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

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".

[i.4] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".

[i.5] ETSI TS 102 556: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile".

[i.6] ETSI EG 202 549: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

[i.7] ETSI TS 102 051: "ENUM Administration in Europe".

[i.8] COM(2002)263: "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the regions".

NOTE: Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF.

[i.9] ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

[i.10] CESG: "HMG IA Standard Numbers 1 & 2 - Supplement - Technical Risk Assessment and Risk Treatment", Issue No: 1.0, April 2012.

NOTE: The document is no longer supported by CESG and has been replaced with new guidance. See for more information: https://www.cesg.gov.uk/articles/outcomes-over-process-how-risk-management-changing-government.
The document is still available at:
https://www.ncsc.gov.uk/content/files/guidance_files/IS1%20%26%202%20Supplement%20-%20Technical%20Risk%20Assessment%20and%20Risk%20Treatment%20-%20issue%201.0%20April%202012%20-%20NCSC%20Web.pdf, and is available for use under the Open Government Licence: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/1/open-government-licence.htm.

[i.11] CC Users Forum (September 2014): "Collaborative Protection Profiles: The Benefits of an Evolved Common Criteria Implementation".

NOTE: Available from http://www.ccusersforum.org/library/wp/cPP_White_Paper.pdf.

[i.12] ISO/IEC 27002:2005: "Information technology -- Security techniques -- Code of practice for information security management".

[i.13] ISO/IEC 27001:2005: "Information Technology - Security Techniques - Information Security Management Systems - Requirements".

[i.14] ptc/04-10-02: "Object Management Group. UML 2.0 Superstructure Specification", edition, 2004.

[i.15] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[i.16] Directive 2002/19/EC 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).

[i.17] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).

[i.18] Directive 2002/21/EC 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).

[i.19] Directive 2002/22/EC 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).

[i.20] Directive 2002/58/EC 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).

[i.21] ISO 31000:2009: "Risk management - Principles and guidelines".

NOTE: The above reference supersedes the reference to AS/NZS 4360: "Standards Australian, Risk Management" in earlier editions of the present document.

[i.22] ISO/IEC 18028:2005 (Parts 4 and 5): "Information technology -- Security techniques -- IT network security".

NOTE: ISO/IEC 18028 is a multipart publication and the reference above is used to refer to the series.

[i.23] 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.24] 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.25] ETSI TS 102 165-2 (2007): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.26] ETSI TS 187 001: "Network Technologies (NTECH); NGN SECurity (SEC); Requirements".

[i.27] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.28] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.29] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.30] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[i.31] ISO/IEC 17799: "Information technology -- Security techniques -- Code of practice for information security management".

[i.32] Common Methodology for Information Technology Security Evaluation: "Evaluation methodology", July 2009 Version 3.1 Revision 3 Final.

NOTE: Available at https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EG 202 387 [i.1], ISO/IEC 17799 [i.31], ISO/IEC 18028 [i.22] and the following apply:

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

availability: property of being accessible and usable on demand by an authorized entity ISO/IEC 18028 [i.22]

confidentiality: ensuring that information is accessible only to those authorized to have access

cyber herd immunity: a form of immunity to attack wherein a critical mass of vulnerable assets are protected against a certain type of attack such that it becomes unprofitable for attackers to attempt to discover unprotected assets to attack

impact: result of an information security incident, caused by a threat, which affects assets

integrity: safeguarding the accuracy and completeness of information and processing methods

mitigation: limitation of the negative consequences of a particular event

nonce: arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

NOTE: Although random and pseudo-random numbers theoretically produce unique numbers, there is the possibility that the same number can be generated more than once.

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

residual risk: risk remaining after risk treatment

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

threat: potential cause of an incident that may result in harm to a system or organization

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset (clause 6.2 of Common Criteria part 1 - ISO/IEC 15408-1 [i.27]).

NOTE 2: A **threat** is enacted by a **threat agent**, and may lead to an **unwanted incident** breaking certain pre-defined security objectives.

threat agent: entity that can adversely act on an asset

unwanted incident: incident such as loss of confidentiality, integrity and/or availability

NOTE: See ISO 31000 [i.21].

user: person or process using the system in order to gain access to some system resident or system accessible service

vulnerability: weakness of an asset or group of assets that can be exploited by one or more threats

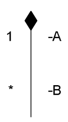
NOTE: A **vulnerability**, consistent with the definition given in ISO/IEC 18028 [i.22], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**.

