TISPAN NGN Security standards

Judith E. Y. Rossebø
ETSI TISPAN WG7 Chairman
Telenor GBD&R

© ETSI 2009. All rights reserved
Overview

- ETSI TISPAN NGN
- TISPAN Security Standards
- TISPAN NGN R3 Security Standards
  - Overview
  - CPN Security
  - IPTV Security
- Hot topics for Future Work
- Summary
TISPAN NGN Releases

- **NGN Release 1**: (December 2005)
  - Adopts the 3GPP IMS standard for SIP-based applications, and adds further functional blocks and subsystems to enable fixed access to IMS and to handle non-SIP applications

- **NGN Release 2**: (April 2008)
  - Release 1 enhancements (transfer of IMS enhancements and PSS to 3GPP)
  - PSTN/ISDN Emulation – analogue and ISDN
  - New topics: IPTV, Home Networks, Corporate Networks

- **NGN Release 3**: (ongoing, target for stage 3: March 2010 with some exceptions)
  - Improvement of several aspects introduced in the previous Releases, such as:
    - IPTV service evolution
    - IP Network to Network interconnection
    - Home Network interconnection
  - New topics: CDN
  - Feasibility studies: P2P, Interactions RACS – Home networks
TISPAN – the NGN global solution

- IMS-based IPTV
- PES IMS
- Hosted Enterprise Services
- Business Trunking Services
- Dedicated IPTV
- PSTN/ISDN Emulation

Service & Control Functions

Transport User Profiles

Network Attachment Subsystem

Resource & Admission Control Subsystem

Transport Control Functions

Transport Functions

Home Network

Legacy Terminals

3G Radio Access

IPTV

NGN Terminals

Service User Profiles

ETSI TISPAN

Other Networks (NGN/PSTN/IP)

NGCN Business Trunking
TISPAN NGN Security Standards:

- NGN Security requirements (TS 187 001)
- NGN eTVRA (TR 187 002)
- NGN Security architecture (TS 187 003)
- NGN Lawful Interception functional entities, information flow and reference points (TS 187 005)

- Specifications for (PUC) Prevention of Unsolicited Communication in the NGN (DTS/TISPAN-07034-NGN-R3)
- RFID Security and Privacy (DEN/TISPAN-07042)

- New! RFID system and network security and privacy protection (DTR/TISPAN-07044)
- New! Security services and mechanisms for customer premises networks connected to TISPAN NGN
- New! Data Retention in the NGN (TS 187 017)
TISPAN NGN security feasibility studies

- Security of the Interconnection – study of:
  - Current security measures and gap analysis
  - Definition of the security architecture for the NNI

- IPTV Security Architecture – study of:
  - Models and key management systems for service protection with the aim to develop the model for the NGN
  - Functional entities and mechanisms for service protection with the aim to define these for the NGN
  - A framework open to the integration of content protection solutions
SECURITY:
Customer Premises Network Threat, Vulnerability and Risk Analysis

STF357 and TISPAN-WG5/WG7
For the full analysis see: draft TR 187 002
TISPAN sees Home Networks as an IMS NGN end-point

Customer Premises Network (CPN)

NGN /IMS Core + transport

Customer Network Devices (CND)

NGN Terminals

Access Network

Network Attachment Subsystem

Resource & Admission Control Subsystem

CPN TVRA – Purpose and Scope

- TVRA (Threat, Vulnerability and Risk Analysis) is an ETSI standard for risk assessment, security analysis and security requirements elicitation

- The purpose of TVRA is to improve the security of a system by:
  - Providing an understanding of the security threats to a system
  - Specifying possible countermeasures where necessary

- The purpose of CPN TVRA was to integrate a comprehensive and consistent but not excessive set of security functionalities into the Customer Network Gateway (home gateway)
  - The gateway must protect the user equipment and itself against attacks, malicious exploitation or other security attacks
    (a) from within the CPN
    (b) from attacks originating in the network (NGN)
CPN Target Of Evaluation (TOE)

TOE Environment

CPN

SIP Terminal
IMS Terminal
Terminal Adapter
Set Top Box

Target Of Evaluation

CNG

NGN

Gm
Ut
Ut ' e1', 'e3'

Gm
Ut ' e1', 'e3'

Gm
Ut ' e1', 'e3'

Dj
'e1', 'e3'

The ETSI TVRA method involves 7 steps:

- Identify Security Objectives
- Identify Functional Security Requirements
- Produce Inventory of Assets
- Classify Vulnerabilities and Threats
- Quantify Likelihood and Impact of Threats
- Determine Risks
- Specify Detailed Requirements (Countermeasures)
Threat Analysis

Threats considered:

- Denial of service
- Eavesdropping
- Masquerade
- Unauthorized access
- Loss of information
- Corruption of information
- Repudiation

The system is designed to support $n$ Usage Cases and Functions, each of which has a Value and a Cost to users or the operator.

