ETSI GS NFV-SEC 001 V1.1.1 (2014-10)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV);
NFV Security;
Problem Statement

Disclaimer

This 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-SEC001

Keywords

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

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 (http://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**", "**may not**", "**need**", "**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 aims to:

- To identify potential security vulnerabilities of NFV and to determine whether they are new problems, or just existing problems in different guises.
- To provide a reference framework within which these vulnerabilities can be defined.

Out of scope: To list vulnerabilities that NFV suffers from that are no different from pre-existing vulnerabilities of networking and virtualisation technologies and are not altered by the virtualisation of network functions.

Intended audience: Security experts wanting to deploy NFV but needing to identify and solve potential security issues and then to attain security accreditation for systems.

Ultimate goal of the NFV Security Expert Group: Identify and propose solutions to any new vulnerabilities that result from the introduction of NFV. To enable checks for these vulnerabilities to be incorporated into processes for security accreditation of products based on NFV.

2 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 http://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.

2.1 Normative references

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

Not applicable.

2.2 Informative references

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] Homomorphic Encryption.

NOTE: http://en.wikipedia.org/wiki/Homomorphic_encryption.

[i.2] Trusted Computing Group.

NOTE: http://www.trustedcomputinggroup.org/.

[i.3] Unified Extensible Firmware Interface (UEFI) forum.

NOTE: http://www.uefi.org/home/.

[i.4] ISO/IEC 11889-1 (March 2009(en)): "Trusted Platform Module - Part 1: Overview".

[i.5] CERT Vulnerability Note VU#362332 (August 2010).

[i.6] NIST SP 800-147 (April 2011): "Basic Input/Output System (BIOS) Protection Guidelines".

[i.7] NIST SP 800-155 (December 2011): "DRAFT BIOS Integrity Measurement Guidelines".

[i.8] TPM Main Specification (March 2011).

NOTE: http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

[i.9] Virtualized Trusted Platform Architecture Specification (September 2011).

NOTE: http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

[i.10] NIST SP 800-147b (July 2012): "DRAFT BIOS Protection Guidelines for Servers".

[i.11] NFV White paper (October 2012): "Network Functions Virtualisation, An Introduction, Benefits, Enablers, Challenges & Call for Action. Issue 1".

NOTE: http://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[i.12] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.13] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.14] ETSI GS NFV INF 001-1 (V0.3.8 April 2014): "Network Functions Virtualisation; Infrastructure Architecture; Sub-part 1: Overview", (work in progress).

[i.15] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.16] David Kleidermacher and Mike Kleidermacher: "Embedded Systems Security", Newnes, April 2012.

[i.17] Rowan Klöti, Vasileios Kotronis and Paul Smith: "OpenFlow: A Security Analysis". In Proc. Wkshp on Secure Network Protocols (NPSec). IEEE, October 2013.

[i.18] Diego Kreutz, Fernando M.V. Ramos and Paulo Verissimo: "Towards secure and dependable software-defined networks". In Proc. 2nd ACM SIGCOMM workshop on Hot topics in software defined networks, HotSDN '13, pages 55-60, New York, NY, USA, 2013. ACM.

[i.19] ONF Security Discussion Group.

NOTE: https://www.opennetworking.org/working-groups/discussion-groups.

[i.20] OpenFlow Switch Specification.

NOTE: Available via http://archive.openflow.org/wp/documents/.

[i.21] Recommendation ITU-T Y.3500 (July 2014) | International Standard ISO/IEC 17788 "Information technology - Cloud computing - Overview and Vocabulary".

[i.22] Thomas Ristenpart, Eran Tromer, Hovav Shacham and Stefan Savage: "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds". In Proc. Conference on Computer and Communications Security (CCS'09), pages 199--212. ACM, November 2009.

[i.23] Dawn Song, David Wagner and Adrian Perrig: "Search on Encrypted Data". In Proc. IEEE Symposium on Security and Privacy, May 2000.

[i.24] IETF draft-mrw-sdnsec-openflow-analysis-02 (April 2013): "Security Analysis of the Open Networking Foundation (ONF) OpenFlow Switch Specification", Margaret Wasserman and Sam Hartman, (work in progress).

[i.25] IEEE 802.1ah: "Provider Backbone Bridges".

