ETSI GS NFV-SEC 006 V1.1.1 (2016-04)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV);
Security Guide;
Report on Security Aspects and Regulatory Concerns

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-SEC006

Keywords

NFV, regulation, 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 is a guide to developers of NFV related documents and applications in means to address the security aspects and regulatory concerns as they impact the security of deployed networks that conform with these documents and applications. The present document contains detailed descriptions of security concerns, attacks, as well as an overview of regulatory concerns and how they can be treated in system design to give the highest level of assurance that the resultant system is secure and complies with current regulation and best practice. The present document is intended for use by developers of NFV documents and the guidance is given in a manner that assists non-experts in security and regulation to prepare such documents.

In addition to the guidance and explanatory text the present document contains, in annex A, a pro forma template for use in ETSI ISG NFV documents to capture the security concerns and mitigations that apply.

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 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 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.3] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.4] Privacy Impact Assessment Handbook (2009).

NOTE: Available at http://www.piawatch.eu/node/48.

[i.5] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.6] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.7] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (Text with EEA relevance).

[i.8] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

NOTE: Available at http://eur-lex.europa.eu/

[i.9] ETSI GS NFV-SEC 004: "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implication".

[i.10] ETSI GS NFV-SEC 010: "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".

[i.11] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.12] UK Information Commissioners Office: Conducting Privacy Impact Assessments Code of Practice.

NOTE: Available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[i.13] ETSI ETR 332:"Security Techniques Advisory Group (STAG); Security requirements capture".

[i.14] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[i.15] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.16] Domains of Attack list and descriptions.

NOTE: Available at http://www.mitre.org. Please consult this website for detailed descriptions of each attack: http://capec.mitre.org/data/graphs/3000.html.

[i.17] IEC 60906-2: "IEC system of plugs and socket-outlets for household and similar purposes - Part 2: Plugs and socket-outlets 15 A 125 V a.c. and 20 A 125 V a.c.".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 165-1 [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 165-1 [i.1] and the following apply:

PP	Protection Profile
TVRA	Threat Vulnerability Risk Analysis

4 Security design guide

4.1 Overview and introduction

Security cannot be an afterthought, and has to be considered throughout the planning/development/deployment/runtime lifecycle. Unfortunately, effective security design is not trivial and there is a constant tension between functionality and security that inherently couples the two. A significant danger is that in progressing functionality it will become harder and harder to provide deeply rooted security in system designs. As with design of any type there are a number of ways to approach security in system design. The primary starting point in much of security is to identify an attack and pair it with a means to thwart the attack, such that a tuple of {issue, mitigation} will exist across the system.

