ETSI TR 187 009 V2.1.1 (2008-07)

Technical Report

Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN

Reference

DTR/TISPAN-07025-NGN-R2

Keywords

Regulation, 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 seeks to determine if UC is a risk to the NGN user or to the NGN Operator (a CSP using NGN technology to provide services).

The present document offers justification for UC countermeasures by presenting the results of a Threat Vulnerability and Risk Analysis (TVRA) that quantifies the likelihood and impact of UC in the NGN where UC is initiated in a variety of forms described using a number of scenarios for illustration.

The present document defines the term unsolicited communication in the context of the NGN.

Where risk is shown from UC in the NGN the present document considers means to mitigate the risk using metrics of applicability, effectiveness and architectural instantiation.

NOTE: Whilst this 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 present document 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] OMA-RD-CBCS-V1-0-20060711-C: "Categorization Based Content Screening Framework Requirements".

[i.2] OMA-AD-CBCS-V1-0-20060828-D: "Categorization-based Content Screening Framework Architecture".

[i.3] IETF RFC 5039: "The Session Initiation Protocol (SIP) and Spam".

[i.4] ETSI TS 183 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

[i.5] ETSI ETS 300 128: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Service description".

[i.6] ETSI TS 183 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol Specification".

[i.7] ETSI TS 183 007 (V2.0.0): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

[i.8] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services.

[i.9] 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 - OJ L 201, 31.07.2002).

[i.10] ETSI TS 102 165-1: "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.11] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.12] 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.13] IETF draft-niccolini-sipping-spitstop: "Signalling TO Prevent SPIT (SPITSTOP) Reference Scenario".

[i.14] IETF draft-niccolini-sipping-feedback-spit: "SIP Extensions for SPIT identification".

[i.15] IETF draft-jung-sipping-authentication-spit: "Authentication between the Inbound Proxy and the UAS for Protecting SPIT in the Session Initiation Protocol (SIP)".

[i.16] IETF draft-schwartz-sipping-spit-saml: "SPAM for Internet Telephony (SPIT) Prevention using the Security Assertion Markup Language (SAML)".

[i.17] IETF draft-froment-sipping-spit-authz-policies: "Authorization Policies for Preventing SPIT".

[i.18] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.19] ETSI TS 186 006-1: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Part 1: Protocol Implementation Conformance Statement (PICS)".

[i.20] ETSI EN 300 798: "Digital Audio Broadcasting (DAB); Distribution interfaces; Digital baseband In-phase and Quadrature (DIQ) interface".

[i.21] ETSI TR 141 031: "Digital cellular telecommunications system (Phase 2+); Fraud Information Gathering System (FIGS); Service requirements; Stage 0 (3GPP TR 41.031 version 6.0.0 Release 7)".

[i.22] ETSI TS 122 031: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 1 (3GPP TS 22.031 version 6.0.0 Release 7)".

[i.23] ETSI TS 123 031: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Fraud Information Gathering System (FIGS); Service description; Stage 2 (3GPP TS 23.031 version 6.0.0 Release 7)".

[i.24] ITU-T Recommendation X.1244 (former X.ocsip): "Overview of countering SPAM for IP multimedia application".

[i.25] ITU-T Recommendation X.fcsip: "Technical Framework of Countering IP Multimedia SPAM".

[i.26] ITU-T Recommendation X.1231: (former X.csreq) - "Requirement on countering SPAM".

[i.27] 3GPP TR ab.cde [draft]: "Group Services and System Aspects; Protection against SMS, MMS and IMS SPAM; Study of Different SPAM Protection Mechanisms. Release 8.".

NOTE: This work item was never be finalized, for references please have a look at:

- 3GPP,"Protection against SMS and MMS spam", SP-060446, SA#32;
- Orange, "Consumer protection against spam and malware", S3-060331, Athens, April 2006;
- Nokia, "Anti-spam work in OMA and IETF", S3060504, 3GPP S3#44, Talinn, July 2006;
- Orange, "Spam Flagging using In-band Signaling in Mobile and Broadband Networks", S3-070094 TSGS3#46 Beijing 2007.

[i.28] 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".

3 Abbreviations

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

ACR	Anonymous Communication Rejection
CAMEL	Customized Applications for Mobile network Enhanced Logic
CBCS	Categorization Based Content Screening
CSP	Communications Service Provider
DAB	Digital Audio Broadcasting
DIQ	Digital baseband In-phase and Quadrature interface
DoS	Denial of Service
FIGS	Fraud Information Gathering System
gsmSCF	GSM Service Control Function
gsmSSF	GSM Service Switching Function
HPLMN	Home Public Land Mobile Network
ICAP	Internet Content Adaptation Protocol
ICB	Incoming Communication Barring
IDD	International Direct Dialling
IETF	Internet Engineering Task Force
IP	Internet Protcol