[i.26] IEEE 802.1ad: "Provider Bridges".

[i.27] IETF draft-mahalingam-dutt-dcops-vxlan-09 (April 2014): "VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", M. Mahalingam and others, (work in progress).

[i.28] IETF draft-davie-stt-06 (April 2014): "A Stateless Transport Tunneling Protocol for Network Virtualization (STT)", Bruce Davie and Jesse Gross, (work in progress).

[i.29] IETF draft-sridharan-virtualization-nvgre-04 (February 2014): "NVGRE: Network Virtualization using Generic Routing Encapsulation", Murari Sridharan and others, (work in progress).

[i.30] IETF RFC 3031 (January 2001): "Multiprotocol Label Switching Architecture", Eric Rosen, Arun Viswanathan and Ross Callon.

[i.31] ETSI/TC LI#35 LI(14)P35037r2 "NFV LI Considerations".

[i.32] NFV White paper (October 2013): "Network Functions Virtualisation, Network Operator Perspectives on Industry Progress".

NOTE: http://portal.etsi.org/NFV/NFV_White_Paper2.pdf.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.15] and the following apply:

Forwarding Function: provides forwarding connectivity between multiple (two or more) network interfaces

NOTE 1: This distinguishes a Forwarding Function from just any networked application. A Forwarding Function receives data at any of the interfaces, processes it, then outputs some transformation of the original to other network interface(s).

EXAMPLE: Message routing or the filtering provided by a firewall. Some examples of other network functions are shown in Figure 1.

NOTE 2: 'Some transformation' is necessarily vague. It is meant to preclude server applications that might take in requests on one interface and send out responses on another. But it is meant to include, say, deep packet inspection or a packet filter that takes in data packets on one interface and forwards most to an output interface, but discards or re-orders some packets in the process. It also includes switches or network address translators that largely forward the data unchanged, but make a few focused changes to addresses. It even includes meters that take a packet flow as input and output a stream of measurement data that summarises the characteristics of the input flows.

NOTE 3: Although a Forwarding Function is defined by its multiple data interfaces, the definition does not preclude other interfaces for control (e.g. routing messages) and management - and these are certainly within scope of security problem analysis.

NOTE 4: All Forwarding Functions are Network Functions, but some Network Functions do not involve forwarding. For instance, most directory, control or management functions are Network Functions but not Forwarding Functions.

hypervisor: computer software, firmware or hardware running on a host computer that creates, runs and monitors guest virtual machines.

NOTE: A hypervisor enables multiple instances of a variety of guest operating systems to share the virtualised hardware resources of the host.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.15] and the following apply:

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
BGP	Border Gateway Protocol (IETF)
BIOS	Basic Input/Output System
CA	Certification Authorities
CPU	Central Processing Unit
DMA	Direct Memory Access
ECDSA	Elliptic Curve Digital Signature Algorithm
FB	Functional Block
FTP	File Transfer Protocol (IETF)
GRE	Generic Routing Encapsulation (IETF)
GS	Group Specification (ETSI)
I/O	Input/Output
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IOMMU	I/O Memory Management Unit
ISG	Industry Specification Group (ETSI)
IS-IS	Intermediate System to Intermediate System (IETF)
ISO	International Organisation for Standardization
IT	Information Technology
JTAG	Joint Test Action Group
LAN	Local Area Network
LI	Lawful Interception (ETSI TC)
LOM	Lights-Out Management
MAC	Medium/Media Access Control
MANO	Management & Orchestration
MMU	Memory Management Unit
MPLS	Multi-Protocol Label Switching (IETF)
NAT	Network Address Translator
NFV	Network Functions Virtualisation
NFVIaaS	NFV Infrastructure as a Service
NIST	National (US) Institute of Standards and Technology
NOC	Network Operations Centre
NV-GRE	Network Virtualisation using GRE
ONF	Open Networking Foundation
OS	Operating System
OSPF	Open Shortest Path First (IETF)
PCI	Peripheral Component Interconnect
QoS	Quality of Service
RSA	Rivest-Shamir-Adleman
SDN	Software Defined Network
SMMU	System MMU (ARM)
SR-IOV	Single Root I/O Virtualisation (a PCI special interest group standard)
STT	Stateless Transport Tunnelling
TC	Technical Committee
TCG	Trusted Computing Group
TLS	Transport Layer Security (IETF)
TPM	Trusted Platform Module (TCG)
UEFI	The Unified Extensible Firmware Interface forum
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtualised Network Function
VNFaaS	VNF as a Service
VNPaaS	Virtualised Network Platform as a Service
VPN	Virtual Private Network
VT-c	Virtualisation Technology for connectivity (Intel)