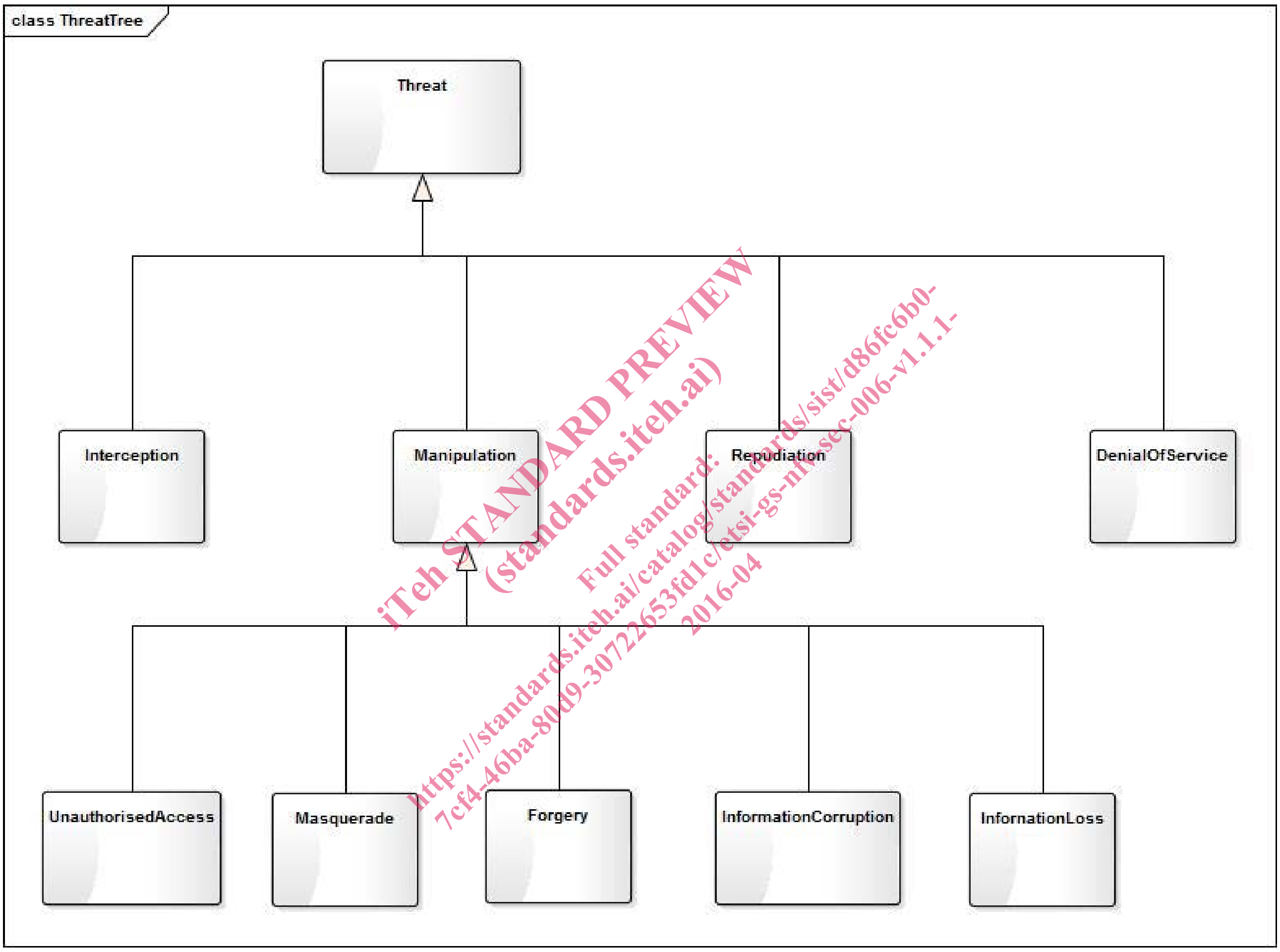

Figure 1: Illustration of a threat tree to identify forms of threat in systems

Whilst an understanding of threat trees (see figure 1) is useful it is not sufficient and has to be mapped to a wider understanding of countermeasures. For example the tuple {masquerade, authentication} suggest that if the authentication element is implemented properly it will counter masquerade, but the pre-requisites of authentication include identity management and credential management. If authentication is a cryptographic process further issues arise that include the viability of the authentication algorithms over time (and associated cryptographic strength), the means to distribute credentials (the pairing of identity and the cryptographically significant data used to assert it), and so forth.

In the regulatory domain the mind-map shown in figure 2 identifies some of the relationships between protection technology and attack types, and the relationship between privacy and regulation is highlighted. The latter is important as regulation exists to protect the obligation or right to privacy as identified in a number of acts and laws, however there are a number of exceptions to the right to privacy identified by the same broad set of acts and laws that generally give rights for law enforcement to have reasonable rights to protect the wider population sometimes with a short term risk to the individual. Such exceptions include the need to provide for Lawful Interception, and to retain data in the network in support of law enforcement.