There are $k$ Assets.

Each Asset has 0, 1 or more Weaknesses.

Each Weakness has 1 or more Risks.

Each Risk allows one or more possible Attacks with a probability of negative impact on the Assets, i.e., expectation of damage.

Each Attack can be prevented or reduced by one or more Countermeasures.

Each Countermeasure needs one or more AddOn Functions (Functionality) to implement/enable the Countermeasure.

Each additional AddOn Function is itself an Asset; ...and needs to be reconsidered in the Total System Design; ... And may even add Usage Cases which add value.
CPN TVRA – Results

- The CPN TVRA identified the security attacks that pose either a major or critical risk to the CNG, and thus the CPN
- The CPN TVRA specified a set of detailed security requirements to counter the identified attacks
  - 4 confidentiality requirements
  - 9 identification, authentication and authorization requirements
  - 5 integrity requirements
  - 3 availability and DoS prevention requirements
- The requirements that resulted from the CPN TVRA were analyzed by WG5 and WG7
  - In order to obtain a concise, minimal set of essential requirements
  - Taking into account the views/feedback/input of the different stakeholders (e.g. operators, suppliers, regulators) regarding cost/benefit issues
Example

- **Weaknesses:** General protocol weaknesses, Lack of DoS protection
- **Threat:** Flooding the CPN for Denial of Service
- **Countermeasure:** DoS attack detection capabilities, Dos attack prevention measures

- **Resulting in the following DoS protection requirement:**
  - On detection of any system failure or discontinuity not specifically handled by other mechanisms the CNG shall revert to a known safe state.
IPTV Security Architecture TR 187 013

- Study of options for IPTV security architecture to provide IPTV service protection
- Provides a general model for IPTV key management and distribution architecture
  - Explores candidate key hierarchies (3 layer and 4 layer models)
- Several candidate solutions are analyzed against the TISPAN IPTV security requirements
  - MBMS
  - OMA BCAST
  - DVB Simulcrypt-based approach for service protection
- The aim is to provide an open framework to allow the operator a choice between one or more protection solutions
  - OMA BCAST solution as first recommended
TISPAN IPTV Protection

- Service protection: the protection of content (e.g. files or streams) and service information during delivery which may include content already protected and meta data that the service provider adds to the content.
  - Note: The service may be composed of the content to be transferred and other data and service components. Service protection addresses protecting this composition while in transit and regulates authorized access to the service. Additionally it addresses ensuring the service availability, as defined in the service level agreements.

- Content protection: protection of content or content assets during its entire lifetime.
  - NOTE: The content provider defines the lifetime that the protection is required for.
RFID system and network security and privacy protection (DTR/TISPAN-07044)

- Response to EU Mandate 436 in relation to privacy, data protection and information security

Two objectives:
- Describe and set guidelines for promoting confidence and trust in RFID applications
- Define recommendations for RFID system and network security and privacy protection
Specifications for PUC in the NGN
(DTS/TISPAN07034-NGN-R3)

- Requirements for PUC
- PUC functional architecture
- Mapping of the architecture for the following NGN scenarios:
  - Home networks, CND – CNG – NGN.
  - Enterprise networks, NGCN – NGN.
  - Single user scenario, UE – NGN.
- Proposing UC detection & handling for each of the scenarios.
Hot Topics for Beyond R3

- TISPAN NGN security
  - RFID security and Privacy
  - IPTV security (enhancement of stage 2, definition of stage 3)
  - Adding UC prevention as a feature (enhancement of stage 2, stage 3)
  - Security for Customer Premises Networks (CPN) (stage 2, stage 3)
  - Security for NGN management networks.
  - Protection mechanism in context of Identity Management.
  - Security for the Internet of Things (IoT) in the context of the NGN
  - NGA (next generation access network) security (for example security for GPON) in coordination with BBF
  - Analyse the inter-relation between security features and architecture of the NGN (IPTV, NAT-T, NASS, RACS etc.) in terms of how to employ consistent security architecture and mechanism
TISPAN WG7 is responsible for the management and co-ordination of the development of security specifications for TISPAN.

- For the NGN, TISPAN WG7:
  - Defines security requirements;
  - Defines the security architecture
    - Interactive Webpage available;
  - Conducts threat and risk analyses for specific NGN use cases
  - Proposes countermeasures.

WG7 security standardisation is risk-based:
Using the ETSI TISPAN methodology for systematic threat, vulnerability and risk analysis (TVRA)
THANKS FOR YOUR ATTENTION

ETSI TISPAN Portal:
http://portal.etsi.org/Portal_Common/home.asp
For more information

- European Telecommunication Standardisation Institute
  [www.etsi.org](http://www.etsi.org)

- TISPAN security working group chair
  judith.rossebo@telenor.com

- TISPAN security working group vice chair
  Thilo.Ewald@nw.neclab.eu