**3GPP TSG-SA3 Meeting #101-e *S3-203129***

**e-meeting, 9 -20 Novenber 2020** Revision of S3-20xxxx

**Source: China Mobile**

**Title: Adding hardening requirements for GVNP of type 1**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution adds hardening requirements for GVNP of type 1 into clause 5.2.5.5.8.***

# 2 References

[X] 3GPP TR 33.117: "Catalogue of general security assurance requirements"

# 3 Rationale

The hardening requirements were proposed in TS 33.117 are general and generally apply to GVNP of type 1. Compared to the physical network products, GVNP of type 1 has not hardware, but contains 3GPP functions, other functions and guest OS, it also has infrastructure management traffic rather than O&M traffic, control plane traffic and data plane traffic etc. It also has the intra traffic between two VFNCs rather than the inter traffic between two VNFs. The hardening requirements for GVNP of type 1 shall consider how to reduce the exposure from these new features.

This contribution proposes hardening requirements and related test cases for GVNP of type 1based on the hardening requirements in TS 33.117. We propose to add these hardening requirements and related test cases into clause 5.2.5.5.8.

# 4 Detailed proposal

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

##### 5.2.5.5.8 Security requirements and related test cases to Hardening for GVNP of type 1

###### 5.2.5.5.8.1 Introduction

The requirements proposed in the present clause aim to securing virtualized network products (including the network functions in service-based architecture) by reducing its surface of vulnerability. In particular the identified requirements aim to ensure that all the default virtualized network product configurations (including operating system software, firmware and applications) are appropriately set. The hardening requirements were proposed in TS 33.117 are general and generally apply to GVNP of type 1. So, the hardening requirements for GVNP of type 1 also include four aspects, i.e. general hardening requirements (i.e. technical baseline), operating system, web server, network devices.

Compared to the physical network products, GVNP of type 1 has not hardware, but contains 3GPP functions, other functions and guest OS, it also has inter-VNF traffic and intra-VNF trafficin addition to than O&M traffic, control plane traffic and data plane traffic etc. The following clauses describe how to reduce the exposure from these new features.

###### 5.2.5.5.8.2 Technical Baseline

5.2.5.5.8.2.1 No unnecessary or insecure services / protocols

All text from TS 33.117 [4], clause 4.3.2.1 applies to GVNP of type 1.

5.2.5.5.8.2.2 Restricted reachability of services

All text from TS 33.117 [4], clause 4.3.2.2 applies to GVNP of type 1.

5.2.5.5.8.2.3 No unused software

All text from TS 33.117 [4], clause 4.3.2.3 applies to GVNP of type 1.

5.2.5.5.8.2.4 No unused functions

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.4 applies to GVNP of type 1, except the requirements and testing on hardware functions.

5.2.5.5.8.2.5 No unsupported components

As GVNP of type 1 does not contain the hardware layer, all text from TS 33.117 [4] clause 4.3.2.5 applies to GVNP of type 1, except the requirements and testing on hardware components.

5.2.5.5.8.2.6 Remote login restrictions for privileged users

All text from TS 33.117 [4], clause 4.3.2.6 applies to GVNP of type 1.

5.2.5.5.8.2.7 Filesystem Authorization privileges

All text from TS 33.117 [4], clause 4.3.2.7 applies to GVNP of type 1.

###### 5.2.5.5.8.3 Operating System

Guest OS provided by the vendors is generally based on Linux. All hardening requirements of OS in clause 4.3.3 of TS 33.117 [4] are general requirements and apply to GVNP of type 1.

###### Editor’s Note: Hardening requirements for Guest OS not based on Linux are FFS.5.2.5.5.8.4 Web Severs

All hardening requirements of Web Servers in clause 4.3.4 of TS 33.117 [4] are general requirements and the same for both the virtualised network product and the physical network product. So, all text from TS 33.117 [4], clause 4.3.4 applies to GVNP of type 1.

###### 5.2.5.5.8.5 Virtualised Network Products

5.2.5.5.8.5.1 Traffic separation

All text from TS 33.117 [4], clause 4.3.5.1 applies to GVNP of type 1, except for the supporting physical separation of traffic belonging to different network domains. The detailed requirement and test case are as fillowing.

*Requirement Name*: Traffic Separation

*Requirement Description*:

The virtualized network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 [x] for further information.

*Threat reference*: 5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation.

*Test case*:

**Test Name:** TC\_TRAFFIC\_SEPARATION

**Purpose:**

To test whether traffic belonging to different network domains is separated.

**Procedure and execution steps:**

**Pre-Condition:**

NOTE: This test applies if the virtualized network product is meant to handle traffic from different network domains, e.g. both O&M and control plane traffic.

The virtualized network product has at least two separate logical interfaces dedicated to different network domains. Virtualized network products for which the test applies and that fail to meet this precondition fail the test by definition.

**Execution Steps**

**Execute the following steps:**

1. The tester checks whether the virtualized network product refuses traffic intended for one network domain on all interfaces meant for the other network domain, and vice versa.

2. Step 1 is to be performed for all pairs of different network domains.

**Expected Results:**

The two tests should be successful.

**Expected format of evidence:**

A PASS or FAIL.

5.2.5.5.8.5.2 Separation of inter-VNF and intra-VNF traffic

*Requirement Name*: inter-VNF and intra-VNF Traffic Separation

*Requirement Description*:

The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated.

Editor’s Note: Threat analysis for this requirement and corresponding the test cases is to be added. A figure illustrating the scenario needs to be added.

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