ETSI TR 187 002 V1.2.2 (2008-03)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis

Reference

RTR/TISPAN-07023-NGN-R1

Keywords

analysis, 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

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/chaircor/ETSI_support.asp

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://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 Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document presents the results of the Threat Vulnerability Risk Analysis (TVRA) for two scenarios of release 1 of the NGN. Those two analysed scenarios are PSTN/ISDN Emulation and NASS-IMS bundled authentication.

The present document follows the method and proforma for carrying out a TVRA [5] and incorporates material of the NGN threat and risk analysis herein.

The present document identifies security-relevant interfaces in the NGN, identifies security-relevant scenarios for use in the NGN, analyses NGN in terms of security threats and risks by performing a security threat and risk analysis, and classifies the identified vulnerabilities and the associated risk presented to the NGN.

This threat and risk analysis makes a number of assumptions that are believed to hold for typical deployment scenarios of NGN R1. Note however, that depending on actual instantiation of NGN, some of the made assumptions may not fully hold; this may potentially impact the associated risks.

NOTE: Security threats and risks for issues NGN release 2 or later may also be captured in the present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

[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".

[2] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[3] IEEE 802.11i: "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

[4] ISO/IEC 13335: "Information technology - Guidelines for the management of IT security".

[5] ETSI TS 102 165: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security".

[6] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[7] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[8] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[9] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[10] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[11] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

[12] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".

[13] ETSI EN 383 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control (BICC) Protocol or ISDN User Part (ISUP) [ITU-T Recommendation Q.1912.5, modified]".

[14] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 Release 7)".

[15] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102 Release 7)".

[16] AS/NZS 4360: "Risk Management".

[17] 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).

[18] 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).

[19] 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).

[20] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[21] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

[22] IETF RFC 2327: "SDP: Session Description Protocol".

[23] IETF RFC 3015: "Megaco Protocol Version 1.0".

[24] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[25] IETF RFC 3261: "SIP: Session Initiation Protocol".

[26] ETSI ES 283 003: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]".

[27] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203 Release 7)".

[28] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 Release 6)".

[29] ITU-T Recommendation H.248: "Gateway control protocol".

[30] 3GPP TR 33.803: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Coexistence between TISPAN and 3GPP authentication schemes (Release 7)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [1] and the following apply:

attack: attempt to bypass security controls on a computer

T-*nnn*: numeric identifier for a threat

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

NOTE: See ISO/IEC 13335 [4].

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

NOTE: See AS/NZS 4360 [16].

vulnerability: flaw or weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy

NOTE: Vulnerability is often used synonymously with weakness.

3.2 Abbreviations

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

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AGCF	Access Gateway Control Function
AGW	Access GateWay
A-MGF	Access Media Gateway Function
ARGW	Access Residential media GateWay
AS	Application Server
CC	Call Control
CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CLF	Connectivity session and repository Location Function
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
DNS	Domain Name System
DoS	Denial-of-Service
DTMF	Dual Tone Multi Frequency
EAP	Extensible Authentication Protocol
ECN	Electronic Communication Network
ECN&S	Electronic Communications Networks and Services
ECS	Electronic Communication Service
ESP	Encapsulating Security Payload
FFS	For Further Study
GPRS	GSM Packet Radio System
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol security
ISDN	Integrated Services Digital Network
ISIM	IMS subscriber Identity Module
ISO	International Standards Organization
ISUP	ISDN User Part
MGC	Media Gateway Controller
MGW	Media GateWay
MRFP	Media Resource Function Processor
NASS	Network Access SubSystem
NGN	Next Generation Network
NT	Network Termination
OSI	Open Systems Interconnection
P-CSCF	Proxy Call Session Control Function
PDBF	Profile Data Base Function
PES	PSTN/ISDN Emulation Subsystem
PS	Packet-Switched
PSTN	Public Switched Telephone Network
RACS	Resource Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RGW	Residential GateWay
R-MGF	Residential Media Gateway Function
ROM	Read-Only Memory
RTP	Realtime Transport Protocol
RTSP	Real-Time Streaming Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SEG	SEcurity Gateway
SGW	Signalling GateWay
SIP	Session Initiation Protocol
SpoA	Service point of Attachment

TDM	Time Division Multiplex
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TOE	Target Of Evaluation
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability Risk Assessment
UAAF	User Access Authorization Function
UE	User Equipment
UICC	Universal Integrated Circuit Card
UML	Unified Modelling Language
UPSF	User Profile Server Function
VLAN	Virtual Local Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

4 NGN-relevant Security Interfaces and Scenarios

This clause identifies the NGN use cases and therefore the NGN security environment that the TVRA has been applied to.

4.1 Security-relevant NGN Scenarios

Scenarios are presented following a complexity ordering, from a simple generic model to rather more complex scenarios.

4.1.1 Basic NGN scenario (ECN&S model)

The Electronic Communication Network (ECN) and Electronic Communication Service (ECS) model as shown in figure 1 is the model used in the Framework Directive [17] and simplifies the network into a set of provision types. An ECN is a communication network and roughly speaking addresses the lowest 3 layers of the ISO/OSI protocol stack. An ECS is a communication service and roughly speaking addresses the highest layers of the ISO/OSI stack. In order to connect a user connects to both an ECS and an ECN.

The basic model shows that the CPE may consist of more than one equipment type and that the NT has two connection points, one for services (SpoA) and one for Transport (or network) (TpoA).

