ETSI TR 187 002 V2.1.1 (2008-12)

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-07030-NGN-R2

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 the NGN.

The present document follows the method and proforma for carrying out a TVRA defined in TS 102 165-1 [i.4] 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 the NGN.

NOTE 1: Depending on the actual instantiation of the NGN some of the assumptions declared in the present document may not fully hold and this may alter the associated risks.

NOTE 2: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

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

The following referenced documents are not essential to the use of the ETSI deliverable but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

[i.3] ISO/IEC 13335: "Information technology - Guidelines for the management of IT security".

[i.4] ETSI TS 102 165-1, (V4.2.1): "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.5] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[i.6] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.7] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.8] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[i.9] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[i.10] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[i.11] 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".

[i.12] 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]".

[i.13] 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)".

[i.14] AS/NZS 4360: "Risk Management".

[i.15] 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.16] 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.17] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[i.18] IETF RFC 3261: "SIP: Session Initiation Protocol".

[i.19] 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)".

[i.20] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 Release 6)".

[i.21] ITU-T Recommendation H.248: "Gateway control protocol".

[i.22] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".

[i.23] ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

[i.24] IETF RFC 2535: "Domain Name System Security Extensions".

[i.25] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[i.26] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".

[i.27] IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".

[i.28] Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".

[i.29] Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".

[i.30] Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".

[i.31] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.32] 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.33] 3GPP TR 33.803: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Coexistence between TISPAN and 3GPP authentication schemes (Release 7)".

[i.34] 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.35] ETSI TS 183 017: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol Specification".

[i.36] IETF RFC 1631: "The IP Network Address Translator (NAT)".

[i.37] IETF RFC 1918: "Address Allocation for Private Internets".

[i.38] IETF RFC 3489: "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".

[i.39] IETF draft, draft-ietf-behave-rfc3489bis-13 (November 2007): "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".

[i.40] IETF draft, draft-ietf-mmusic-ice-19 (October 2007): "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[i.41] IETF draft, draft-behave-turn-02 (February 2006): "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)".

[i.42] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN".

[i.43] ETSI SR 002 211: "Electronic communications networks and services; Candidate list of standards and/or specifications in accordance with Article 17 of Directive 2002/21/EC".

[i.44] ETSI TS 181 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN services and IPTV".

[i.45] Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Definitions and abbreviations

3.1 Definitions

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

attack: attempt to bypass security controls on a computer

NAT traversal: term used to describe the problem of establishing connections between hosts in IP networks which use NAT devices (either locally or remotely) to modify their local IP address

Network Address Translation: method by which IP addresses are mapped from one realm to another in order to provide transparent routing to hosts

NOTE: NAT devices are used to connect address domains with private (unregistered) addresses to public domains with globally unique (registered) addresses.

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 [i.3].

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

NOTE: See AS/NZS 4360 [i.14].

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
AF	Application Function
AGCF	Access Gateway Control Function
AGW	Access GateWay
AH	Authentication Header
A-MGF	Access Media Gateway Function
A-RACF	Access-Resource and Admission Control Function
ARGW	Access Residential media GateWay
AS	Application Server
BGF	Border Gateway Function
BTF	Basic Transport Function
CC	Call Control
CD	Compact Disc
CHAP	Challenge Handshake Authentication Protocol
CLF	Connectivity session and repository Location Function
CPE	Customer Premises Equipment
C-RACF	Core-Resource and Admission Control Function
CSCF	Call Session Control Function
DNS	Domain Name System
DNSSEC	DNS SECurity
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
FQDN	Fully Qualified Domain Name
GPRS	GSM Packet Radio System
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	IMS subscriber Identifier
IP	Internet Protocol
IPsec	Internet Protocol security
IPTV	Internet Protocol TeleVision
ISDN	Integrated Services Digital Network
ISIM	IMS Subscriber Identity Module
ISO	International Standards Organization
ISUP	ISDN User Part
IVR	Interactive Voice Response
MAC	Message Authentication Code
MD	Message Digest
MGC	Media Gateway Controller
MGW	Media GateWay
MRFP	Media Resource Function Processor
NANP	NGN Access Network Provider
NASS	Network Access SubSystem
NAT (1)	Network Address Translator (device)
NAT (2)	Network Address Translation (process)
NAT-T	Network Address Translation Traversal
NCP	NGN Connectivity Provider
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
PoC	Push to talk over Cellular
PS	Packet-Switched
PSTN	Public Switched Telephone Network
RACS	Resource Admission Control Subsystem
RAMR	Realistic-Achievable-Mesurable-Relevant
RCEF	Resource Control Enforcement Function
RGW	Residential GateWay
R-MGF	Residential Media Gateway Function
ROM	Read-Only Memory
RTCP	Realtime Transport Control Protocol
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
SPDF	Service Policy Decision Function
SpoA	Service point of Attachment
STUN	Simple Traversal of UDP through NAT
TCP	Transport Control Protocol
TDM	Time Division Multiplex
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TOE	Target Of Evaluation
TPF	Transport Processing Function
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability Risk Assessment
UAAF	User Access Authorization Function
UDP	User Datagram Protocol
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.