3.2 Symbols

For the purposes of the present document, the symbols given in OMG UML2 [i.14] and the following apply:

Generalization/Specialization: UML concept showing relationship between entities A and B where the two entities exhibit the property that A (top of arrow) is the general case whereas B is the specific case

EXAMPLE: A countermeasure is a specialized asset.



Composition: UML concept showing relationship between entities A and B where A "is composed of" B

EXAMPLE: Vulnerability "is composed of" a threat and a weakness.

Dependency: UML concept showing relationship between entities A and B where B is dependent upon A

EXAMPLE: Security requirements "depend on" security objectives.

Aggregation: UML concept showing relationship between entities A and B where A "is an aggregate of" B

EXAMPLE: System "is an aggregate of" assets.

3.3 Abbreviations

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

ACK	ACKnkowlegement
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CC	Common Criteria
CIA	Confidentiality Integrity Availability
CIAAA	Confidentiality, Integrity, Availability, Authenticity and Accountability
CM	Configuration Management
CPU	Core Processor Unit
DDDS	Dynamic Delegation Discovery System
DDoS	Distributed Denial of Service
DNS	Domaine Name Service
DNSSEC	DNS SECurity
DoS	Denial of Service
EAL	Evaluation Assurance Level
ENUM	Electronic NUMbering
ERD	Entity Relationship Diagram
FAU	Functional class AUdit

NOTE: From ISO/IEC 15408-2 [i.28].

FCO Functional class Communication

NOTE: From ISO/IEC 15408-2 [i.28].

FCS Functional class Cryptographic Support

NOTE: From ISO/IEC 15408-2 [i.28].

FDP Functional class user Data Protection

NOTE: From ISO/IEC 15408-2 [i.28].

FIA Functional class Identification and Authentication

NOTE: From ISO/IEC 15408-2 [i.28].

FMT Functional class Security Management

NOTE: From ISO/IEC 15408-2 [i.28].

FPR Functional class Privacy

NOTE: From ISO/IEC 15408-2 [i.28].

FPT Functional class Protection of the TSF

NOTE: From ISO/IEC 15408-2 [i.28].

FRU Functional class Resource Utilization

NOTE: From ISO/IEC 15408-2 [i.28].

FTA Functional class TOE Access

NOTE: From ISO/IEC 15408-2 [i.28].

FTP Functional class Trusted Path/Channels

NOTE: From ISO/IEC 15408-2 [i.28].

HTTP Hyper Text Transmission Protocol
ICMP Internet Control Message Protocol
IMS IP Multimedia Subsystem
IN Intelligent Network
IP Internet Protocol
ISO International Standards Orgainsation
IT Information Technology
LAN Local Area Network
NAPTR Naming Authority PoinTeR
NGN Next Generation Network
NTP Network Time Protocol
OSI Open System Interconnection
PP Protection Profile
SIP Session Initiation Protocol
SNMP Simple Network Management Protocol
SQL Structured Query Language
SSH Secure SHell
ST Security Targets
SYN (TCP) SYN(chronize)
TCP Transport Control Protocol
TISPAN Telecommunications and Internet converged Services and Protocols for Advanced Networking
TOE Target Of Evaluation
TSF TOE Security Function
TSP TOE Security Policy
TTP Trusted Third Party
TVRA Threat Vulnerability and Risk Analysis
UDP User Datagram Protocol
UML Unified Modelling Language
URI Uniform Resource Identifiers

4 Introduction

4.1 Role of TVRA

It is recognized that without an understanding of the system, the threats to the system and a systematic countermeasure cost-benefit analysis that appropriate selection of countermeasures cannot be made. Within ETSI a Threat Vulnerability and Risk Analysis (TVRA) is used to identify risk to the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The TVRA method described in the present document is primarily aimed at use within the standards domain to give justification for the development of standards based security solutions. In addition the TVRA may be used as the source of parts of a Protection Profile (PP), see ETSI ES 202 382 [i.24]. Large parts of the descriptive text of a PP may in turn be derived from the TVRA:

- Security objectives;
- Security requirements;