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

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".