ETSI GS NFV-SEC 012 V3.1.1 (2017-01)

Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/NFV-SEC012

Keywords

architecture, NFV, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines requirements for host system elements on which sensitive workloads are to be run. The present document defines requirements to ensure isolation of sensitive workloads from non-sensitive workloads sharing a platform. The present document discusses a wide range of different technologies which aim to increase the security of a host system for the workloads which will be executing on it.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".

[2] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[3] ISO/IEC 18031:2001: "Information technology -- Security techniques -- Random bit generation or equivalent specification".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST Publication (SP) 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".

[i.2] NIST Publication (SP) 800-88 revision 1: "Guidelines for Media Sanitization".

[i.3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.4] Greg Hoglund, Gary McGraw (2007): "Exploiting Online Games: Cheating Massively Distributed Systems", Addison-Wesley, New Jersey.

[i.5] ETSI TS 103 487 "CYBER; Baseline security requirements regarding sensitive functions for NFV and related platforms".

[i.6] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.7] NIST SP800-123: "Guide to General Server Security".

[i.8] NIST SP800-125: "Guide to Security for Full Virtualization Technologies".

[i.9] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model".

[i.10] ETSI GR NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.11] ETSI GS NFV-INF 004 (V1.1.1): "Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain".

[i.12] TCG: "Virtualized Trusted Platform Architecture Specification", Version 1.0, Revision 0.26.

[i.13] NIST SP 800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

host system: collection of hardware, software and firmware making up the system which executes workloads

NOTE 1: When the host system is part of the NFVI, it is the "hypervisor" and "host" as defined by ETSI NFV-INF 004 (V1.1.1) [i.11]. In the case of virtualisation of workloads within the MANO domain, there is no corresponding definition available.

NOTE 2: The definition in ETSI NFV-INF 004 [i.11] specifically excludes containers, but the present document does not.

workload: component of the NFV architecture that is virtualised in the context of a particular deployment

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABAC	Attribute-Based Access Control
DH	Diffie-Hellman
DHE	Diffie-Hellman Exchange
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
ECP	Elliptic Curve modulo a Prime
GMAC	Galois Message Authentication Mode
HBRT	Hardware-Based Root of Trust
HMEE	Hardware-Mediated Execution Enclave
ICV	Integrity Check Value
HSM	Hardware Security Module
IOMMU	Input-Output Memory Management Unit
MANO	MANagement and Orchestration
MODP	More mODular exPonential
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PRF	Pseudo-Random Function
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman

SSL	Secure Sockets Layer
TCB	Trusted Computing Base
TCG	Trusted Platform Group
TLS	Transport Layer Security
TPM	Trusted Platform Module

4 Principles

4.1 Introduction

Trust, as defined in ETSI GR NFV-SEC 003 [i.10], is an important component of security. One weakness of software as opposed to hardware, is that software can be copied in whole or in part. Trust that is rooted in software may be less reliable than trust rooted in hardware, quickly, easily, and any number of times. For the particular case of sensitive workloads that have to be trusted, only the highest assurance in the root of trust is considered acceptable, thus for the purposes of the present document the root of trust shall be provided in hardware.

There is, however, a concomitant concern that when a device is subject to black box testing, it is impossible to determine if the responses to interrogation come from hardware or software. To counter this, a NFVI vendor shall be able to provide evidence on demand that the root of trust is a hardware element. The means by which the vendor provides such evidence is not considered in the present document but should be mutually agreed between the vendor and operator.

A vendor shall be able to provide evidence on demand to authorized parties of the security claims for the root of trust. The means by which the vendor provides such evidence is not considered in the present document, but should be mutually agreed between the vendor and operator. An examples of 3rd party assurance programme is Common Criteria (defined in ISO/IEC 15408 [i.9]).

The host system, acting as a black box (closed) environment, shall provide access to authorized external entities only to those capabilities identified in the authorization agreement.