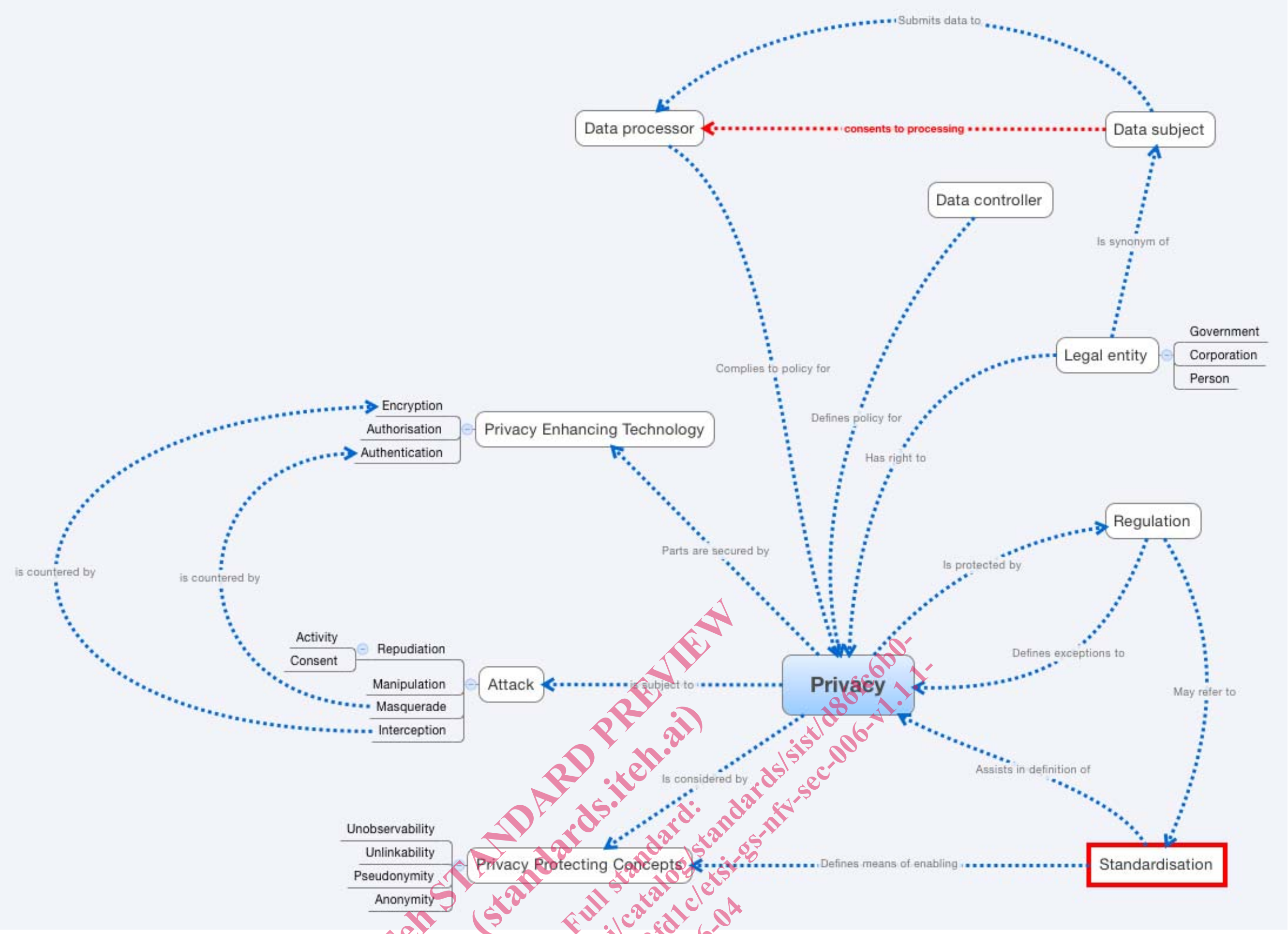

Figure 2: Mind-map illustrating complexity of privacy and privacy protection

In designing a secure system an understanding of the impact of attack has to be developed. For example, when two functions share a host, a Denial of Service attack on one may affect the other. The mitigation may be to not co-host high-priority functions with low-priority functions.

