**3GPP TSG-SA3 Meeting #99e *S3-201135***

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

**Source: China Mobile**

**Title: Adding security functional requirements deriving virtualisation and related test cases for GVNP of type 2**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

It is proposed to add the security functional requirements deriving virtualisation and related test cases for GVNP of type 2 into clause 5.2.5.y.7.

# 2 Rationale

This contribution describes the security functional requirements deriving virtualisation and related test cases for GVNP of type 2 and adds these requirements into clause 5.2.5.y.7.

# 3 Detailed proposal

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

5.2.5.y.7 Security functional requirements deriving from virtualisation and related test cases

All texts in clause 5.2.5.x.7 apply to GVNP of type 2. In addition, GVNP of type 2 has the following security requirements related to virtualisation resource management, executive environment creation and VM escape which are derived from virtualisation and related test cases.

5.2.5.y.7.1 Security functional requirements on virtualisation resource management

*Requirement Name*: secure virtualisation resource management

*Requirement Description*:

1. To prevent a compromised VIM from changing the assigned virtualised resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, the VNF shall alert to the OAM when the VNF cannot detect a VNFC message.

2. A VNF shall log the access from the VIM.

Editor’s note: The VIM manages the virtualisation resource assignment and synchronization of virtualized resource state information. In the implementation, the VIM and the virtualisation layer are coupled and provided by one vendor, they trust each other. The operations should check whether the VIM is trust or not.

*Threat Reference:* TBA

*Test case*:

**Test Name:** TC\_SECURE VIRTUALISATION RESOURCE MANAGEMENT

**Purpose:**

1. To test whether the VNF alerts to the OAM when find the abnormal situation, e.g. a VNFCI is deleted by VIM.

2. VNF shall log the access from the VIM.

**Procedure and execution steps:**

**Pre-Condition:**

There are an OAM and a NFVO (or simulated OAM and NFVO) on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester logs to the VIM and deletes a VM of a VNF;

**Expected Results:**

1. The VNF alerts to the OAM. The alert from the VNF is found in the OAM.

2. The VNF logs the alert.

**Expected format of evidence:**

Screenshop contains the alert in the OAM and the alert in the log of the VNF.

5.2.5.y.7.2 Security functional requirements on executive environment creation

*Requirement Name*: secure executive environment creation

*Requirement Description*:

When an attacker tampers a driver which provided by the hardware and used to create the executive environment, the virtualisation layer shall alert the driver error to the administrator for checking the error and finding the attack at latter.

Editor’s note: The operators should check whether the hardware is trust or not and ensure the virtualisation layer and the VNF to be run on the trusted hardware.

*Test case*:

**Test Name:** TC\_SECURE EXECUTIVE ENVIRONMENT CREATION

**Purpose:**

To test the virtualisation layer alerts the driver error.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer, a VIM (or simulated virtualisaion layer, a VIM) and a host on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester tampers a driver on the server and implements the excutive environment creation.

2. The tester checks whether the virtualisation layer alerts the driver error or not.

**Expected Results:**

 The virtualisation layer alerts the driver error.

**Expected format of evidence:**

Screenshop contains the alert.

5.2.5.y.7.3 Security functional requirements on VM escape

*Requirement Name*: VM escape protection

*Requirement Description*:

To defence the attack that an attacker utilizes a vulnerability of a VNF to attack a virtualisation layer and then control the virtualisation layer, the virtualisation layer shall implement the following requirements:

1. The virtualisation shall reject the abnormal access from the VNF (e.g. the VNFunauthorized accesses the memory which is not allocated to the VNF) and log the attacks.

*Test case*:

**Test Name:** TC\_VM ESCAPE PROTECTION

**Purpose:**

To test the virtualisation layer rejects the abnormal access from the VNF and logs the attacks from the VNF.

**Procedure and execution steps:**

**Pre-Condition:**

There are a virtualisation layer and a VNF on the test environment.

**Execution Steps**

**Execute the following steps:**

1. The tester logs the VNF and makes an abnormalaccess (e.g. the VNFunauthorized accesses the memory which is not allocated to the VNF) to the virtualisation layer.

2. The tester checks whether the virtualisation layer rejects the abnormal access from the VNF and logs the attacks.

**Expected Results:**

 The virtualisation layer rejects the abnormal access from the VNF and logs the attacks.

**Expected format of evidence:**

Screenshop contains the log.

Note: The security requirements and related test cases in clause 5.2.5.y.7.3 only considered in the decoupling scenario.

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