

4. During VNF instantiation, the VIM selects a VNF image with a correct integrity protection value from the image repository to instantiate the VNF image.

5. During VNF instantiation, the VIM selects a VNF image with an incorrect integrity protection value from the image repository to instantiate the VNF image.

**Expected Results:**

1. The VNF package is successfully onboarded into the NFVO;

2. The not-valid VNF package is not onboarded;

4. The VNF image with a correct integrity protection value is instantiated by the VIM;

5. The VNF image with an incorrect integrity protection value is not instantiated by the VIM.

**Expected format of evidence:**

Snapshots containing the result of the VNF package on boarding and the VNF image instantiation.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*