VT-d	Virtualisation Technology for directed I/O (Intel's IOMMU)
VXLAN	Virtual eXtensible LAN

4 Industry Context

Traditionally, Network Functions have been bundled into bespoke hardware appliances. In contrast, network functions virtualisation (or NFV) is the deployment of these services as software modules that run on common off-the-shelf generic hardware [i.11] over a hypervisor or container that controls access to the hardware devices.

Network function virtualisation has become economic because the sheer scale of the data centre market has drawn investment and skills towards generic server technology; 9 million IT servers are bought globally each year, but only 180 thousand edge routers. It is safe to predict that a network equipment facility will become physically the same as a data centre. Virtualised network functions will also be managed in common with IT management processes - as orchestrated remote software installations deployed independently to hardware upgrades.

The transition towards network functions virtualisation will be incremental. As each bespoke appliance reaches the end of its life it will be replaced by a software equivalent. Independently, more server blades, storage or network interface cards will be plugged in to existing racks to provide the necessary hardware resources. For further information, see [i.11] and for an update on industry activity on NFV see [i.32].

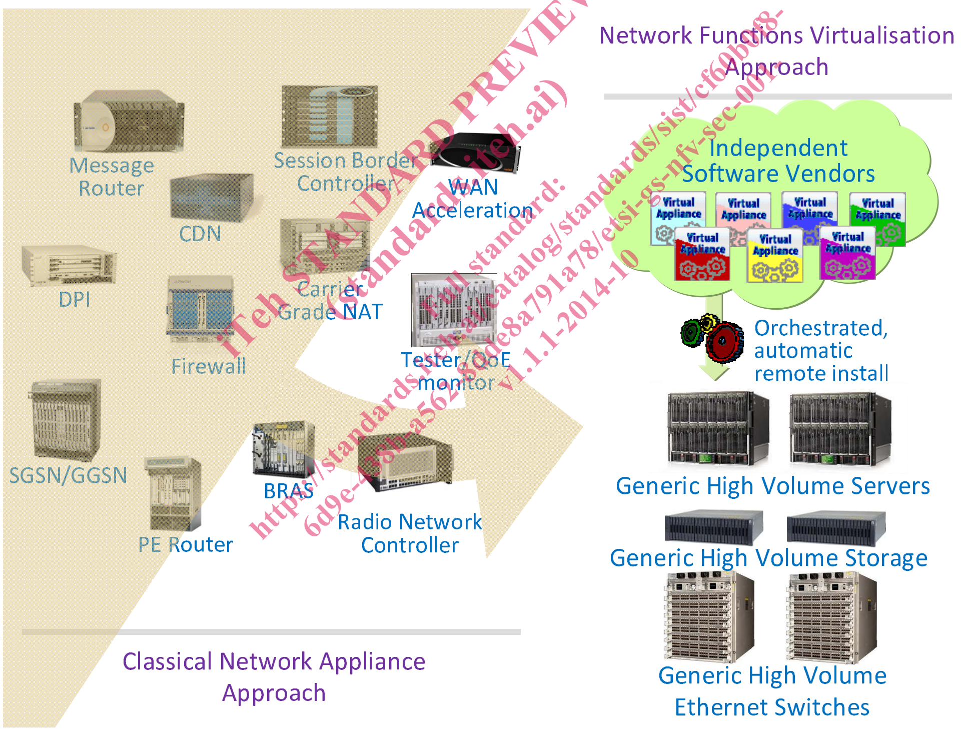
Network Functions Virtualisation Approach
Message Router
Session Border Controller
WAN Acceleration
CDN
Independent Software Vendors
Virtual Appliance
DPI
Carrier Grade NAT
Firewall
Tester/QoE monitor
Orchestrated, automatic remote install
SGSN/GGSN
BRAS
Generic High Volume Servers
PE Router
Radio Network Controller
Generic High Volume Storage
Generic High Volume Ethernet Switches
Classical Network Appliance Approach

Figure 1: Examples of Network Functions showing the Incremental Process of Virtualisation

NOTE 1: Network functions virtualisation should not be confused with virtual networks like virtual local area networks (VLANs) or virtual private networks (VPNs) - the two concepts are orthogonal. Another term for virtual networks is overlay networks, and again NFV is orthogonal to overlays. A virtual network is a logical partition carved out of a physical network by ensuring its logical connectivity is isolated from other virtual networks. In contrast, NFV only concerns whether the functions of the nodes of a network are implemented as software on generic hardware and hypervisor technology, rather than on bespoke hardware.