ISDN	Integrated Services Digital Network
IST	Immediate Service Termination
ITU	International Telecommunication Unit
MCID	Malicious Call Identification
NGN	Next Generation Network
ODB	Operator Determined Barring
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
OMA	Open Mobile Alliance
PICS	Protocol Implementation Conformance Statement
PSTN	Public Switched Telecommunications Network
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SIPPING	Session Initiation Proposal Investigation
SPIT	SPAM over Internet Telephony
TAP	Transferred Account Procedure
TVRA	Threat Vulnerability and Risk Analysis
UC	Unsolicited Communication
UE	User Equipment
UMTS	Universal Mobile telecommunication System
VPLMN	Visited Public Land Mobile Network
WG	Working Group

4 General overview

In the email environment the instance of SPAM, the common name used to refer to bulk Unsolicited Communication (UC) where the benefit is weighted in favour of the sender, has proliferated in recent years. SPAM is recognized as a problem and is regulated against, at least in part, in the context of the Privacy Directive 2002/58/EC [i.9], specifically in article 13. However, as has been noted in SR 002 211 [i.28]: "Whilst proprietary technical means exist to assist algorithms that identify and filter spam emails, the legal framework for application of such means in face of processing error is uncertain. Article 13 supports the legal instruments under which spammers may be prosecuted but does not seem to imply technical provision."

As the NGN moves towards adoption of similar protocols for signalling and transport as used in email applications and services, there is a threat that similar UC phenomena will migrate to the NGN and may escalate in severity.

NOTE 1: UC existed in the pre-NGN PSTN/ISDN and treatment of such calls when characterized as either nuisance or malicious calls has been well documented and is not repeated in the present document.

In order to be considered as NGN Unsolicited Communication (UC) the characteristics of a call that allows it to be classified as UC have to be defined. The characteristics of telephony in the modern era of International Direct Dialling suggest that in the general case communication is unsolicited, i.e. when the phone rings it is rarely as a result of a planned and jointly agreed event (solicited) between the communicating parties. Unsolicited cannot be used as a synonym for unwelcome, similarly unsolicited cannot be used as a synonym for attack. The classification of a call by the recipient is complex and the definition of SPAM given in SR 002 211 [i.28] suggest that 3 criteria have to be met at the same time:

1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and

2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and

3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

The characteristics of the NGN may lead to greater load on the infrastructure as a result of more attempts to deliver UC as the signalling offers the possibility to deliver multiple media to the destination in parallel (e.g. voice and text).

The aim of security in the NGN is multifold and includes the ability to restrict the ability of threat agents to operate where the threat agents give rise to unwanted incidents, and to ensure that CSPs of NGNs have tools that allow them to operate in conformance to national and regional regulation in the areas of privacy and user (customer) protection. The means used to achieve this may encompass mechanisms, processes and methods that give assurance of confidentiality, integrity, authenticity, authority, reliability and availability of the services of the NGN.

NOTE 2: In the present document SPIT (voice SPAM) is used with the same meaning as UC (Unsolicited Communication).

5 Threat analysis for UC in the NGN

NOTE: In this study it is not investigated who is the source of UC, as an example set this could be classified as:

- specific users, user groups or call centres;
- IVR systems;
- or even normal legal users with a strong identity where their UE gets misused by e.g. trojans horses, viruses or worms to spread UC.

5.1 UC attack configurations for basis of TVRA

NOTE: In each of the scenarios that follow the NGN may be composed of 2 or more interconnected domains.

5.1.1 Scenario 1: One-to-One UC

In this scenario the single originator attempts to invoke one or more communication sessions towards a single destination.

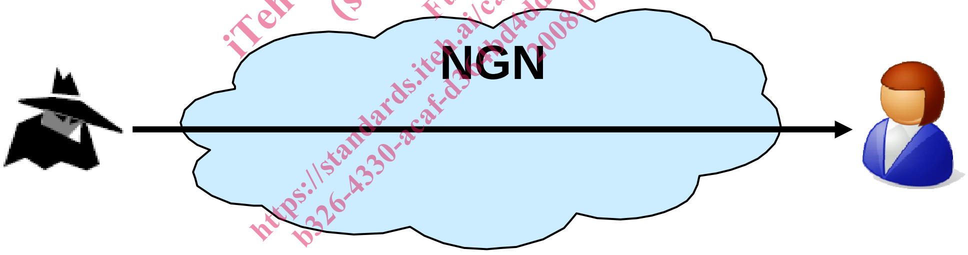

Figure 1: Scenario for 1-to-1 UC

UC pattern:

- one originator;
- one destination;
- one or many communication attempts.

EXAMPLE: Telemarketing where an originator tries to places calls to one user.

This scenario, when applied to email, would not normally be considered as SPAM as although it meets the 3 criteria from SR 002 211 [i.28], it fails when considered as bulk transmission.

This scenario, when applied to pre-NGN networks, would not normally be considered as UC as telemarketing is a legitimate business exercise. In most telecommunications networks offered under the Authorization Directive 2002/20/EC [i.8], there are voluntary codes of conduct within the telemarketing industry to ensure that users (potential recipients) are able to control their exposure to unsolicited telemarketing.