5 Platform requirements

5.1 Core hardware requirements

1) The host system shall implement a Hardware-Based Root of Trust (HBRT) as Initial Root of Trust with the following requirements:

   - The HBRT shall be both physically and electronically tamper-resistant.
   - The HBRT shall be both physically and electronically tamper-evident.
   - The HBRT physical and software interfaces between the HBRT and other hardware components of the host system to which it directly communicates shall be protected from eavesdropping, manipulation, replay or similar attacks.
   - The level of resistance against attacks of the HBRT shall be verifiable and trustable using a certification process.
   - It shall be possible to restrict the booting procedure if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material.
   - Any tampering to the HBRT should lead to detectable degradation of its function.
   - The HBRT shall be physically protected such that any attempts to remove or replace the HBRT shall cause physical damage to both the HBRT and host system hardware to which the HBRT is attached, rendering both inoperable.

- The HBRT shall be (physically and/or logically) bound to the host system, so that any attempt to remove the HBRT will be detected and prevent normal operation of the host system.
- The HBRT shall include an Immutable Unique Identification value physically linked to the physical root of trust that can be used as identification of the platform. This value shall be stored in a shielded location protected from unauthorized use and disclosure.
- The HBRT shall provide capabilities to allow itself to be part of an attestation function.
- The host system shall have a mechanism to discover the tampered/non-tampered status of the HBRT.
- The host system shall have an interface to provide authorized external services with information about the tampered/non-tampered status of the HBRT.
- The host system shall provide a mechanism to report to authorized external services when tamper events occur.
- The HBRT shall implement a key management function with the requirements in the following bullet 2.

2) The host system shall implement a key management system which includes key generation, key storage, key deletion and cryptographic processing with the following requirements:

- The cryptographic material shall be stored in a shielded location, protected against eavesdropping and physical and environmental tampering.
- The key generation processing shall be protected against eavesdropping and physical and environmental tampering.
- The key management system shall include an access right management to the sensitive data.
- The key management system shall ensure a complete deletion of outdated keys under deletion request.
- The key management system shall be scalable and ensure a high availability service.
- The key management system shall be remotely manageable to allow evolution, security strengthening, and countermeasure deployment of the system.

The host system shall provide cryptographically separated secure environments to different applications.

5.2 Core software requirements

The following core software requirements are defined within the present document:

- Secure logging
- OS-level access control
- Logical authentication controls
- Communications security (e.g. Confidentiality, Integrity, Availability, Non-repudiation)
- Secure firmware (e.g. BIOS) upgrade
- Secure remote management of keys, cryptographic algorithms and security services offered by the platform to ensure ability of evolution, security strengthening, and countermeasure deployment

It shall be possible to restrict the booting procedure by preventing the running of workloads if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material. The intent of this requirement is to stop VNFs/VNFCIs being loaded onto possibly compromised hardware and to allow appropriate mitigations to be put in place.

6 Lifecycle

6.1 Trusted Computing Base

The Trusted Computing Base (TCB) comprises those components of the system - hardware, software and processes - that need to be trusted by default: it is on this foundation that the host system operates and on which the workload can operate with defined levels of trust in the overall security of the system. An example of a simplified boot scheme diagram for a TCB which utilizes at TPM as its Hardware-Based Root of Trust (HBRT) is provided in figure 1.

