NGN Security standards for Fixed-Mobile Convergence

Judith E. Y. Rossebø
Telenor R&I
ETSI TISPAN WG7 Chairman
(judith.rossebo@telenor.com)

2nd ETSI Security Workshop: Future Security
16-17 January 2007 - Sophia-Antipolis, France
Overview

- ETSI TISPAN
  - WG7 security
- ETSI NGN security
  - Process for Security Standardisation
  - Threat analysis and example
- ETSI NGN Security Standards
  - Current focus
  - NGN security documents – published and ongoing
- Conclusions
What is ETSI TISPAN?

TISPAN: Telecommunication and Internet converged Services and Protocols for Advanced Networking

NGN: Next Generation Networks

TISPAN NGN: Converged Fixed-Mobile solutions

A significant step has been taken to enable the Multimedia Fixed-Mobile Convergence in TISPAN NGN Release 1

cooperating with 3GPP
TISPAN NGN Architecture

IMS

NASS
Network Attachment Subsystem

Policy control, resource reservation, admission control. Network Address Translator and Firewall traversal.

Dynamic provision of IP address User, Authentication, Authorisation, Location management etc.

TISPAN xDSL Connectivity Network

Access Transport Network

Resource Control Subsystem

PSTN/ISDN Emulation to support legacy terminals

(SIF-based) IP Multimedia Subsystem Core IMS

PSTN/ISDN emulation Subsystem

Fixed Mobile Convergence FMC:
IMS supports Fixed and Mobile networks in a single architecture

January 2007
TISPAN NGN fixed-mobile convergence

- ETSI TISPAN proposes an architecture basis consisting of a range of subsystems:
  - Access network attachment subsystem
  - Resource and admission control sub-system
  - PSTN-ISDN emulation subsystem
  - IP Multimedia Subsystem (IMS) (from 3GPP)
  - IPTV Subsystem
- TISPAN is adopting standards from other bodies where appropriate
- When applicable TISPAN re-uses 3G specifications
  - in a process of endorsement where IMS is jointly developed
TISPAN Working Group (WG) 7 is responsible for the management and co-ordination of the development of security specifications for TC TISPAN.

- For TISPAN NGN Release 1, TISPAN WG7 has:
  - Defined security requirements;
  - Defined a security architecture for NGN R1;
  - Conducted threat and risk analyses for specific NGN use cases;
  - Proposed countermeasures.
  - Standardized Lawful Interception functional entities, information flow and reference points.

WG7 security standardisation is risk-based:
Using the STF292 methodology for systematic threat, vulnerability and risk analysis (TVRA)
Process for Security Standardisation

Changes in the Telecommunications Environment → eTVRA analysis → Countermeasures

Countermeasures → eTVRA analysis → Changes in the Telecommunications Environment
Example Scenario: Access to IMS

IMS authentication is linked to the access mechanism, e.g., access line identification.
Threat Analysis
Example 1:

- What is the Threat?
  - No explicit authentication at IMS level for legacy deployments

- Why does it happen?
  - Insufficient coupling to core IMS functions opens for attack

- Is this likely to occur?
  - Highly likely – the attack method may be reapplied

- Consequences (unwanted incidents):
  - Denial of Service (to the real user)
  - Fraud/Costs/financial losses to the real user for calls made by attacker
  - Loss of reputation for the service provider

The risk is not acceptable – countermeasures are required
NASS-IMS bundled: "line-id poisoning" attack

Legend:
P-A-N-I = P-Access-network-info

1) [IMPI_victim != line-id_victim-ref(s)] binding provisioned in UPSF

4) S-CSCF fetches line-id_victim-ref(s) from UPSF as line-id_victim in P-A-N-I matches some of line-id_victim-ref(s)
   => UE_badguy1 authenticated as UE_victim!

3) NBA-not-aware P-SCSF (eg. legacy 3GPP R5/R8 P-CSCF) lets P-A-N-I through to S-CSCF untouched

Similar attack can be identified and blocked in NBA-aware P-CSCF

IMS core

UPSF

I-CSCF

S-CSCF

P-CSCF

P-CSCF_NBA_not_aware

CLF

Access Network 1 (NASS)

Access Network 3

Access Network 2

UE_badguy1

UE_victim

UE_badguy2

2) IMS registration
   - False IMPI_victim in SIP
   - False line-id_victim in P-A-N-I
Mapping of security threats to requirements and to countermeasures

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T-16</td>
<td>NASS-IMS bundled: IP Spoofing</td>
<td>1 (highly likely)</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>R-AA-24</td>
<td>See clause 5.2.1.4.4.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R-AA-13</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R-NF- 2</td>
<td></td>
</tr>
<tr>
<td>T-11</td>
<td>NASS-IMS bundled: Interception at the customer interface, air interface present</td>
<td>4 (highly likely)</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>R-CD-18</td>
<td>Security protection along the e1 IF; see [8].</td>
</tr>
<tr>
<td>T-14</td>
<td>NASS-IMS bundled: Attack potential for manipulation at the customer interface, air interface present</td>
<td>4 (highly likely)</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>R-CD-13</td>
<td>Security protection along the e1 IF; see [8].</td>
</tr>
<tr>
<td>T-19</td>
<td>NASS-IMS bundled: “line-id poisoning” attack</td>
<td>4 (highly likely)</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>R-AA-24</td>
<td>Work in progress (TR 33 803 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R-AA-13</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R-NF- 2</td>
<td></td>
</tr>
</tbody>
</table>
WG7 security countermeasure – Authentication to IMS:

- **ISIM over UICC**
  - Endorsement of the IMS access security mandates this
  - IMS access security extended with NAT traversal due to TISPAN needs.
  - The challenge of using ISIM over UICC in any device is partially being met by ETSI TC SCP:
    - “ETSI TC SCP ... has selected USB technology as the solution for high speed protocol for the UICC from Release 7.”