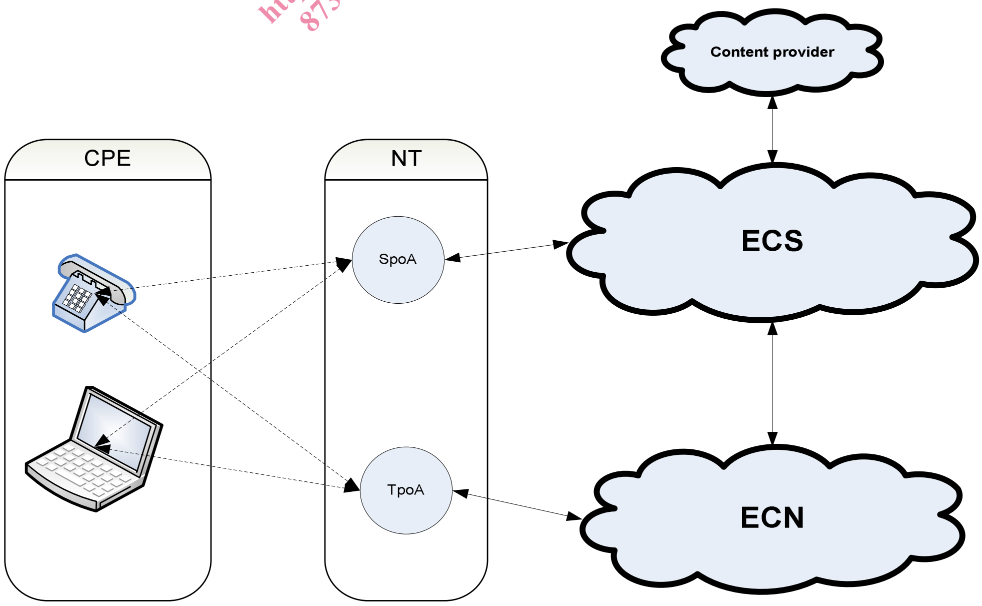
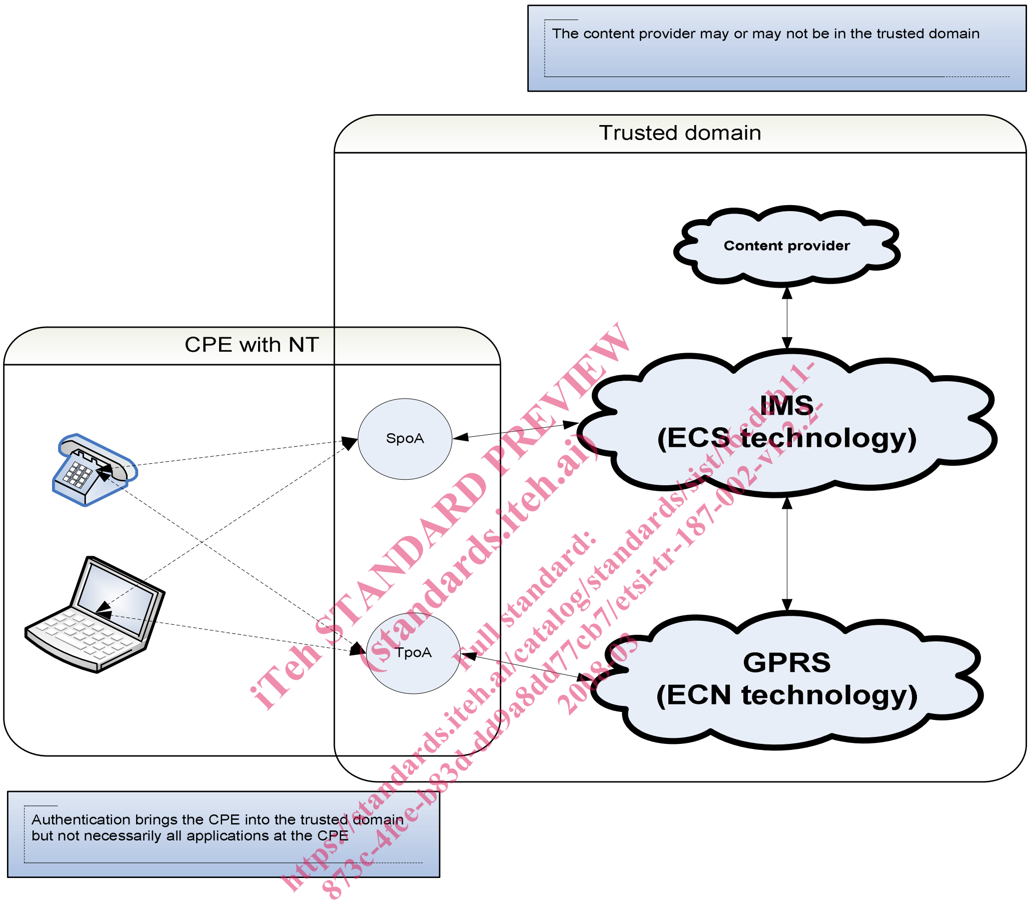


Figure 1: Basic ECN&S model for the NGN

4.1.2 IMS scenarios

4.1.2.1 3GPP IMS

The 3GPP IMS model does not in general distinguish ECS and ECN but there is a broad assumption that IMS lies on top of the PS subsystem which is an implementation of ECN using 3GPP specific access technology. The trusted domain therefore encompasses each of the NT, ECN (the GPRS network) and ECS (the IMS network), see figure 2 for a simplified IMS scenario.


The content provider may or may not be in the trusted domain

Authentication brings the CPE into the trusted domain but not necessarily all applications at the CPE

Figure 2: Simplified view of 3GPP IMS domains mapped to ECNS

The authentication mechanism does not provide separate authentication of each service on the broad assumption that all services are offered to the same identity and therefore there is no need to give authorization and authentication on a per-service basis.