Technical Specification Group Services and System Aspects **TSGS#19(03)0101**

Meeting #19, Birmingham, UK, 17-20 March 2003

**Source:** **SA WG3**

**Title:** **1 CR to 33.203: Malicious UE bypassing the P-CSCF (Rel-5)**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

The following CR was approved by SA WG3 meeting #27 and is hereby presented to TSG SA#19 for approval.

| SA doc# | Spec | CR | R | Phase | Subject | Cat | Current Version | WI | SA WG3 doc# |
|---|---|---|---|---|---|---|---|---|---|
| SP-030101 | 33.203 | 036 | - | Rel-5 | Malicious UE bypassing the P-CSCF | F | 5.4.0 | IMS-ASEC | S3-030119 |
| | | | | | | | | | |

**3GPP TSG-SA3 Meeting #27**
**Sophia Antipolis, France, 25.-28.2.2003**

***Tdoc ⌘S3-030119***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **33.203** | **CR** | **036** | ⌘ **rev** | **-** | ⌘ | Current version: | **5.4.0** | ⌘ |

*For* ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Malicious UE bypassing the P-CSCF | | |
| ***Source:*** | ⌘ | SA WG3 | | |
| ***Work item code:*** | ⌘ | IMS-ASEC | ***Date:*** ⌘ | 26/02/2003 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-5 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Malicious UE could send SIP messages directly to the S-CSCF and bypass the P-CSCF and I-CSCF. |
| ***Summary of change:*** | ⌘ | Recommendations added to protect against bypassing P-CSCF. Additionally, if inter-CSCF traffic is not protected by the NDS/IP mechanisms, then physical protection measures or IP traffic filtering should be applied. However, it is highlighted that this is not in the scope of 3GPP specification. |
| ***Consequences if not approved:*** | ⌘ | Specification would be ambiguous whether this attack scenario applies or not. Without this change the implementation of the specification may result in an insecure system. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | Annex X (new) | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements ".

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

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

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] IETF RFC 2403 (1998) "The Use of HMAC-MD5-96 within ESP and AH".

[16] IETF RFC 2404 (1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[17] IETF RFC 3310 (2002): "HTTP Digest Authentication Using AKA". April, 2002.

[18] IETF RFC 3041 (2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[19] IETF RFC 2402 (1998): "IP Authentication Header".

[20] IETF RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms ".

[21] Draft-ietf-sip-sec-agree-05 (October 2002): "Security Mechanism Agreement for SIP Sessions".

# Annex X (informative): Recommendations to protect the IMS from UEs bypassing the P-CSCF

After the UE does a successful SIP REGISTER with the P-CSCF, malicious UE could try to send SIP messages directly to the S-CSCF. This could imply that the UE would be able to bypass the integrity protection provided by IPSec ESP between the UE and the P-CSCF.

NOTE: The TS 24.229 [8] defines a trust domain that consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF, the MGCF, the MRFC and all the AS:s that are not provided by 3rd party service providers. There are nodes in the edge of the trust domain that are allowed to provide with an asserted identity header. The nodes in the trust domain will trust SIP messages with asserted identity headers. The asserted identity information is useful as long as the interfaces in an operator's network can be trusted.

If a UE manages to bypass the P-CSCF it presents at least the following problems:

1) The P-CSCF is not able to generate any charging information.

2) Malicious UE could masquerade as some other user (e.g. it could potentially send INVITE or BYE messages).

The following recommendations for preventing attacks based on such misbehavior are given:

- Access to S-CSCF entities shall be restricted to the core network entities that are required for IMS operation, only. It shall be ensured that no UE is able to directly send IP packets to IMS-entities other than the required ones, ie. assigned P-CSCF, or HTTP servers.

- Impersonation of IMS core network entities at IP level (IP spoofing), especially impersonation of P-CSCFs by UEs shall be prevented.

- It is desirable to have a general protection mechanism against UEs spoofing (source) IP addresses in any access network providing access to IMS services.

If neither inter-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.