NOTE 2: The scope of this problem statement does not include cases where there is no hypervisor or container. In other words, network functions running as software over a monolithic operating system, even if on industry-standard hardware are out of scope of the present document, given that bare metal introduces no security changes relative to the baseline (which is bare metal).

5 Security Reference Framework

5.1 Deployment Scenarios

Figure 2 illustrates the elements with potentially separate security responsibility in different deployment scenarios: the building, the host compute hardware, the hypervisors and the guest virtual network functions within their virtual machines.

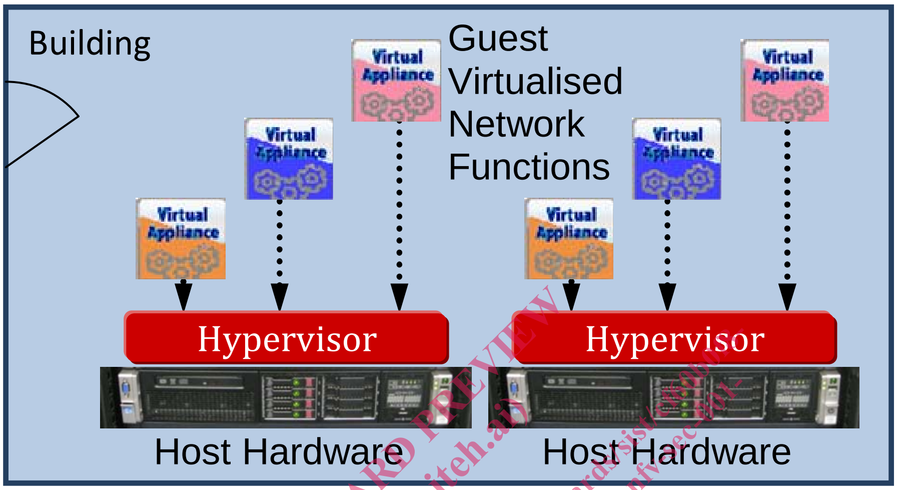

Figure 2: Deployment scenario elements

Below some deployment scenarios are described that are likely in realistic contractual arrangements.

For convenience they are summarised in Table 1. The right-most column also identifies which NFV deployment scenarios are similar to the common deployment models used in cloud computing, as identified by the ITU-T [i.21]. It can be seen that the cloud computing industry uses deployment models that sometimes, but not always, relate to those expected for NFV. The ITU-T document [i.21] also defines Cloud Service Models (Infrastructure, Platform and Software as a Service). It is possible that virtualisation of network functions might eventually become commoditised into a set of similar service models, but the NFV industry needs to be allowed to mature before jumping to conclusions on popular service models.

Table 1: Some realistic deployment scenarios

Deployment Scenario	Building	Host Hard-ware	Hyper-visor	Guest VNF	cf. ITU-T Cloud Vocabulary
Monolithic Operator	N	N	N	N	Private Cloud
Network Operator Hosting Virtual Network Operators	N	N	N	N, N1, N2	Hybrid Cloud
Hosted Network Operator	H	H	H	N	
Hosted Communications Providers	H	H	H	N1, N2, N3	Community Cloud
Hosted Communications and Application Providers	H	H	H	N1, N2, N3, P	Public Cloud
Managed Network Service on Customer Premises	C	N	N	N	
Managed Network Service on Customer Equipment	C	C	N	N	
NOTE: The different letters represent different companies or organisations, and are chosen to represent different roles, H = hosting provider, N = network operator, P = public, C = customer.					

Monolithic Operator: The same organisation that operates the virtualised network functions deploys and controls the hardware and hypervisors they run on and physically secures the premises in which they are located.