**3GPP TSG-SA3 Meeting #102-e *S3-210306r1***

**e-meeting, 18 -29 January 2021** Revision of S3-210306

**Source: China Mobile**

**Title: Clarifying generic assets and threats for GVNP of type 1**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This contribution clarifies generic assets and threats for GVNP of type 1.***

# 2 Rationale

The description of interface in clause 5.2.3.2.4 has been updated, the difference and interacction between ETSI-defined interfaces and 3GPP defined interfaces has been described in the contribution 2. S3-xxxx, this contribution proposes to delete the related editor’s note.

This contribution proposes to reformulate the threats relating to ETSI-defined interfaces, denial of Service in clause 5.2.4.2.2.3 and 5.2.4.2.2.8 respectively. The related ENs are also proposed to delete.

# 3 Detailed proposal

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

#### 5.2.4.2 Generic assets and threats of GVNP for type 1

##### 5.2.4.2.1 Generic assets of GVNP for type 1

The critical assets of GVNP for type 1 that need to be protected are:

- User account data and credentials (e.g. passwords, private key);

- Log data;

- Configuration data, e.g. GVNP's IP address, ports, VPN ID, Management Objects (e.g. user group, command group) etc.

- Guest Operating System, i.e. the files that make up the guest OS and its processes (code and data);

- GVNP Application;

- Sufficient processing capacity: that processing powers are not consumed close to limits;

- The interfaces of GVNP to be protected and which are within SECAM scope: for example:

- OAM interface, for remote access: interface between GVNP and OAM system

- Interface between virtualised network function (VNF) and VNFM

- Interface between VNF and virtualisation layer, for providing the execution environment to run VNF

- GVNP Software package (binary code or executable code) which includes

- VNFD;

- VNF image and image description file;

- Configuration data (e.g. manifest file as defined in [15])

##### 5.2.4.2.2 Generic threats for GVNP of type 1

###### 5.2.4.2.2.1 Introduction

In clause 5.3.1 of TR 33.926 [3], the identified threats are grouped into seven categories, one covering threats relating to 3GPP-defined interfaces and the other six corresponding to the categories proposed by STRIDE. Since these seven categories are for generic 3GPP network products, they are also applicable to GVNP of type 1. In addition, GVNP of type 1 also needs to consider the threats related to ETSI-defined interfaces. As a result, there are eight categories of threats for GVPN of type 1. The following clauses describe the threats according to these security categories and use the template of threat description in clause 5.3.1 of TR 33.926 [3]. For threats descriptions of current seven categories, the present document will focus on the differences between GVNP threats and GNP threats which are described in TR 33.926 [3].

###### 5.2.4.2.2.2 Threats relating to 3GPP-defined interfaces

For GVNP of type1 and GNP in TR 33.926 [3], the threats related to 3GPP-defined interfaces are the same. So, all texts in clause 5.3.2 of TR 33.926 [3] apply to GVNP of type 1. It means that there is no need repeat the threats relating to 3GPP-defined interfaces which are covered in 3GPP security specifications. If threats relating to 3GPP-defined interfaces are found not sufficiently covered in existing 3GPP security specifications, they need to be addressed in the SCAS for virtualised network products.

###### 5.2.4.2.2.3 Threats relating to ETSI-defined interfaces

Two of the interfaces defined in ETSI NFV specification [11] are identified as the critical assets of GVNP type 1, i.e. interface between VNF and VNFM, interface between 3GPP VNF and virtualisation layer. The threats on these interfaces are as follows.

- Threats on interface between 3GPP VNF and VNFM: if the interface is not protected, an attacker can attack all the requests/responses sent between the VNF and the VNFM. For example, the attacker can insert, tamper or delete e.g. scaling requests, healing requests, subscribe requests, query requests and other management related requests sent from the instantiated GVNP of type 1 to the VNFM, hence the virtualised resource or relevant status information obtained by the instantiated GVNP of type 1 is not as requested. This affects the normal operation of the instantiated GVNP of type 1, and even causes DoS attacks, information leakage.

NOTE: The Virtualisation layer is out of 3GPP scope, but its protection will affect the security of the upper layer it supports. If the Virtualisation layer is compromised, the VNF on top of it could also be easily compromised. In such case, the messages sent over the VNF-VNFM interface can be manipulated by the compromised VNF, which is however not a threat coming from the VNF-VNFM interface. The analysis above focuses on the threats directly placed on VNF-VNFM interface, when it is not well protected.