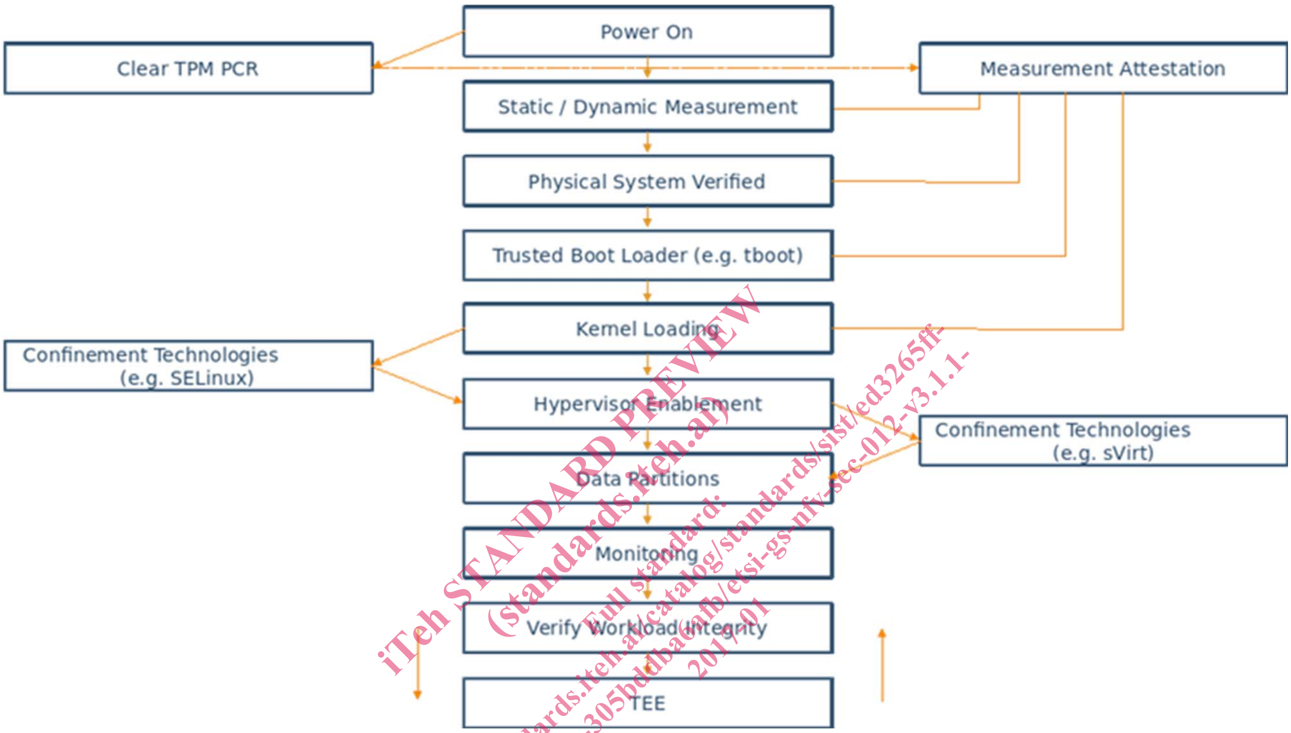

Figure 1: Example of a simplified boot scheme diagram using a Trusted Platform Module (TPM)

The detailed steps for building a TCB will be NFVI-vendor dependent, and are beyond the scope of the present document. One example of detailed guidance is Virtualised Trusted Platform Architecture Specification, Version 1.0, Revision 26 (TCG) [i.12].

The host system shall support the use of a service providing remote attestation.

Although the scope of the present document does not allow for requirements to be imposed on systems external to the host system, the attestation server should be implemented as a "bare-metal" deployment, rather than as a virtualised workload. This is because the attestation server needs to serve as one of the fundamental roots of trust of the MANO domain, and from there to the NFVI domain.

The measures discussed in the present document provide various protections for the host system and the workloads which execute on it. Vulnerabilities may exist which allow attackers using a compromised workload to "break out" to its host system. While the measures in clause 8.2, when correctly implemented, can mitigate against such compromises, a serious compromise of a host system may have implications beyond that single host system. This is especially true where explicit or implicit trust relationships exist between host systems in, for example, virtualised computing clusters. Although out of the scope of the present document, it is important that, when considering a deployment, the implications of explicit and implicit trust relationships are considered.

6.2 Workload provisioning

The host system shall have an interface to provide authorized external services with information about its ability to prohibit host or hypervisor memory deduplication techniques that allow for sharing of memory pages between workloads.