

ETSI TS 102 165-1 V4.2.3 (2011-03)

Technical Specification

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 102 165-1 V4.2.3 \(2011-03\)](https://standards.iteh.ai/catalog/standards/etsi/c7e56fb6-7cea-4aaa-bf07-5dedfc0e8b4c/etsi-ts-102-165-1-v4-2-3-2011-03)

<https://standards.iteh.ai/catalog/standards/etsi/c7e56fb6-7cea-4aaa-bf07-5dedfc0e8b4c/etsi-ts-102-165-1-v4-2-3-2011-03>



Reference

RTS/TISPAN-07050-NGN-R3

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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTETM is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	6
Foreword.....	6
Introduction	6
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	9
3 Definitions, symbols and abbreviations	10
3.1 Definitions.....	10
3.2 Symbols.....	11
3.3 Abbreviations	11
4 Introduction	13
4.1 Role of TVRA	13
4.2 Generic TVRA relationships	15
4.3 Countermeasure strategies.....	18
4.3.1 Asset redesign	18
4.3.2 Asset hardening	18
4.4 Relationship with Common Criteria evaluation	18
5 TVRA method.....	19
5.1 Overview	19
5.1.1 Target of Evaluation description.....	21
5.1.1.1 Security environment	21
5.1.1.2 Security objectives.....	22
5.1.1.3 Security requirements.....	23
5.1.1.3.1 The relationship between security objectives and security requirements	23
5.1.1.3.2 Security requirements statements	23
5.1.2 Threats and threat agents	25
5.2 Actors and roles.....	27
5.3 Rationale.....	27
6 Method process	27
6.1 Overview	27
6.2 Step 1: Identification of Target Of Evaluation (TOE).....	28
6.3 Step 2: Identification of objectives	29
6.4 Step 3: Identification of functional security requirements.....	29
6.5 Step 4: Systematic inventory of the assets.....	30
6.6 Step 5: Systematic identification of vulnerabilities	31
6.6.1 Identification of weakness	32
6.6.2 Identification of a vulnerability	32
6.6.3 Identification of attack method (threat agent)	32
6.6.3.1 Assessment of the practicality.....	32
6.6.3.1.1 Knowledge factor	32
6.6.3.1.2 Time factor	33
6.6.3.1.3 Expertise factor.....	34
6.6.3.1.4 Opportunity factor	34
6.6.3.1.5 Equipment factor	34
6.6.3.1.6 Intensity factor.....	35
6.7 Step 6: Calculation of the likelihood of the attack and its impact	35
6.8 Step 7: Establishment of the risks	36
6.8.1 Impact of intensity	37
6.8.2 Classification of risk	37
6.8.2.1 Overview.....	37
6.9 Step 8: Security countermeasure identification	38

6.9.1	Countermeasures in the system.....	38
6.9.2	Composite countermeasures applied to the system.....	39
6.9.3	Impact of countermeasures applied to the system.....	39
6.10	Step 9: Countermeasure Cost-benefit analysis	39
6.10.1	Standards design	39
6.10.2	Implementation	39
6.10.3	Operation	40
6.10.4	Regulatory impact.....	40
6.10.5	Market acceptance	40
6.11	Step 10: Specification of detailed requirements	41
Annex A (normative):	TVRA proforma.....	42
Annex B (informative):	The role of motivation	43
Annex C:	Void	44
Annex D (informative):	Denial of service attacks	45
D.1	DDoS Attacks viable on the NGN	45
D.1.1	Land.....	45
D.1.2	SYN Flood.....	45
D.1.3	Ping of Death.....	45
D.1.4	Process Table.....	46
D.1.5	Smurf Attack	46
D.1.6	SSH Process Table	46
D.1.7	TCP Reset.....	46
D.1.8	Teardrop	46
D.1.9	UDP Storm	46
D.2	DDoS characteristics	47
D.3	Defence against DDoS	47
D.3.1	Preventive Mechanisms.....	47
D.3.2	Reactive Mechanisms.....	47
D.3.2.1	Signature detection mechanisms	48
D.3.2.2	Anomaly detection mechanisms	48
D.3.3	Difficulties of defence	48
Annex E (informative):	TVRA database structure	49
E.1	Database structure	49
E.2	SQL code for TVRA database.....	51
E.2.1	Lookup tables	51
E.2.2	Core tables.....	52
E.2.3	Linking tables.....	54
E.2.4	Sample queries (used to complete input to eTVRA proforma)	55
Annex F (informative):	Use of ISO/IEC 15408-2 security functional classes in security requirements statements	56
F.1	Overview	56
F.2	Review of functional capabilities	58
F.2.1	Authentication and identification	58
F.2.2	Communication class (non-repudiation)	59
F.2.3	User data protection class.....	60
F.2.4	Privacy class.....	64
F.2.5	Resource utilization class	66
F.2.6	Trusted path/channel class.....	66
F.2.7	Security management class.....	67
F.2.8	Protection of the TSF class.....	68
F.2.9	Cryptographic support class	70
F.2.10	Security audit class	71

F.2.11	TOE Access class	72
Annex G (normative):	TVRA Risk Calculation Template and Tool	74
Annex H (normative):	TVRA Countermeasure Cost-Benefit Analysis Template and Tool	75
Annex I (informative):	Bibliography	77
I.1	UML	77
Annex J (informative):	Change history	78
History		79

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ETSI TS 102 165-1 V4.2.3 \(2011-03\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/c7e56fb6-7cea-4aaa-bf07-5dedfc0e8b4c/etsi-ts-102-165-1-v4-2-3-2011-03>

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://webapp.etsi.org/IPR/home.asp>).

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 Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

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

Part1: "Method and proforma for Threat, Risk, Vulnerability Analysis";

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

Introduction

The present document is one of a set of documents that addresses standardization of security protocols and mechanisms within the context of the eEurope 2005 programme. 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 [1]: "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 [2]: "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: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Method and proforma for Threat, Risk, Vulnerability Analysis" (the present document).**
- ETSI TS 102 165-2 [4]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); 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 eEurope 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 [14] 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 [15] 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 [16] 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 [17] 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 [18] 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).

In particular the present document forms part of the standardization initiative for the Next Generation Network (NGN) platform to be used in eEurope and upon which the trust and viability of the e-enabled community will, to a very large part, depend on.

The eEurope 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"*.

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ETSI TS 102 165-1 V4.2.3 \(2011-03\)](https://standards.iteh.ai/catalog/standards/etsi/c7e56fb6-7cea-4aaa-bf07-5dedfc0e8b4c/etsi-ts-102-165-1-v4-2-3-2011-03)

<https://standards.iteh.ai/catalog/standards/etsi/c7e56fb6-7cea-4aaa-bf07-5dedfc0e8b4c/etsi-ts-102-165-1-v4-2-3-2011-03>