ETSI TR 185 008 V2.0.0 (2008-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of security mechanisms for customer networks connected to TISPAN NGN R2

Reference

DTR/TISPAN-05017-NGN-R2

Keywords

authentication, gateway, network, service, 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

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 present an analysis of the security mechanisms that could be supported in the customer environment (Customer Network Gateway or Customer Devices) with reference to the overall end to end security architecture for the NGN defined by WG7. As examples, these mechanisms can be related to authentication (for connectivity and for services), firewalling and network access/parental control, virus protection, intrusion detection, Anti Spam capabilities. The activity will be performed in close relationship with WG7.

The reactions to threats or the protections against threats described in the present document will involve only the CPN, not the external network.

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

None.

2.2 Informative references

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

[2] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (Release 7) (3GPP TR 21.905)".

[3] ISO/IEC 7498-2: "Information Processing Systems - Interconnection Reference Model - Part 2: Security Architecture".

[4] draft-ietf-nea-requirements-04.txt, Network Endpoint Assessment (NEA): "Overview and Requirements", August 2007.

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

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

[7] ETSI TS 133 246: "Universal Mobile Telecommunications System (UMTS); 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[8] ETSI TS 133 110: "Universal Mobile Telecommunications System (UMTS); Key establishment between a UICC and a terminal".

[9] ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[10] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN Customer Devices architecture and interfaces".

[11] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[12] IETF RFC 1827: "IP Encapsulating Security Payload (ESP)".

[13] IEEE 802.11a: "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band".

[14] IEEE 802.11b: "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band".

[15] 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".

[16] IEEE 802.11g: "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: Further Higher Data Rate Extension in the 2.4 GHz Band".

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication: property by which the correct identity of an entity or party is established with a required assurance.The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [2])

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [3])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

3.2 Abbreviations

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

AES	Advanced Encryption Standard
AV	Anti-Virus
CND	Customer Network Device
CNG	Customer Network Gateway
CPN	Customer Premises Network
EAP	Extensible Authentication Protocol
FMCA	Fixed-Mobile Convergence Alliance
IDS	Intrusion Detection System
IMS	IP Multimedia subsystem
IPSEC	Internet Protocol SECurity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MMS	Multimedia Messaging Service
MPLS	Multiple Protocol Label Switching
NAC	Network Access Control
NAT	Network Address Translation
NEA	Network Endpoint Assessment
P-CSCF	Proxy-Call Session Control Function
PDA	Personal digital assistant
RTP	Real-time Transport Protocol
SMS	Short Message Service
SSL	Secure socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UC	Unsolicited Communication
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTM	Unified Threat Management
VPN	Virtual Private Network
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WPA2	Wi-Fi Protected Access 2

4 CPN Reference Architecture

A typical example of architecture could be the following one, where several types of devices are connected to the CNG. Of course, there could be several of each type.