- Threats on interface between 3GPP VNF and virtualisation layer: an attacker can attack an instantiated GVNP of type 1 through a compromised virtualisation layer. For example, cryptographic keys or other security critical data of an instantiated GVNP of type 1 could be stolen by an attacker with access to the virtualisation layer, or the virtualised resource provided by the Virtualisation layer to the instantiated GVNP of type 1 can be manipulated or the bootloader of Guest OS of an instantiated GVNP of type 1 can be tampered by an attacker via a compromised virtualisation layer.

Editor's note: More threats described in TR 33.848[9] or/and ETSI specification etc. are to be added if identified as related to the above two interfaces.

###### 5.2.4.2.2.4 Spoofing identity

5.2.4.2.2.4.1 Default Accounts

The threat in clause 5.3.3.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. The difference is that VNF is accessed through VNC (Virtual Network Console) rather than through the physical console interface, an attacker can use a default account to access a VNF via VNC.

5.2.4.2.2.4.2 Weak Password Policies

The threat in clause 5.3.3.2 of TR 33.926 [3] is generic, so it also applies to GVNP. However, the attacker using the weak password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.2.4.2.2.4.3 Password peek

The threat in clause 5.3.3.3 of TR 33.926 [3] is generic, so it also applies to GVNP. However, the attacker using the peeked password accesses GVNP through VNC (Virtual Network Console) rather than through the physical console interface.

5.2.4.2.2.4.4 Direct Root Access

The threat in clause 5.3.3.4 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. There are no differences between direct root accesses for GVNP and GNP described in TR 33.926 [3].

5.2.4.2.2.4.5 IP Spoofing

The threat in clause 5.3.3.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. However, the objective of unauthorized access is a VNF, not a computer.

5.2.4.2.2.4.6 Malware

The threat in clause 5.3.3.6 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.4.7 Eavesdropping

The threat in clause 5.3.3.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

###### 5.2.4.2.2.5 Tampering

5.2.4.2.2.5.1 Software Tampering

The threat in clause 5.3.4.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1. Different from traditional physical network products, as the entire GVNP is instantiated by the image(s) and other information (e.g. configuration data, software environmental parameters, licence terms information, script, manifest file, checksum, etc. as defined in [15]) within a software package, additional threats are analysed as follows:

*- Threat Name*: Software Tampering

*- Threat Category*: Tampering

- *Threat Description*: Compared with GNP software, GVNP software has additional attack surfaces, e.g. in the process of VNF package onboarding, during which the software package of a GVNP can be tampered/altered if not protected. An attacker, for example, can inject malicious code or tamper the information inside the unprotected package during onboarding. Then after the instantiation of the GVNP, the tampered code can be executed to conduct several attacks (e.g. DoS, Information Stealing, Frauds and so on).

*- Threatened Asset*: all critical assets of GVNP type 1 as listed in clause 5.2.4.2.1.

Editor's Note: Whether the additional threat can impact all critical assets of GVNP type 1 listed in clause 5.2.4.2.1is FFS

5.2.4.2.2.5.2 Ownership File Misuse

The threat in clause 5.3.4.2 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

Editor's Note: More analysis on whether the threat in clause 5.3.4.2 of TR 33.926 [3] or more threats can apply to GVNP of type 1 is FFS

5.2.4.2.2.5.3 Boot tampering for GVNP of type 1

For GVNP of type 1, there is no hardware. This is different from external device boot of GNP described in clause 5.3.4.3 of TR 33.926 [3]. The threat is described as follows:

*- Threat name*: GVNP of type 1 boot tampering

*- Threat Category*: Tampering

*- Threat Description:* the GVNP bootloader may be maliciously tampered by an attacker, e.g. the attacker tampers the bootloader of GVNP through a malicious virtualisation layer.

