ETSI TR 103 308 V1.1.1 (2016-01)

TECHNICAL REPORT

CYBER;
Security baseline regarding LI and RD for NFV and related platforms

Reference

DTR/CYBER-0006

Keywords

cyber security, Lawful Interception, NFV

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
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:
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 (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 Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

Introduction

ETSI ISG NFV (and others) are creating an ecosystem whereby traditional network functions that may have been tangible, are now virtualized, potentially onto commercial "off the shelf" hardware. There is a requirement for ISG NFV to utilize features and functions available within the underlying platform for the purposes of ensuring lawful interception (LI) and Retained Data (RD) operations are appropriately protected and delivered - the present document intends to outline those requirements, capabilities and how they could be utilized.

The security principles themselves can include:

- Effective use of TPMs/Roots-of-Trust/Trusted-boot.
- Hardware and Software Integrity for NFV related platforms.
- Validation of hardware components.
- Restriction of interfaces.
- Process isolation.
- Effective and appropriately secure logging/reporting/crash management.
- Control of 'Root' account or equivalents.
- OAM access is authenticated and isolated as appropriate.
- Availability of patching/software update process.
- Management of logical entities in terms of physical and (potentially) legal constraints.

The present document intends to promote the minimum set of security features that telecommunications network equipment subject to LI or RD operations should have, and operators should expect, regardless of whether the vendor wishes to undergo an assurance process.

The establishment of a baseline will also simplify establishing security principles for more specific network equipment. For example, the baseline would be a natural place to start when establishing security principles/requirements for NFV hosts.

1 Scope

The present document treats the Lawful Interception (LI) and, where relevant, Retained Data (RD) capability being virtualized, taking into account the legal and physical challenges of doing so. This initial study is focused on the LI and RD aspects and establishes the fundamental security principles for generic platforms upon which the related groups can build. It includes a minimum set of security principles for those generic telecommunications platforms that are subject to LI that will allow the virtualized network functions to utilize the features necessary to afford them appropriate protection and at the same time to undertake appropriate activities (LI and RD). Establishing such a baseline will help the industry as a whole to be better protected against Cyber threats.

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 reference 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.

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

Not applicable.

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] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.2] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.3] S. Cadzow: "Secure Cryptographic Mechanisms - entropy and randomness".

NOTE Available at http://www.tvra-tools.eu/blog/technology/cryptography/secure-cryptographic-mechanisms-entropy-and-randomness/.

[i.4] T. Ristenpart and S. Yilek: "When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography", ISOC, 2010.

[i.5] Z. Gutterman, B. Pinkas and T. Reinman: "Analysis of the Linux Random Number Generator".

3 Definitions and abbreviations

3.1 Definitions

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

Element Management System (EMS): management function for a VNF

Hosting Provider: entity that owns and/or runs the NFVI and is assumed to provide the interfaces for an operator to manage their VNF

Network Functions Virtualisation Infrastructure (NFVI): totality of all hardware and software components that build up the environment in which VNFs are deployed

NFV Management and Orchestration (MANO): component consisting of the Orchestrator, Virtualized Infrastructure Manager and VNF Manager

NOTE: It may additionally contain other management related systems as necessary (e.g. including but not limited to security orchestration).

Operator: runs the network and manages the VNFs

Orchestrator: component in charge of the management of NFV infrastructure and software resources

Virtualized Infrastructure Manager: allocates resources to the NFV infrastructure (i.e. energy efficiency)

Virtualized Network Function (VNF): software implementation of a network function

VNF Manager: in charge of the lifecycle of an NFV

3.2 Abbreviations

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

AUC	Authentification Centre
CPU	Central Processor Unit
EMS	Element Management System
GPU	Graphics Processing Unit
GSMA	Global System for Mobile communications (GSM) Association
IN	Intelligent Network
IPC	Inter-Process Communication
ISG	Industry Specification Group
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MANO	Management and Orchestration
NFS	Network File System (protocol)
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
OAM	Operatjion and Maintenance
PRNG	Pseudo Random Number Generator
RD	Retained Data
SDN	Software Defined Networking
SMS	Short Message Service
SSL	Secure Sockets Layer
TC	Technical Committee
TPM	TrustIed Platform Module
VM	Virtual Machine
VNF	Virtualized Network Function
VNFI	Virtualized Network Function Infrastructure

4 Problem statements

4.1 In support of LI and RD for NFV

The following requirements derived from LI and RD work in both ISG NFV and TC LI describe the challenges facing NFV. The following general security issues need to be considered:

- The LI VMs are likely to have to exist in a separate security domain.
- The VM hypervisor administration often needs to enable the LI functionality but once paired to an external LI administration system it needs not to be possible to disable it again without authorization by the LI administration system.
- All VMs in the array may need to use code signing integrity protection to prevent unauthorized and/or undetected VM module code changes.
- The LI administration system needs to be able to dual sign the LI VMs and check the signatures.
- Each LI VM may need to be pairable using separate security keys.
- All events performed by the LI VMs need to generate logged events which can be read by the LI administration system (prevents changes to VMs outside of audit times). Log events which result from events occurring within the LI VMs need to only be visible to the LI administration system and not the hypervisor or other VMs/administrators.

