ETSI TS 102 165-1 V5.2.3 (2017-10)

TECHNICAL SPECIFICATION

CYBER;
Methods and protocols;
Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)

Reference

RTS/CYBER-0018

Keywords

authentication, confidentiality, 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

Essential patents

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering methods and protocols for security standardization, as identified below:

Part 1: "Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)";

Part 2: "Protocol Framework Definition; Security Counter Measures".

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

The present document is one of a set of documents that addresses standardization of security protocols and mechanisms within the context of the *e*Europe 2005 programme and which, within ETSI, has been considered as a tool in the "Design for Assurance" approach to achieving security in ICT systems. The suite of documents is composed as follows:

- ETSI EG 202 387 [i.1]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".
- ETSI ES 202 383 [i.23]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".
- ETSI ES 202 382 [i.24]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".
- **ETSI TS 102 165-1: "CYBER; Methods and protocols; Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)" (the present document).**

- ETSI TS 102 165-2 [i.25]: "CYBER; Methods and protocols; Protocol Framework Definition; Security Counter Measures".
- ETSI TS 102 556 [i.5]: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile".
- ETSI EG 202 549 [i.6]: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

These documents are developed based on the objectives of the *e*Europe programme and are also developed to ensure they comply with the overall objectives of the European regulatory framework as defined in the following documents:

- Directive 2002/19/EC [i.16] of the European Parliament and of the council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
- Directive 2002/20/EC [i.17] of the European Parliament and of the council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).
- Directive 2002/21/EC [i.18] of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
- Directive 2002/22/EC [i.19] of the European Parliament and of the council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
- Directive 2002/58/EC [i.20] of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The *e*Europe 2005 action plan has been drawn up to focus on "*the widespread availability and use of broadband networks throughout the Union … and the security of networks and information, eGovernment, eHealth and eBusiness*" requiring a supporting infrastructure, which is truly pan-European. To quote COM(2002)263 [i.8]: "*By 2005 Europe should have … a secure information infrastructure*".

1 Scope

The present document defines a method primarily for use by ETSI standards developers in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system.

NOTE: The method described has been tailored to apply to pre-production but can be applied to production devices with due attention given to possibility that the application of countermeasures may be unachievable for a re-design strategy.

The method described in the present document builds from the Common Criteria for security assurance and evaluation defined in ISO/IEC 15408 [i.27], [i.28], [i.29] and specifically targets the means to build a Threat Vulnerability and Risk Analysis (TVRA) to allow its reference by an ETSI specification developed using the guidelines given in ETSI EG 202 387 [i.1] and ETSI ES 202 382 [i.24]. The TVRA forms part of the documentation set for the Target Of Evaluation as specified in ETSI ES 202 382 [i.24] with its intended audience being a developer of standards based Protection Profiles.

The use of the method described in the present document for application outside the "Design for Assurance" paradigm described in ETSI EG 202 387 [i.1] is supported but some of the examples and stages of evaluation may not be appropriate.

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.

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 EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.2] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.3] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".