- **Solution for legacy deployments:**
  - Access to IMS granted based on access network mechanism (NASS-IMS bundled)
  - Optionally, HTTP-digest restricted to fixed access to IMS from legacy terminals
WG7 security – Current focus:

- New threats and risks landscape
- Fixed-mobile convergence
- Media security
- NGN (security) protocols must work in presence of NATs
- IPTV security
- Impact of unsolicited communication in the NGN environment
- Adoption of the eTVRA method and closer alignment with Common Criteria
NGN Security Documents

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

- NGN security documents in progress
  - NGN Security countermeasures (TS 187 006)

- NGN Feasibility studies in progress
  - Generalized NAT traversal (TR 187 007)
  - Media security (TR 187 008)
  - Impact of unsolicited communication in the NGN (new)
Security Guidance and Methods Documents:

- **ETSI Common Criteria (CC) Guidance documents for standards:**
  - Guide to CC for standards developers (EG 202 387)
  - PP method and proforma (ES 202 382)
  - ST method and proforma (ES 202 383)
  - Application of security countermeasures to service capabilities (EG 202 549)

- **ETSI Security Standardisation guidance and methods documents**
  - eTVRA (TS 102 165-1:2006)
  - Protocol Framework Definition; Security Counter Measures (TS 102 165-2:2006)

- **ETSI scheduled work:**
  - STF-QY : Use of CC capabilities in NGN
  - STF-QZ : Security and management of identity in NGN
NGN SEC from common methods

ETSI security standardisation method documents

TR 187 002 NGN eTVRA

TR 187 001 NGN Security Requirements

TS 187 003 NGN Security Architecture

TS 187 006 NGN Countermeasures

NGN Security requirements analysis

NGN Security documents
NGN Feasibility Studies Feed into TISPAN
Core Security Documents:

- WI 07021 Feasibility Study on Media Security
- WI 07022 NAT Traversal Feasibility Study Report
- WI 07025 Feasibility Study of Prevention of Unsolicited Communication in the NGN
- TR 187 001 NGN Security Requirements
- TR 187 002 NGN eTVRA
- TS 187 003 NGN Security Architecture
- TS 187 006 NGN Countermeasures
WG7 security - Conclusions

- TISPAN WG7 has addressed NGN security
  - New risks
    - an IP-world...
    - a large legacy base...
    - diversity of access and terminals...

- ETSI TISPAN WG7 has addressed the threats and challenges for securing the NGN
  - Systematic threat, vulnerability and risk analysis (TVRA)
  - Based on the results of the TVRA countermeasures are being standardised

- ETSI TISPAN WG7 is now working to secure advanced services by considering:
  - Fixed-mobile convergence
  - Media security
  - NGN (security) protocols working in presence of NATs
  - IPTV security
  - Impact of unsolicited communication in the NGN environment
THANKS FOR YOUR ATTENTION

Questions/Comments?

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 specialist task force leader [scott.cadzow@etsi.org](mailto:scott.cadzow@etsi.org)
- TISPAN security working group chair [jJudith.rossebo@telenor.com](mailto:jJudith.rossebo@telenor.com)
ETSI Common Criteria Guidance documents

ISO 15408 Common Criteria

ES 202 383 Security Target Method & Proforma
ES 202 382 Protection Profile Method & Proforma
EG 202 387 Common Criteria Guideline for Standards
EG 202 549 Application of Security Countermeasures to Service Capabilities

Common Criteria part 3

Interpretation for standards audience
ETSI Security Standardisation guidance documents

- TC MTS Methods for standards develops
- ETSI Making better standards
- TS 102 165-1 eTVRA Method & proforma
- ETR332

Root ETSI CC guidance documents

ETSI security standardisation guidance documents
Building up ETSI security frameworks

- ISO 9798 Methods
- ISO 10181 Method frameworks
- ISO 2500x Management guidance
- ETSI security standardisation guidance documents
- TS 102 165-2 Method stage1/2
- ETSI security standardisation method documents
Requirements engineering and analysis
(STF work in 2007)
NBA related R1 security requirements (1):
back up slide – clickable link

- (R-AA-13): For the early deployment scenarios (see note 1), where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure. This authentication provides simultaneous access to the access network and IMS services.

  NOTE 1: The two special early deployment scenarios are:
  (A). IMS authentication is linked to access line authentication (no nomadicity)
  (B). IMS authentication is linked to access authentication for IP Connectivity (limited nomadicity can be provided)
NBA related R1 security requirements (2): back up slide

- (R-AA-24): NASS shall support both the use explicit (e.g. PPP or IEEE 802.1x) and/or implicit line authentication (e.g. MAC address authentication or line authentication) of the users/subscribers. In the case of the implicit access authentication, it shall rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer.

- (R-NF-2): Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.
Endorsement strategy

- ETSI TS 133 102; Security architecture
  - No endorsement
- ETSI TS 133 141; Presence service; Security
  - To be endorsed with endorsement of 33.222
- ETSI TS 133 203; Access security for IP-based services
  - To be endorsed to offer protection of SIP signalling.
- ETSI TS 133 210; Network Domain Security (NDS)
  - To be endorsed to allow the use of SEGs in the TISPAN NGN architecture.
- ETSI TS 133 220; Generic Authentication Architecture (GAA); Generic bootstrapping architecture
  - To be endorsed to support endorsement of 33.222.
- ETSI TS 133 222; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)
  - To be endorsed to support endorsement of 33.141.
- ETSI TS 133 310; Network Domain Security (NDS); Authentication Framework (AF)
  - To be endorsed for certificate management