*- Threatened Asset:* guest operating system

5.2.4.2.2.5.4 Log Tampering

The threat in clause 5.3.4.4 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.5 OAM traffic Tampering

The threat in clause 5.3.4.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.6 File Write Permissions Abuse

The threat in clause 5.3.4.6 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.5.7 User Session Tampering

The threat in clause 5.3.4.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

###### 5.2.4.2.2.6 Repudiation

5.2.4.2.2.6.1 Lack of User Activity Trace

The threat in clause 5.3.5.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

###### 5.2.4.2.2.7 Information disclosure

5.2.4.2.2.7.1 Poor key generation

The threat in clause 5.3.6.1 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.2 Poor key management

The threat in clause 5.3.6.2 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.3 Weak cryptographic algorithms

The threat in clause 5.3.6.3 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.4 Insecure Data Storage

*- Threat name*: Insecure Data Storage

*- Threat Category*: Information Disclosure

*- Threat Description:* The GVNP remotely stores sensitive data (e.g. passwords, private keys, logs) on the logical volume that the VIM allocates to the GVNP. An attacker can retrieve these data if they have been stored in an insecure way (e.g. clear text, unsalted hashes).

*- Threatened Asset*: Any sensitive data stored on the logical volume of the GVNP

5.2.4.2.2.7.5 System Fingerprinting

The threat in clause 5.3.6.5 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.6 Malware

- Threat name: Malware

- Threat Category: Information Disclosure

- Threat Description: A malware installed on the logical volume that the VIM allocates to the GVNP can access to the stored sensitive data (e.g. subscription data, logs).

- Threatened Asset: Any sensitive data stored on the logical volume of the GVNP

5.2.4.2.2.7.7 Personal Identification Information Violation

The threat in clause 5.3.6.7 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.8 Insecure Default Configuration

The threat in clause 5.3.6.8 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.9 File/Directory Read Permissions Misuse

The threat in clause 5.3.6.9 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.10 Insecure Network Services

The threat in clause 5.3.6.10 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.11 Unnecessary Services

The threat in clause 5.3.6.11 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.12 Log Disclosure

The threat in clause 5.3.6.12 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.13 Unnecessary Applications

The threat in clause 5.3.6.13 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.14 Eavesdropping

The threat in clause 5.3.6.14 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

5.2.4.2.2.7.15 Security threat caused by lack of GVNP traffic isolation

The threat in clause 5.3.6.15 of TR 33.926 [3] is generic, so it also applies to GVNP of type 1.

###### 5.2.4.2.2.8 Denial of Service

The threats in all clauses of clause 5.3.7 for TR 33.926 [3] are generic, so they also apply to GVNP of type 1. In addition, there is DoS attack due to changing virtualisation resource that is used by GVNP. The detailed threat description is as follows:

*- Threat name*: changing virtualisation resource without authorization

*- Threat Category*: DoS

*- Threat Description*: There are several ways to cause a DoS attack for the GVNP: attackers having access to a compromised virtualisation layer can change the virtualisation resource used by the instantiated GVNP of type1 without authorization, or a malicious VM deployed for one instance of a VNF on a host can illegally occupy the resources of the instantiated GVNP of type1 deployed on the same host, resulting in resource limitation of the instantiated GVNP of type1, or attackers having access to a compromised VNFM can scale in a Type 1 or scale down the virtualisation resource used by a GVNP or even terminate a Type 1 instance without authorization.

*- Threatened Asset*: GVNP applications, sufficient processing capacity

###### 5.2.4.2.2.9 Elevation of privilege

The threats in all clauses of clause 5.3.8 for TR 33.926 [3] are generic, so they also apply to GVNP of type 1.

###### 5.2.4.2.2.10 Summary of threats for GVNP of type 1

The threats for GVNP of type 1 can be compared to TR 33.926 [3] and summarized as following:

|  |  |  |
| --- | --- | --- |
| Threat Category | Detailed threat | Comparison to TR33.926 [3] |
| Threats relating to 3GPP-defined interfaces | - | All threats can be applied. |
| Threats relating to ETSI-defined interfaces | - | New threats:  - The threats on interface between 3GPP VNF and VNFM  - The threats on interface between 3GPP VNF and virtualisation layer |
| Spoofing identity | Default Accounts | Threats can be applied with difference that access through VNC instead of physical console interface. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | Threats can be applied with difference that objective is VNF instead of computer. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.2.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tampering for GVNP of type 1 | Different threats. See detail in clause 5.2.4.2.2.5.3. |
|  | Log Tampering | Threats can be applied. |
|  | OAM traffic Tampering | Threats can be applied. |
|  | File Write Permissions Abuse | Threats can be applied. |
|  | User Session Tampering | Threats can be applied. |
| Repudiation | Lack of User Activity Trace | Threats can be applied. |
| Information disclosure | - | Different threats. See detail in clauses 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.2.2.8. |
| Elevation of privilege | - | All threats can be applied. |

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