4.2 Risk, risk analysis, and risk management

Designing for the effective security of a system cannot be done without a reasonable understanding of risk, there are a large number ways of modelling security in systems that look variously at the process (Identify, Mitigate, Monitor as a continuous loop), and at the interactions of assets. The model given in ETSI TS 102 165-1 [i.1] and copied below makes a number of assumptions including:

- systems are compositions of a set of assets;
- assets may have inherent vulnerabilities;
- a vulnerability when discovered with a viable threat becomes a weakness;
- exploitation of a weakness leads to something unwanted in the system (unwanted incident); and,
- threat agents are used to enact threats and many threat agents may work together to exploit a weakness.

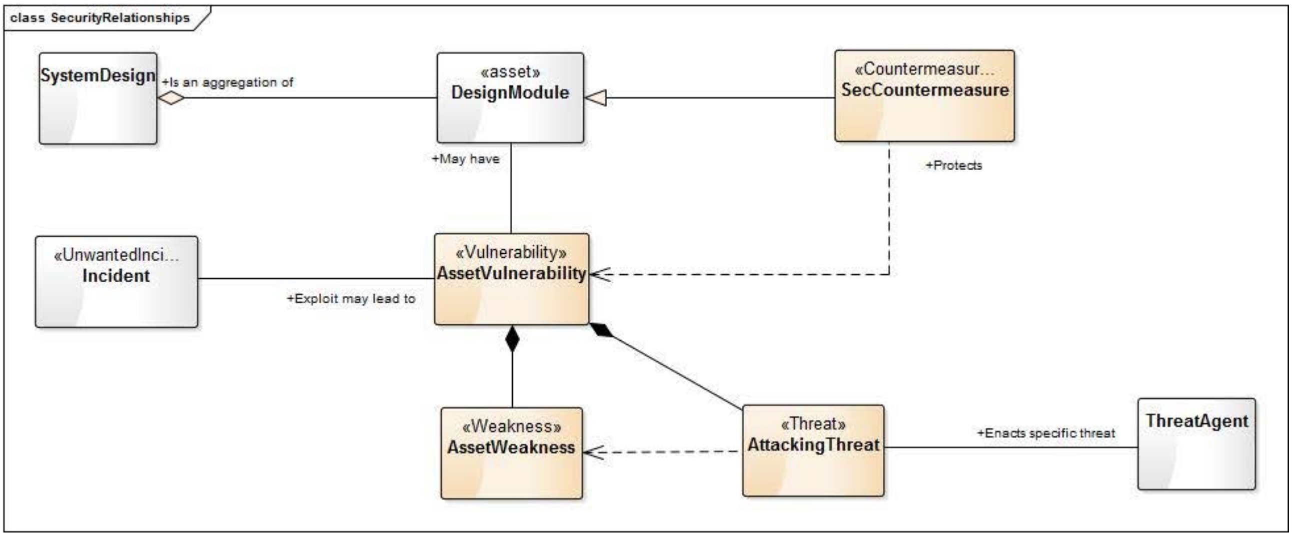

Figure 3: Generic security TVRA model from ETSI TS 102 165-1 [i.1]

There are a number of questions that arise from the generic model shown in figure 3 and these include:

- What are the assets of my system?
- How do I determine the vulnerabilities and when they become exploitable weaknesses?
- How do I protect my system?

The present document is part of the process in the identification of assets and their vulnerabilities by recommending a set of topics to be considered in every deliverable of ISG NFV.

Threats are potential events that can cause a system to respond in an unexpected or damaging way. It is useful to categorize threats to determine effective and deployable mitigation strategies. The identification and analysis of NFV relevant security threats (general and application specific) should include the following categories:

- Spoofing of identity (masquerade).
- Tampering with data (manipulation).
- Inappropriate information disclosure.
- Denial of service.
- Improper elevation of privileges.

Clauses 4.3 and 4.4 describe a number of strategies for identifying the threats in general terms in the NFV context.

4.3 Design for assurance

The Design for Assurance paradigm is closely aligned to the design for test paradigm. The aim of these paradigms is to ensure that when designing a system an independent tester can validate that the system actually performs to the design specification. The primary difference between design for test and design for assurance is that in the latter there are specific security claims that are being made and verified.