**3GPP TSG-SA3 Meeting #100bis-e *S3-20xxxx***

**e-meeting, 12 - 16 October 2020** Revision of S3-202546 + S3-202559

**Source: Nokia, Nokia Shanghai Bell, China Mobile**

**Title: SCAS VNP: Software Tampering and Information disclosure**

**Document for: Approval**

**Agenda Item: 2.2**

# 1 Decision/action requested

***SA3 is kindly asked to approve the proposed changes in TR 33.818 v0.7.0.***

# 2 References

[1] 3GPP TR 33.818 v0.7.0 Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS); for 3GPP virtualized network products

# 3 Rationale

In current TR 33.818 v0.7.0 [1], the threat analysis for software tamper was misplaced. This pCR proposes to move the text to the current sub-clause. Subsequently, the threat summary of each of the GVNP types and the threat reference in the corresponding test case addressing the threat were corrected accordingly. Some different threats about information disclosure were proposed. So, the security threat comparisons to the TR 33.926 shall also be updated. This contribution also proposes to change the security threat comparisons to the TR 33.926 of all types for GVNPs.

Additionally, description of the same threats in the summaries for Type 2 and Type 3 are simplified to avoid duplicated statements.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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 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.

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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 clause 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. |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.3.2.5 Tampering

5.2.4.3.2.5.1 Software Tampering

The threat in clause 5.2.4.2.2.5.1 of the present document for GVNP of type 1 also applies to GVNP of type 2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.3.2.7 Information disclosure

The threat in all sub-clauses of clause 5.2.4.2.2.7 also applies to GVNP of type 2.

5.2.4.3.2.8 Denial of Service

The threat in all sub-clauses of clause 5.3.7 for TR 33.926[3] also applies to GVNP of type 2.

In addition, all text from clause 5.2.4.2.2.8 also applies to GVNP of type 2 in decoupling scenario.

Editor’s Note: Additional threats are FFS.

5.2.4.3.2.9 Elevation of privilege

The threat in all sub-clauses of clause 5.3.8 for TR 33.926[3] also applies to GVNP of type 2.

5.2.4.3.2.10 Summary of threats for GVNP of type 2

The threats for GVNP of type 2 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 | - | All threats relating to ETSI-defined interfaces of Type 1 apply here. Additional new threats:- The threats on interface between virtualisation layer and hardware- The threats on interface between virtualisation layer and VIM |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 1 apply here. |
|  | 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 and virtualisation layer rather than computer. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.3.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tampering for GVNP of type 2 | Different threats. See detail in clause 5.2.4.3.2.5.3. |
|  | 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 clause 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.3.2.8. |
| Elevation of privilege | - | All threats can be applied. |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 5th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.4.2.5 Tampering

5.2.4.4.2.5.1 Software Tampering

The threat in clause 5.2.4.2.2.5.1 of the present document for GVNP of type 1 also applies to GVNP of type 3.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 6th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2.4.4.2.7 Information disclosure

The threat in all sub-clauses of clause 5.2.4.2.2.7 also applies to GVNP of type 3.

5.2.4.4.2.8 Denial of Service

All texts from clause 5.2.4.3.2.8 also apply to GVNP of type 3.

Editor’s Note: Additional threats are FFS.

5.2.4.4.2.9 Elevation of privilege

The threat in all sub-clauses of clause 5.3.8 in TR 33.926[3] also applies to GVNP of type 3.

5.2.4.4.2.10 Summary of threats for GVNP of type 3

The threats for GVNP of type 3 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 | - | All threats relating to ETSI-defined interfaces of Type 2 apply here. Additional new threat:- The threats on interface between hardware and Virtualised Infrastructure Manager (VIM) |
| Spoofing identity | Default Accounts | The threats relating to Default Accounts of Type 1 apply here. |
|  | Weak Password Policies | Same as above. |
|  | Password peek | Same as above. |
|  | Direct Root Access | Threats can be applied. |
|  | IP Spoofing | The threats relating IP Spoofing of Type 2 appy here. |
|  | Malware | Threats can be applied. |
|  | Eavesdropping | Threats can be applied. |
| Tampering | Software Tampering | Different threats. See detail in clause 5.2.4.4.2.5.1. |
|  | Ownership File Misuse | Threats can be applied. |
|  | Boot tempering for GVNP of type 3 | Different threats. See detail in clause 5.2.4.4.2.5.3. |
|  | 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 clause 5.2.4.2.2.7.4 and 5.2.4.2.2.7.6. |
| Denial of Service | - | Different threats. See detail in clause 5.2.4.4.2.8. |
| Elevation of privilege | - | All threats can be applied. |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 7th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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 during onboarding and its integrity shall be validated by the NFVO.

*Threat Reference*: Clause 5.2.4.2.2.5.2 of the present document, "Software Tampering "; TR 33.848, Clause 5.18, “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 image 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 package by validating the digital signature of the VNF package using the certificate of VNF vendor according to the documentation;

3. During VNF 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;

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

4. 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 Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*