4.2 For LI in NFV

- **Virtual Network Functions can be verified** - the intent behind this principle is that VNFs are signed and that the static component of the VNF can be verified during boot, run-time, suspension and transfer. Additionally, data used by the VNFs is properly structured and hence its integrity can be checked.
- Data used by the VNF is properly structured (according to known schemata), can be integrity checked (e.g.: signing, etc.) and is tamper-proof.
- **The virtualization layer contains a security component** - the intent behind this principle is that security is a central component of the virtualization layer. In addition, the virtualization layer needs to facilitate the integrity scanning of VNFs and the monitoring of network links.
- **Host platforms are updatable and auditable** - the intent behind this principle is that host platforms are limited in functionality and that this functionality has been scrutinized and kept up-to-date.
- **The virtual and physical architecture is managed** - the intent behind this principle is the operator is able to define a secure virtual architecture that will be implemented by the host infrastructure. Furthermore, operators need to be able to place security constraints on the physical architecture that is hosting the virtual network.
- **NFV management needs to incorporate security management** - the intent behind this principle is that the NFV management system is the entity which is able to fully understand the risks to the architecture. As such, it needs to be able to ensure that components of the system are instructed to protect data appropriately and that the monitoring processes are in place to detect any compromise of the system. The target list is critical information, which should be protected such that only the appropriate LI functions are entitled to read or modify this information.
- **The location is verified and evidential -** the location of any LI activity is known to ensure LI activity takes place where it can be protected and is legal to do so. This is critical to LI functionality. An essential requirement is that the LI takes place in the country/jurisdiction, or authorized countries/jurisdictions, that issued the authorization (this means that any LI-VMs plus the network function VMs that are being monitoring need to be in-country).
- **The virtual machine only operates with "known" LI virtual machines -** if an LI VM is instantiated it can only operate with the VM's it is allowed to. This implies the use of techniques described elsewhere in the present document e.g. software signing, attestation, trusted elements.

- **The target list and related signalling is appropriately protected -** the target list needs to be encrypted, as may the output traffic on X1. Any encryption needs to be robust, and not under full control within the VM layer.
- **Timestamps** - Synchronization needs to be built into the fabric of NFV by way of either physical layer functions on the NIC or NID or Operating System support for precise time. NFV could also enable a more tightly synchronized network by making precise time a generic function available everywhere.
- **The NFV system has to provide a source of true random numbers** - the intent behind this is to avoid the problem of weakened cryptography due to inherent problems in pseudo-random number generation in virtual machines.

5 Transposed LI and RD requirements into NFV platforms

5.1 Attestation

- User wants to store an attribute (e.g. hardware ID, location, etc.) and user needs to subsequently trust when that attribute is recalled/requested.
- User needs to verify arbitrary system information (e.g. VNF integrity).
- User needs to verify authentication of arbitrary system information (e.g. is VNF signed by a trusted party).

NOTE: User in this context means management entity or network operator.

5.2 Data at rest encryption

Although this could be implemented higher up the stack, to be done well it may require hardware support, for the encryption of target lists.

Selectors used to identify traffic to forward to the LEMF are sensitive and have to be stored in a secure manner. Access to these selectors should be restricted to those who should have access, and an audit record should be kept of the addition, update, access and removal of the selectors. The system used to store the LI selectors has to support secure distribution of those selectors to the parts of the network that need them to perform LI. The storage mechanism chosen should be resistant to a compromise of the virtualization layer.

5.3 Data in Transit Encryption

Similarly to data at rest encryption, all data in transit should be secured using suitable meanings in an end-to-end manner. If end-to-end security cannot be achieved then any break should be via a trusted entity.

5.4 Verified, Trusted or Measured Boot

Ensures system integrity. A secured boot is a process where the integrity of various components in a boot sequence have been measured and found to be either:

- in accordance with expected values or;
- within tolerable ranges for the required host profile.

See ETSI GS NFV-SEC 003 [i.2], clause 4.4.5.1 for further details.

This is important for Sensitive Application Functions. The VNFI may be to verify integrity of databases, static configuration data and application root key chain (e.g. AUC)

5.5 Tamper Evidence and Resistance

Databases, communication, storage should have resistance to data tampering, and also it should be evident if the data has been tampered with.