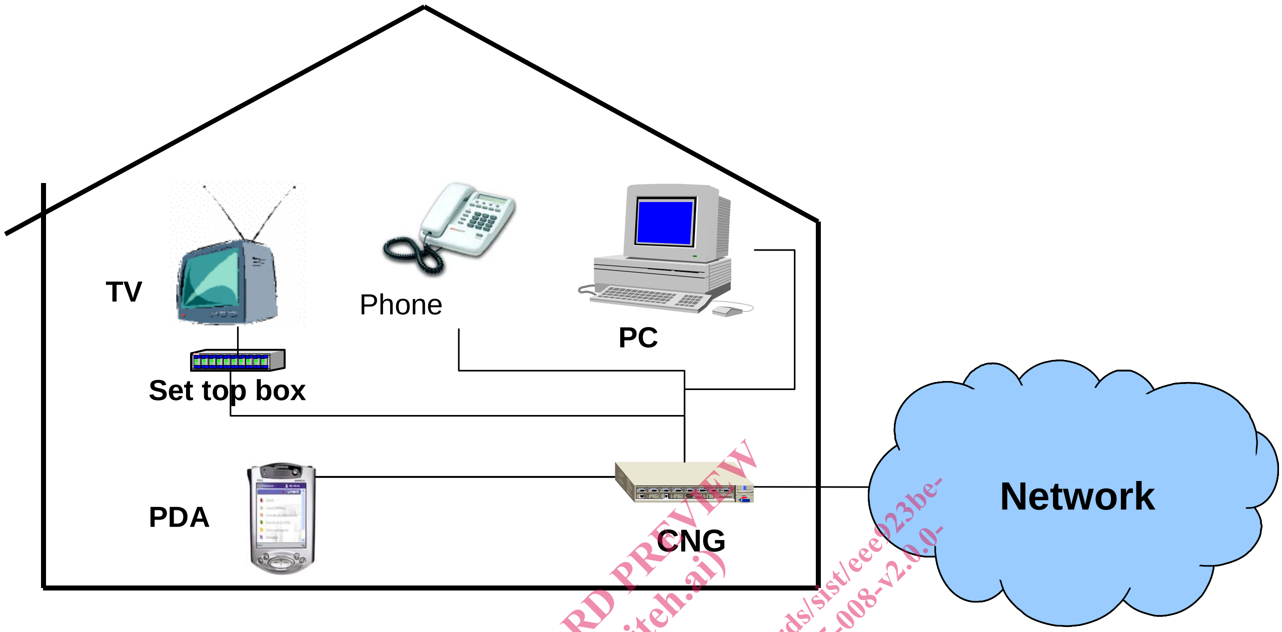

Figure 1: Example of CNP architecture

5 Main security threats and security recommendations

Considering the CPN, security problems can have two origins. They can be originated from inside the CPN, or from outside the CPN. The external origin itself can be sub-divided into two parts, the legitimate network to which the CPN is connected, or a non legitimate network to which the CPN can be accidentally connected (e.g. WLAN).

Threats on security can be categorized with the following:

- System/device integrity: case of the virus attack, malware.
- Unsolicited information: it can be either spam problems (can lead to device integrity problem in case of virus transmission) or display of text, pictures, video, not initially requested by the customer.
- Unauthorized access: this could either be an external third party accessing the CPN (and using it to access services through the CNG), or someone authorized to access an use the CPN but accessing unauthorized data in the network (e.g. children accessing adult content).
- Confidentiality: private data can be protected from interception during communication, or from being stolen (due to spyware or unauthorized access).
- Service availability: contains all the actions that would lead to a DoS.
- Masquerade: this term covers all the possibilities for a spoofing attack as already known on the Internet. This is mainly man-in-the-middle attack and internet protocol spoofing, URL spoofing and phishing, referer spoofing, poisoning of file-sharing networks, caller ID spoofing, e-mail address spoofing, login spoofing.

The starting point for security recommendations is the following already existing security requirements found in TS 185 005 [9]:

- [The CNG shall support mechanisms to authenticate itself to the NGN for connectivity purposes.
- The CNG shall support mechanisms to authenticate itself to the NGN for service usage purposes.

- The CNG shall support mechanisms to authenticate CNDs to the NGN for service usage purposes if they are not able to fully support the related procedures in an autonomous way.
- The CNG shall support mechanisms for authentication of wireless CNDs for local connectivity. Similar mechanisms may be also implemented for non-wireless devices.
- The CNG and CPN shall support mechanisms that prevent access to the network by unauthorized users.
- The capacity of the authorized entities should depend on the security policies defined by the service providers, managing the CNG.
- The CNG and the CPN shall implement mechanisms to limit the visibility of the WAN side network and resources to authorized entities.
- The diagnostic operations on the CPN by an operator shall be performed in accordance with rules protecting the users' privacy.
- CPN environment shall be protected with a stateful firewall function, which may be implemented in the CNG.
- The CNG and the CPN shall be able to support parental control related functionalities limiting the use of the broadband connection on a user or time basis. Limitations on a content basis may be shared with devoted network servers.]

The following recommendation is proposed to enhance the above existing security requirements defined in TS 185 005 [9] (WI05014):

- A mechanism to allow and manage different levels of user's rights can be implemented.

6 Security mechanisms for Customer Premises Network

Depending on the various threats and their large abilities to disrupt the CPN, several security mechanisms should be taken into account.

The CPN environment also hosts several kinds of users: families with children, teleworkers, friends and neighbours and so on. Each users could be the target (or the source) of specific threats and hence may require specific security mechanisms (i.e. VPN for teleworkers, parental control for children, etc.).

6.1 Authentication and authorization mechanisms

Security threats addressed:

- masquerade;
- unauthorized;
- access.

Level of action in the CPN: gateway authentication and authorization, device authentication, user authentication and authorization, message authentication, authentication and authorization of a user for access to a service or set of services, and authentication of the network and/or service provider.

- CNG authentication: connectivity authentication towards the Network Domain Security.
- CND authentication: local authentication towards the local access point (e.g. Wi-Fi access point) embedded in the gateway. Methods to establish shared keys for authentication are proposed within TS 133 110 [8] and TS 133 246 [7].
- User authentication: to access service platform in general.
- Message and Service authentication: to access a specific service/application.